ALIGNING CYBERSECURITY MANAGEMENT WITH ENTERPRISE RISK MANAGEMENT IN THE FINANCIAL INDUSTRY

A thesis submitted for the degree of Doctor of Philosophy

By

Alina Andronache

Brunel Business School

Brunel University London

2019

Dedication

This work is dedicated to my family and friends. They supported and encouraged me unconditionally during my PhD journey, giving me a chance to thrive. It would be hard to express my full gratitude to all who directly or indirectly contributed to this research. There are no words to express my full appreciation.

I would like to thank my family and friends for accepting nothing less than completion from me. Thank you all!

Acknowledgements

This research would not have been possible without the excellent supervision and direction of my academic supervisor, Dr. Abraham Althonayan. I would like to express my sincere appreciation to him for being a tremendous mentor. His continuous guidance, valuable advice, and encouragement have made this academic journey possible.

An extra-special thanks goes to Dr. Weifeng Chen for suggestions, encouragement, and stimulating ideas for presenting my research.

In addition, I would like to thank my fellow doctoral students—those who have moved on, those who have embarked on a new journey, and those who are just finishing—for their support, feedback, and friendship.

Last but not least, my appreciation is extended to respondents who dedicated their time, support, and patience in supporting this research with invaluable industry responses and insights that, in the end, led to the completion of this thesis.

Declaration

This thesis is submitted to Brunel University in support of my application for the PhD degree. This is to certify that this thesis entitled '*Aligning Cybersecurity Management with Enterprise Risk Management in the Financial Industry'* is the result of my own work and has not been previously submitted for any other degree from this or another university. I also declare that all information contained in this document has been produced by me and that the work contained herein is my own except where explicitly specified otherwise in the text. The work presented is in accordance with academic rules and ethical conduct recommended by Brunel University.

List of Publications

Althonayan, A. and Andronache, A. (2019) 'Resiliency under Strategic Foresight: The effects of Cybersecurity Management and Enterprise Risk Management alignment', in: *International Conference on Cyber Situational Awareness, Data Analytics and Assessment Conference (CyberSA 2019),* Oxford, 3-4 June.

Althonayan, A. and Andronache, A. (2019) 'The Emerging Social Media Cyber Risks for Supply Chain Management', in: *International Journal of Operations & Production Management, Special Issue Workshop,* Liverpool, 21-22 March 2019 (unpublished).

Althonayan, A., Matin, S. M. and Andronache, A. (2018) 'Exploring the Ineffectiveness of ERM's and GRC's Role in the Maturity of Organisations' Risk Management', in: *Strategic Management Society, SMS Special Conference,* Hyderabad, 15-18 December 2018.

Althonayan, A. and Andronache, A. (2018) 'Shifting from Information Security towards Cybersecurity Paradigm', in: *International Conference on Information Management and Engineering (ICIME 2018),* Manchester, 22-24 September 2018.

Abstract

Recent years have opened debates amongst academics, practitioners and regulators on how the financial industry's risk resiliency depends on its ability to handle risk holistically. The financial industry is found to be motivated not only by protection purposes or assurance but also by its interest in gaining more return on investment, compliance and effectiveness. It is noticeable that in recent years there has been considerable interest in organisational risk resiliency, but there are still unanswered questions as to why organisations are unsuccessful in applying effective security practice at all levels. Having a robust mechanism to deal with a variety of risks efficiently and in alignment with the organisational strategy has always been something that organisations struggle to accomplish. Changes in internal and external pressures have required organisations to turn their attention from silo operational and managerial risk controls to strategic approaches that can ensure the optimal achievement of the organisation's mission, strategy and objectives.

This research was intended to investigate possible approaches for enabling a more enhanced strategic approach to respond to the extended exposure to all types of risks: to move towards an approach that combines enterprise-wide risk governance with anticipation (proactive response). On the basis that the two types of organisational risk functions cannot be addressed in isolation, this research explored whether the realignment of risk control and risk oversight of the Cybersecurity Management (CsM) and Enterprise Risk Management (ERM) support the establishment of enterprise-wide risk governance. This research responds to the need for harmonised risk handling, reporting, analysis, mitigation and resiliency across an entire organisation. Alignment, in the form of interconnectivity and partnership, can place an entire organisation in a more enhanced state of security through a unified perspective of control, accountability and decision-making. While debates in this subject area have been centred on separate disciplines of ERM, this research posits that CsM and alignment together can further sustain an organisational risk strategy, as together they execute all capabilities in an integrative manner rather than using siloed controls.

The nature of this research is mainly qualitative, as it seeks to explore and interpret the qualitative aspects of the problem. The research was undertaken by considering secondary (literature review, systematic literature evaluation) and primary qualitative data (semi-structured interviews). Weighing up the evidence, it was found that an enterprise-wide alignment of CsM with ERM can enhance risk reporting, analysis, mitigation and resiliency.

However, incorporating both strategies in a unique mechanism appears to be an infrequent approach in the industry. To facilitate a more enhanced strategic approach, this research has examined the effectiveness and sustainability of an integrated *CsM-ERM Strategic Alignment Framework* to support financial organisations in managing their exposure to risks in a strategic manner that employs all efforts towards a single end: to protect and to sustain comprehensive capabilities for the achievement of organisational goals.

Keywords: cybersecurity management; enterprise risk management; financial organisations; risks; resiliency; alignment; strategic approach.

Table of Contents

List of Figures

Chapter One

Chapter Two

Chapter Three

Chapter Four

Chapter Five

Chapter Six

Chapter Seven

List of Tables

Chapter Two

Chapter Three

Chapter Four

Chapter Six

Chapter Seven

List of Abbreviations

AI	Artificial Intelligence
AICPA	American Institute of Certified Public Accountants
AIG	American International Group
ANZ	Australia and New Zealand Banking Group Limited
AS/NZS	Australian/New Zeeland Standards
BoE	Bank of England
BSI	British Standard Institution
CEO	Chief Executive Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CCDCOE	Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
CERT	Computer Emergency Response Team
CESG	Communication Electronic Security Group
CGMA	Chartered Global Management Accountant
CIA	Confidentiality, Integrity, and Availability
CiSP	Cyber-security Information Sharing Partnership
COSO	Committee of Sponsoring Organisations
COO	Chief Operating Officer
COBIT	Control Objectives for Information and Related Technology
CPNI	Centre for Protection of National Infrastructure
CSIS	Centre for Strategic and International Studies
CsM	Cybersecurity Risk Management
EY	Ernst and Young
ENISA	European Union Agency for Network and Information Security

ERM	Enterprise Risk Management
FCA	Financial Conduct Authority
FERMA	Federation of European Risk Management Association
FSOC	Financial Stability Oversight Council
GAISP	Generally Accepted Information Security Principles
GARP	Global Association of Risk Professionals
GLBA	Graham Leach Bliley Act
GRC	Governance, RM, and Compliance
GFC	Global Financial Crisis
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
HM	Her Majesty
IA	Information Assurance
ICAEW	Chartered Accountants in England and Wales
ICAS	The Institute of Chartered Accountants of Scotland
ICT	Information Computer Technology
IEC	International Electrotechnical Commission
IMPACT	International Multilateral Partnership Against Cyber Threats
IoT	Internet of Things
IRM	The Institute of Risk Management
IS	Information Security
ISC^2	International Information System Security Certification Consortium
ISACA	ISACA Information Systems Audit and Control Association
ISM	Information Security Management
ISMS	Information Security Management Systems
ISO	International Organization for Standardisation
IT	Information Technology
GRC	Governance Risk Management and Compliance
NATO	North Atlantic Treaty Organisation
NIST	National Institute of Standards and Technology
NYSE	New York Stock Exchange
OCC	Office of the Comptroller of Currency
OCEG	Open Compliance and Ethics Group

OCSIA	Office of Cyber Security and Information Assurance
OECD	Organisation for Economic Co-operation and Development
PRA	Prudential Regulation Authority
PwC	PricewaterhouseCoopers
RIMS	Risk Management Society
RM	Risk Management
ROI	Return on Investment
ROSI	Return on Security Investment
S&P	Standard and Poor
SAM	Strategic Alignment Maturity
SOCA	Serious Organised Crime Agency
SOX	Sarbanes-Oxley Act
SMEs	Small Medium Enterprises
SRM	Strategic Risk Management
STOPE	Strategy, Technology, Organisation, People, and Environment
TSE	Toronto Stock Exchange
3LoD	Three Lines of Defence
VAR	Value at Risk
VUCA	Volatility, Uncertainty, Complexity and Ambiguity
UBS	Union Bank of Switzerland

1. Chapter One: Introduction

1.1 Introduction

This introductory chapter acts as a guide that structures the overall research. It starts by stating the research rationale by defining the problem, scope and limitations and examining the research aims, objectives and questions that propose to fill the research gap by encompassing the need for alignment between Cybersecurity Management (CsM) and Enterprise Risk Management (ERM). Moreover, the research background demonstrates the research gaps and thus the significance of this study, particularly in view of financial organisations encountering drawbacks in implementing risk control and risk oversight practices. In this early stage, the internal cohesion between the three elements (CsM, ERM, and alignment) is emphasised to augment the rationale of the research. While the investigation initially focuses on general aspects, it aims to articulate the current state of the research problem in order to offer an understanding of the correlation and position of current research, whilst considering prior research and articulating the research gap.

The remainder of the chapter is divided into six sections: Section 1.2 explains the research scope and its projected results; Section 1.3 outlines the rationale of the research, problem definition and problem solution; Section 1.4 presents the aims, objectives and research questions; Section 1.5 explains the research relevance and contribution; Section 1.6 explains the research design and methodology; and Section 1.7 provides a snapshot of the overall structure to outline how CsM alignment with the ERM research problem is going to be explored and validated. Thus, this chapter's propositions are to indicate the setting and direction of the research, in balance with prior contributions within the field (Paltridge and Starfield, 2007).

1.2 Research background

Recent years have opened debates amongst academics, practitioners, and regulators on how financial industry risk resiliency depends upon its ability to handle risk holistically. The reason for outlining enterprise-wide risk governance is because prior research has demonstrated that it represents a core competency for sustainability and efficiency as well as avoiding ripple effects across other interrelated industries (Mikes, 2009; PwC, 2014; Alcaraz and Zeadally, 2015; Verizon, 2018).

Having a robust mechanism to deal efficiently with a variety of risks and in alignment with organisational strategy has always been something that organisations strive to achieve (Webb *et al*., 2016; Kauspadiene *et al*., 2017). Consequently, changes in internal and external pressure have forced organisations to turn their attention from silo operational and managerial risk controls (i.e. risks dealt at department level) to strategic approaches (i.e. enterprise-wide risk oversight) to maximise the achievement of the organisation's mission, strategy and objectives (Soomro, Shah and Ahmed, 2016; Maynard *et al*., 2018; Selamat and Ibrahim, 2018). Besides, migration to the cyberspace of businesses has made changes in terms of risk exposure. Also, in addition to enterprise risks, cybersecurity risk is an additional risk to any organisational risk portfolio. Due to the velocity of cyber risk and dynamic, recent years have raised concerns regarding how organisations should defend themselves when deploying commercial online activities and/or online operations. The Internet created an unprecedented way of doing business yet regardless of business opportunities gained, the cyberspace environment also allows exposure to a threatening landscape (Cavusoglu *et al*., 2015; Craig, 2018). Therefore, several authors believe that even though security has evolved, its maximum efficiency is yet to be attained (Webb *et al*., 2016; Kauspadiene *et al*., 2017).

Hence developments of the Internet have led to the creation of a 'cyber [space] ecosystem', where multiple elements interact (Ernst and Young, 2016) such perspective delimitates the types of perimeters (settings). In this regards, previous studies have indicated that the Internet has captivated users and organisations since its early beginnings due to its remarkable capabilities to interconnect and carry out a significant number of tasks. Seen as the invention of the Twentieth Century, the Internet succeeds to expand globally. As a result, information technology (IT) has emerged, becoming a significant area of interest for various sectors. Consequently, the extended capabilities of the cyberspace *world* in terms of connecting, integrating, and communicating have also created cyber-dependency (COSO, 2015). Despite economic growth, innovation, and creation of opportunities, it appears that cyberspace also has a *darker* side. Regardless of vast research in securing the digital footprint of organisations in cyberspace, the highly publicised security breaches and cases of organisational failures have reaffirmed that challenges of cybersecurity exposure remain a severe problem and one that deserves thoughtful consideration (de Bruijn and Janssen, 2017). Since security breaches are becoming more prevalent, it is likely assumed that cyberspace appears to be transformed into a prospective domain for cybercriminals (Craig, 2018). Therefore, a solution is required to safeguard organisations when deploying

activities/operations online. Even though considerable research has been carried out regarding risk exposure for organisations, past incidents confirm that more research is required to respond appropriately to increased sophistication and occurrence of threats.

Despite vast research, rethinking organisations' strategic risk resiliency has been limited because organisations tend to mirror past siloed approaches of IT security, Information Security, or siloed risk management. Consequently, some organisations' lack of preparation regarding risk exposure has revealed the need for more integrated strategies for managing and controlling risks (Jorion, 2009; Yaraghi and Langhe, 2011; Calandro, 2015). Despite vast research in securing organisations, highly publicised security breaches (corporate scandals) and ERM organisational failures post-Global Financial Crisis (GFC) of 2008 have reaffirmed that challenges in risk exposure continue to be serious problems that deserve consideration (de Bruijn and Janssen, 2017; Bohnert *et al*., 2019; Rubino, 2018; Oliveira *et al.* (2018).

1.3 Research problem

Recent years have shown that financial organisations are more and more concerned about finding a catalyst for risk foresight due to higher exposure to risks, hyper-competition, increased demand for compliance and governance, thus exerting higher pressure to create holistic risk governance. Intrinsically desirable, it points towards a transition to re-evaluating business models, reiterating changing organisational behaviours towards threats, vulnerabilities, and risks, adapting business strategies and optimising risk governance and resiliency capabilities; hence, the stakes and risk-return for critical national infrastructures such as financial organisations are considerably higher and broader in scope.

Attaining enterprise-wide risk governance is a complex issue requiring the alignment of multiple risk functions and the ramification of an organisation. The problem is that the relational mechanism that manages risks and aligns with the business is missing or is partially applied/decentralised, and thus the risk is managed reactively, randomly, and most often it omits to correlate all functions, technology, infrastructures, mechanisms, processes, culture and people. Even though risk governance efficiency has been improved in recent years, in many financial organisations' cases, the benefits derived from Cybersecurity Management (CsM) and Enterprise Risk Management (ERM) are not fully gained, which represents a mismanagement of risk, siloed approach, duplication of risk management outlay, misuse of resources, duplication of efforts, time, and/or inefficient capital allocation.

In response to this concern, alignment has become an organisational imperative for unlocking enterprise-wide risk management, value, risk resiliency, effectiveness, compliance, sustainability, risk foresight, shared responsibility and competitive advantage (Coltman *et al*., 2015; Bohnert *et al*., 2019). The problem statement (inability to achieve holistic management of risks across an organisation) prescribes the adoption of an integrative risk function that has the capability to proactively drive a unified risk oversight able to deal with the increasing multi-dimensional spectrum of risks, sophistication and velocity (Amin, 2019; Mayer *et al*., 2019; Li *et al*., 2019). Meaning that without alignment, risk governance for both CsM and ERM is mostly useless; risks remain unaligned and siloed across an organisation hence, previous approaches facilitated the management of risk up to a certain level.

Accordingly, this research responds to the need for harmonised risk handling, reporting, analysis, mitigation, respectively, resiliency across a whole organisation. Thus, it proposes a 'common mechanism' that is driven by the tenets of alignment (strategic interconnectivity, communication and partnership). It shall ensure maximisation in achieving organisational strategy, vision, and mission as well as helping to reduce/prevent the deficiencies of siloed controls, strengthening an organisation's security posture and building enterprise-wide risk resiliency and foresight of risks; i.e. meaning that it recommends an approach to increase the effectiveness of an organisation to foresee, adapt and plan against unexpected risks and equally identify signs, reduce the potential impact, recover and seek opportunities with future-oriented strategies (Iden, Methlie and Cristsinsen, 2016; Amin, 2019). Thus, alignment shall orchestrate the disjointed risk protection layers through lenses of various dimensions: strategic, structural, social, cultural and operational.

Much progress has been made in managing risk, however, intervention to date only moderated the siloed and reactive practice of managing risks and draws fundamental criticism. In the same vein, previous literature indicated limitations, such as examining only two traditional elements for alignment (e.g. IT security with business strategy; IS with business strategy; RM with business strategy; ERM with IS strategy). Whilst holistic risk governance has roots in two traditional approaches, namely IT Governance and/or traditional view of IT integration (Ramalingam, Arun and Anbazhagan, 2018; Mandani and Ramirez, 2019), and Risk Management (Viscelli, Hermanson and Beasley, 2017; Farrell and Gallagher, 2019; Silva, da Silva and Chan, 2019), the current research recommends the convergence of two types of modern approaches to managing risk: CsM and ERM, with

strategic alignment (third element) and organisational strategy (fourth element). By concentrating ERM capabilities to strengthen CsM capabilities, this research explored whether the realignment of risk control and risk oversight support the establishment of centralised enterprise-wide risk governance capable of addressing ever-increasing challenges (Viscelli, Hermanson and Beasley, 2017).

In conclusion, this research contributes by shedding a contemporary light on the current state of the literature and practice while suggesting an update to the body of knowledge on all three domains: CsM, ERM and alignment. It presents evidence on research gap implementation and highlights the positive effects of an integrated risk governance framework drawing attention towards the value of a paradigm shift in organisational risk governance driven by alignment (heavily grounded on contingency and institutional theory). Therefore, this research presents convincing arguments and contributes to the understanding of why a strategic alignment of CsM and ERM can sustain a financial business in the long term. Besides, it helps to identify key issues that impede the alignment process and thus extends the current literature domain that seems insufficient.

1.4 Rationale of the research

As previously mentioned, in a global and digital economy cyber risks have become a central issue for many stakeholders and shareholders. Evidence suggests that cyber risks in the online environment are among the most important factors considered by academics, practitioners and regulators. Given that security has a pivotal role in online activities, cybersecurity risks are perhaps the most important factors considered by organisations (Calder and Watkins, 2012; Nazareth and Choi, 2014; Chartered Institute of Internal Auditors, 2018). Literature recognising the importance of CsM in every organisation is growing. On the other hand, considerable research has been carried out with regard to Risk Management (RM), and in particular, its relationship with IT functions. Despite open conversation about the advantages and risks regarding the use of cyberspace, Hopkin (2014; 2018) states that cyber threats are merely a part of life, even without our consent. Furthermore, enterprise governance structures such as RM are responsible for guiding organisations in dealing with risks and responding to uncertainties. While RM is methodical and manages a broad range of risks that can affect organisations, the present research is focused on cyberspace threats that may influence or constrain the aims and outcomes of an organisation. Although traditional IT management has subscribed to the belief that it is

responsible for the technical part, there is evidence that supports a more innovative approach: respectively CsM.

It is noticeable that the interest in organisational risk resiliency has registered significant considerations, but there are still unanswered questions as to why organisations are unsuccessful in implementing effective security at all levels. For this reason, this research investigates possible methods for facilitating a more enhanced strategic approach to respond to the extended exposure to enterprise-wide risks and cyber risks altogether; to move towards an approach of *secure by design,* in context of strategy, to establish an enterprise-wide risk governance with anticipation (proactive). In short, the Researcher advocates that the two types of organisational risks cannot be carried out in isolation. Correspondingly, the Researcher advocates realignment of risk control and risk oversight (directing) under CsM and ERM alignment, to establish enterprise-wide risk governance. Such an approach would yield harmonised risk reporting, analysis, mitigation, and resiliency. Henceforth the alignment (interconnectivity and partnership) can place the entire organisation in a more enhanced state of security through a unified perspective of control, accountability, and decision making (Atoum, Otoom and Abu Ali, 2014, 2017). While much attention has been centered on separate disciplines of ERM, CSM and Alignment together can further sustain organisational risk strategy as it conveys all capabilities in an integrative manner.

The key aspect of this argument is that organisations' ability to maintain trajectory towards their vision, mission, and successful operation, it prescribes the adoption of an integrative risk function. ERM has been recognised as an integrative mechanism that drives a unified risk oversight approach that aids understanding of how organisations deal with a multi-dimensional spectrum of risks. ERM has a long history stemming from its capability to align various organisational functions in a multi-strategy approach that provides a holistic view of risks relating to precautionary maps displaying interrelated effects. (Majdalawieh and Gammack, 2017). It is also commonly known that successful ERM is driven by the alignment of risk oversight with strategic planning, respectively organisational strategy (Althonayan, Keith, and Misiura, 2011; Viscelli *et al*., 2017). While adoption of risk oversight is made to lower risks and help to exploit opportunities, practice shows that a universal approach is not available or feasible for organisations (Agarwal and Ansell, 2016). Risks continually evolve, and the consequences of these changes have increased organisations' interest in shifting from a traditional silo perspective that comes with

conventional RM towards a holistic approach of ERM in order to deal with risk in a more all-encompassing way (Althonayan, Keith and Misiura; 2011; Mensah and Gottwald, 2016).

Of more concern is that there are many examples of ERM's failure (e.g. Goldman Sachs, Bear Stearns, JP Morgan, Credit Suisse, Union Bank of Switzerland, UBS), and thus the Researcher considers that the problem is not entirely solved. Furthermore, the existence of the best practices does not necessarily promise to eradicate current problems faced by ERM completely. Research has shown that implementation and, more specifically, abiding to ERM framework alignment have proven a hard task for boards (Reynolds and Yetton, 2015; Wu, Straub and Liang, 2015). One of the main obstacles appears to be the strategic approach because nowadays some organisations see risk accountability as something unique to each department of their organisation. This leads to weaknesses in organisational defence (due to the silo approach) and may cause serious issues (e.g. duplication, lack of transparency of organisational risk profile, misalignment, immature risk control function, and lack of holistic RM). Given the variety of risks, silo security is a risk for organisations, and thus alignment of CsM with ERM governance, (e.g. strategies, planning, structure, processes, skills, competencies, and culture alignment) must be acknowledged and embedded at all levels as a strategic risk governance baseline. By achieving alignment, an organisation is less vulnerable to external changes or internal inefficiency because the alignment creates a standard and centric/unified solution (Bergeron, Raymond and Rivard, 2004).

On the other hand, the cost of cyber incidents has increased losses for the global economy even though it is hard to quantify the overall cost (COSO, 2015). There can thus only be possible biases involved (i.e., the source of information, specific interest if security vendor; specific interest for organisations to retain information internally), and thus the scale, costs, and complexity of incidents for organisations seems difficult to calculate. The precise effect of cyber incidents and costs is a much-debated topic, and it often prevails that year-by-year the cost has increased significantly (Maynard *et al*., 2018; McAfee, 2013; Websense Security Labs, 2015; McAfee, 2018; Verizon, 2018). As financial institutions are the earliest adopters of ERM, there has been increasing concern that the failures experienced by the financial industry in the course of the financial crisis have been due to a false sense of security (Thakor, 2015). As a response to various factors faced by organisations (i.e. GFC of 2008, corporate scandals, new business environment requirements, new regulatory requirements, and higher expectations from collaborators and insurers), the last two decades have shown

changes in business risk behaviour and in strategy risk formulation (both CsM and ERM) (Lyons, 2015; Rubino, 2018). However, previous research has failed to address such issues, and a gap has persisted; a gap that this current research aims to fulfil. Accordingly, a new governance framework, which aligns CsM with ERM, is proposed in order to optimise benefits, address new challenges, and link together individual risks of traditional silos. Among advantages such as the alignment of two risk control functions with overall strategy and a prompt response holistically understood and governed, it builds risk maturity preparedness and thus a strong reputation worthy of achieving (Taylor, 2014). This research proposes to utilise previous literature focused on aligning IT management to business strategy in order to exploit lessons learnt when organisations failed. Thus, for achieving an understanding of the current state, this research proposes to leverage a more complex study by analysing the impact of CsM alignment with ERM from a broader perspective. Overall, this research proposes to merge strategies of CsM and ERM and align the finished product with organisational strategy in order to employ all forces in one single scope so as to protect the organisation and to offer comprehensive capabilities to achieve its goal. Since the previous studies failed to incorporate principles of CsM and ERM, their alignment with a wider strategy will create a single path.

Therefore, this research proposes to generate a framework able to support the alignment of strategies and practices through an integrated approach in order to yield enhanced preparedness in forthcoming risk events. By concentrating ERM capabilities and CsM capabilities in the same scope and not separating them as done in the past (i.e. technical silo, silo security at departmental levels), the alignment will increase the potential of achieving strategic objectives and strategic planning, optimised processes, balanced alignment of risk appetite with exposure, tolerance, communications, and risk prioritisation, to name but a few aspects; all of which will enhance an organisation's overalls security. In reaching the above, this research puts forth aims, objectives, and research questions.

1.5 Research aims, objectives, and questions

To address the research problem, this research is driven by aims, objectives, and questions. While the research aims to evidence the main goal (*general*), scope and intent of research, defining limitations, on the other hand the research objectives are more *specific* in explaining the processes of how the aims shall be achieved (Thomas and Hodges, 2010; Stokes and Wall, 2014; Saunders and Lewis, 2018). Lastly, the research questions facilitate, point by

point, what exactly is addressed, thus ensuring that the research is consistent with the research aims. Therefore, research questions are most often seen as a continuation of research objectives (Stokes and Wall, 2014). To employ the aforementioned, the sections below delineate statements of the research's main goal, direction, and limitations.

1.5.1 Research aims

1) To investigate the alignment of CsM with ERM within the financial industry.
2) To develop a framework that assists CsM with ERM alignment within the financial industry, supported by practical guidance for the implementation of the proposed framework.

1.5.2 Research objectives

1) To identify, analyse and critically evaluate academic, industry-based and regulatory literature regarding CsM, ERM and their alignment and explore the current state of the topic.
2) To analyse the financial industry's environment and current practices regarding alignment.
3) To review and evaluate the effectiveness of current CsM and ERM frameworks.
4) To evaluate the potential and limitations of CsM with ERM alignment within the financial industry, supported by practical guidance.

1.5.3 Research questions

The main purpose of the questions is to secure as follows the emphasis of aims and objectives throughout the content of the research:

1) Why does a strategic alignment of CsM and ERM sustain a financial business in the long-term?
2) What are the key issues that impede the alignment process in the financial industry regarding CsM and ERM?
3) How are theory, practice, and regulation direction applied regarding the current alignment of CsM and ERM within the financial industry?
4) What effects have the implementation of the new framework*?*

1.6 Research relevance and contribution

This research is relevant for academics and practitioners when dealing with risk strategically and holistically. This research has two main contributions: a theoretical one and a practical one. A first contribution is the **theoretical contribution,** and it contributes

to literature by providing an understanding of a three-dimensional view of academics, industry (both organisations' approaches and industry standards), and regulatory requirements. Prior research focusing on how to protect organisations varies and focuses on certain types of risks. Even though prior literature has strengthened the approach and lead to better understanding, what is needed is to respond to risks because prior research has proven pervasive and fragmented (Imenda, 2014; McShane, 2018; Althonayan and Andronache, 2018). Moreover, it has failed in addressing the demand for performing holistic risk governance (e.g. regulatory pressure, stakeholders' pressure, and market pressure). Despite initiatives to establish good security practices, the underlying remark is that in practice organisations still fail to establish strategic alignment across their organisation despite considerable investments. Therefore, this research contributes theoretically by validating and articulating literature legacy, available practitioners' guidance, and effects of regulatory implication.

There is significant literature to support good practices. However, in most cases it only partially addresses views and is thus incomplete (limited). Such limitation renders it necessary to leverage additional solutions. Following the gap identification, the distinctiveness of present research lies in the fact that it aims to research in-depth in order to analyse and explore how the association of CsM and ERM, in the context of strategic alignment, can collectively align risk control and oversight and result in enhanced risk governance. A key aspect of this contribution is that it validates the progress/maturity of each paradigm. Thus, it outlines how each element can complement the other when striving towards a common goal, extracting the value of each and understanding potential inhibitors. It brings together three elements (CsM, ERM and alignment) to ensure maximisation of achieving organisational strategy. It thus establishes that capabilities of ERM, CsM and Alignment a must be integrative if to sustain organisational strategically.

On a practical note, it presents risk governance maturity, and in turn, determines flaws and justifies the value of the holistic approach. In addition to proving guidance for adopting a new direction in dealing with risk, this research shall contribute to the understanding of real-world practice. This research articulates the gaps in each paradigm (ERM, CsM, and strategic alignment) and proposes an approach to overcome drawbacks, but a **second contribution** of this research is made through the development of an inclusive conceptual framework. Another relevant point is that the research maps principles of strategic alignment and also gives consideration to operational, structural, and cultural alignment.

This research demonstrates that priority of security decision is still driven from a silo perspective, resulting in a mismanagement of risks (unaligned). In contrast, this research provides evidence that a common governance infrastructure can create a 'common mechanism' that would prioritise risks, support initiatives, unify planning, and prioritise investments as a security enabler based on current organisational needs; consequently the alignment proposal shall support identification of overall necessity on a multi-layered security basis that orchestrates alignment of risk governance, strategies, objectives, appetite, planning, structure, processes, capabilities, competencies, and risk culture for the purpose of serving organisational mission and vision in a unified manner; along with the preservation of resiliency that advocates the idea of rejecting the 'organisational dissociation'. In other words, the framework embodies a representation of how strategic organisational statement (strategy) is to achieve its main mission. Therefore, through the implementation of the *Framework*, an organisation can lessen over-investment efforts to adapt to internal and external changes (Miles *et al.,* 1978), overlapping of functions, and much more.

The *Framework* proposes to support organisations' risk governance procedures by emphasising strategic responsibility, leadership, accountability, and governance with the intention to seize opportunities, make risk-informed decisions, and contribute to the achievement of the resilience against enterprise risks and cyber risks.

1.7 Research design summary

Referring to Bryman's view, which reasoned that a "research design provides a framework for collection and analyses of data" (Bryman 2012, p. 46), the Researcher concludes that the original purpose of a research design lies in the fact that it proposes to outline a structure that guides the development and execution of the entire research. Moreover, a research design reiterates and outlines the researcher's priorities when answering the specific research problem. The structure of current research incorporates techniques of collecting data (research methods) and instruments (interviews) that help in the exploration of the phenomenon. This research adopted an interpretivist philosophy in order to provide a practical and theoretical perspective of the phenomenology through an inductive approach. The methods for conducting the research represent the tools proposed for identifying, defining, interpreting, and analysing the problem under examination (Bazeley, 2013). In undertaking the research, the exploration and analysis of primary and secondary data is made through an interpretive research paradigm. Likewise, the research methodology and methods

selected are subjected to the research aims, objectives, and research questions. In addition, the research field (financial industry) was another determinant yet simultaneously a delimitation of research boundaries. Furthermore, in determining the research methodology, the theoretical inheritage of previous contributors has been taken into consideration, and thus, previous questions unaddressed in the past have now been acknowledged. Thus, the Researcher adapted and reformed her questions to current business context (Bryman and Bell, 2015). Demonstrating this, the research questions represent the map for literature review, which is a determining factor for the selection and analysis of the literature. Additionally, research questions are the driver for the Discussion Chapter. Moreover, the methodological approach of this research is defined by a cross-sectional time horizon because it seeks to explore how this phenomenon occurred in the past and its effects. To support the investigation, the research design indicates how the research method and analysis shall be applied (Bryman and Bell, 2011). As a result, to investigate the above mentioned, qualitative data analysis is used.

1.7.1 Secondary data from the literature

The first stage of the investigation starts with a literature review, serving as a basis for the following chapters. The research intends to adopt a practical approach, the exploration of secondary data begins with an electronic database search based on keywords suggested by internet search engines and/or hard copies of research from the university library. Based on these techniques and field notes, a preliminary literature evaluation is formed. Through field notes, the researcher registers descriptions to support further the exploration of the research problem investigated, and additional meanings are extracted on these grounds (Zikmund *et al.*, 2013). The triage of prior research is nominated from three dimensions: academic literature, practitioner literature, and regulatory literature, with inclusion and exclusion criteria defined by Chapter One.

1.7.2 Collecting primary data from interviews

With the intention of also incurring knowledge from applied knowledge, the interview method is addressed to senior executives from different financial organisations. At this stage, interviews are elaborated based on preliminary results of literature review and systematic literature review. The realisation of this approach was based on three motivations. Firstly, an efficient interaction with the industry respondents; secondly a collection of primary data that points out the current trends providing a means of comparison with previous data results;

and thirdly, a possible identification of the *missing piece* that completes the whole picture of the research gap through a qualitative and accountable perspective.

In this regard, the interview type selected is semi-standardised because the Researcher wishes to take the opportunity to gain insightful information (tacit knowledge); as opposed to structured interviews where possible answers might be predisposed by the Researcher due to the open-ended nature of the questions. Although interviews are time-consuming, the format gains detailed feedback through questioning experts. Both face-to-face and telephonic interviews were considered as potential alternatives as the Researcher's intention was to address inquiries to professionals from various geographical area. Using telephonic communication for interviews made the research unconditioned geographically and gained a larger sample of respondents (Flick, 2014). The data is analysed and compared with NVivo software (a digital tool, especially for the analysis of qualitative data). Having chosen this methodology, it can be concluded that the research is based on a mono method.

1.8 Research Outline

This research compounds eight chapters. Summaries of each chapter are outlined below.

Chapter 1: Introduction

This chapter provides a snapshot of the overall structure of this research. This serves as a starting point to present the background, context, current status, and understanding of the research problem. Thus, this chapter is to indicate the setting and direction of the research in conjunction to prior contributions within the field. It states the rationale, scope, and limitations of the topic, presenting the challenges encountered by financial organisations in implementing risk control and risk oversight practices. The chapter represents a synthesis that highlights the gap and necessity of alignment between CsM and ERM to deploy holistic risk governance. In this stage, the aims, objectives and questions define the structure planning of this research. Also, the content of the chapter proposes to determine if the alignment has a sustainable strategic prospect. While the investigation initially focuses on general aspects, it aims to articulate the current state of the research problem, to withstand an understanding of the correlation and position of research with the prior research, and articulate the research gap to justify the significance of research problem solution and framework.

Chapter 2: Literature Review

This chapter examines a variety of resources and perspectives (ERM, CsM, alignment) focusing on the financial industry in particular. It presents key aspects of theories and leading practices in a concise format, separating the chapter into three-dimensional perspectives. First view, the academics' literature comprises reviewal of scholars' literature which represents an initial frame. Second view, the practitioners' literature adds a practical understanding of the need to elucidate inadvertencies, pointing out the current state of CsM strategy without the effect of ERM strategic alignment. Third view, the regulators' literature examines the rules for organisations in the financial industry based on requirements, guidelines, or stringent regulations. Based on these three initial steps, the literature examination is synthesised in a multi-dimensional literature taxonomy, gaining a retrospective view of theory and practices to currently identify information what generates holistic risk governance that supports organisations overall strategy. Providing a snapshot view of the current and past approaches (contributions), the researcher uses this derivate as a basis for demonstrating the research gap and to justify the rationale of the research framework. In short, the content of the chapter proposes to determine if alignment has a sustainable strategic prospect in both dimensions.

Chapter 3: Systematic Literature Evaluation

Overall, this third chapter represents a second phase of the literature examination, to systematically evaluate and organise the literature. This chapter proposes to move beyond the descriptive exploration of the phenomenon and explore further possible answers to the questions raised in this research. Key contributors, main approaches, key factors, key benefits, and the key problems are explored at this stage of the research. In this context, it clarifies the role of academics, practitioners, and regulators on how it influences the governance of risks. This chapter represents the second conceptual constructor (after literature review) for the conceptual framework that follows in Chapter 4. Thus, this chapter explores why alignment is necessary, how it is sustained, what the key debates within all three domains are, and, lastly, how theory, practice, and regulatory frameworks interrelate. Therefore, apart from addressing the objectives of this research, this chapter aims to identify the current maturity state of the research problem, analysing practices and evaluating limitations, all of which have the scope to validate the research gap and sustain the validity of the proposed research framework. In short, this chapter provides an overview of ERM,

CsM, and alignment literature contribution based on a systematic literature review in order to illustrate how literature has progressed in terms of this research problem.

Chapter 4: Development of Strategic Alignment Framework of CsM with ERM

While the previous chapter is guided by the fulfilment of questions and objectives, this chapter is governed by attaining the second aim:

> '*To develop a framework that assists CsM with ERM alignment within the financial industry, supported by practical guidance for the implementation of the proposed framework.'*

This chapter derives from the initial findings of the literature review in Chapter Two (first derivate/contribution) and the systematic literature evaluation extracted from Chapter Three (second derivate), which fostered the identification of the research gap (third derivate). Based on these derivates, the structure of the chapter further contributes to compounding the *CsM-ERM Strategic Alignment Framework*, and thus this chapter contains an additional two derivations: supporting theories (fourth derivate) and supporting frameworks and gaps (fifth derivate). On these settings, this chapter compounds all five derivations (as constituents' part) with the purpose of justifying and endorsing the *CsM-ERM Strategic Alignment Framework.*

Chapter 5: Research Design

The format of the research methodology chapter justifies the structure of this research in terms of how the research objectives are addressed, and it explains how they correlate to the research questions (Bryman and Bell, 2007; Bryman, 2012; Saunders and Lewis, 2018). Consequently, this chapter states and justifies how the research is carried out and why, as well as outlining the design and tools selected to undertake the analysis. Thus, this chapter introduces justification for steps taken in the development and execution of the entire research. As a starting point, it contains a theoretical discussion regarding what a research methodology represents and how it consequently sets the researcher's priorities when identifying the research answers (Saunders, Lewis and Thornhill, 2015). Given the purpose of the research, data collection is gathered from primary and secondary sources. Since the collection of a theoretical background requires investigation of both past and current approaches in organisations, the use of secondary data is an appropriate preliminary method. The second step that follows is the collection of primary data based on semi-structured

interviews. Considering retrospective data and analysis of practical approaches, it seeks to clarify how the objectives of this research are accomplished.

Chapter 6: Collection and Analysis of Primary Data

This chapter focuses on the collection, organisation and analysis of data gathered from interviews with respondents involved in CsM, ERM, or both. To collect and analyse data, the research methodology presented in the previous chapter is used. Specifically, for this chapter, the research methodology guidance has the purpose of driving the research objectives and determining the extent of fulfilment. As a result, this chapter introduces the account of research findings from interviews aiming to contextualise the validity of *CsM-ERM Strategic Alignment Framework*. In seeking to investigate the effectiveness and sustainability of CsM and ERM alignment in the context of the financial industry, this chapter employs qualitative content analysis of research findings.

Chapter 7: Discussion

While the results of Chapter Six are assessed against the research objectives, this chapter's goal is to address the research questions and explore how academic, industry, and regulators' views revolve in aggregating answers. Therefore, implications of research findings identified in Chapter Six (content analysis) are further analysed with an additional technique of thematic analysis and are then compared against literature. By employing a thematic technique, the focus of discussion moves from 'description' to 'interpretation' of research findings (Vaismoradi *et al*., 2013). This relies on a qualitative analysis that seeks to understand the phenomenon's antecedents, determinants, barriers, readiness (maturity), and capacity so as to sustain risk governance as a core competency for sustainability and efficiency as well as to avoid ripple effects (internally and externally on other industries) (Verizon, 2018). Specifically, this chapter uses the rigour of thematic analysis to explore if CsM and ERM alignment (interconnectivity and partnership) can place an entire organisation in a more enhanced state of security through a unified approach to risk control, accountability, and strategic decision-making. In this phase, the research framework takes final shape, incorporating the legacy of ERM, CsM and Alignment theory, approaches, gap, management theories, and gap practices.

Chapter 8: Conclusions and Recommendations

This chapter forms a synthesis of findings to provide evidence of how the aims, objectives, and questions of this research are fulfilled. Linking each chapter's contribution, this final chapter concludes the implication of findings in order to validate the framework for the alignment of CsM with ERM in the financial industry. Therefore, conclusions and recommendations are based on all seven chapters of the research to demonstrate well-supported investigation throughout all chapters, contribution, strengths, and limitations.

To visualise the above stated, Figure 1-1 synthesise the structure of this research on various stances.

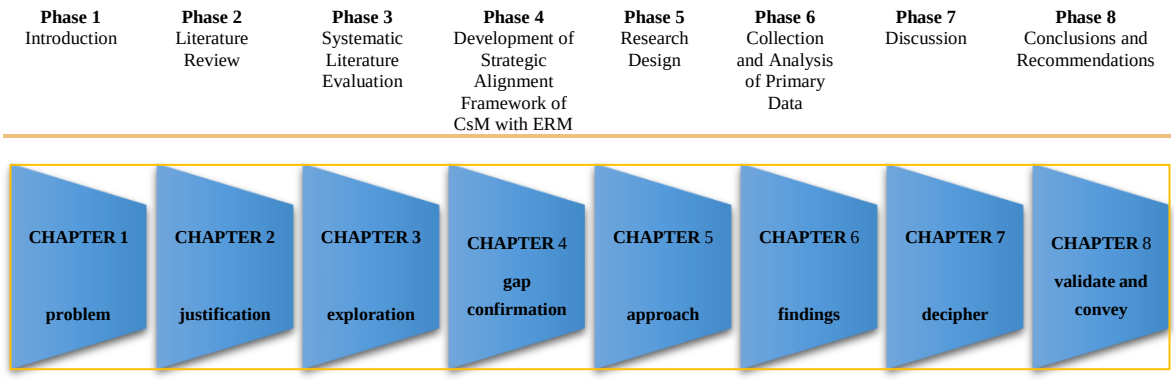


Figure 1-1 Developmental research phases

Source: The Researcher

As can be observed in Figure 1-1, the *first phase* of the research begins with Chapter One, where an overview of the research is presented from an exploratory stance. In *phase two*, Chapter Two presents the literature review, investigating and analysing prior contribution of scholars, practitioners, and regulators in order to explain and comprehend the current state of knowledge through different perspectives. Continuing, *phase three* continues to explore the research problem and identifies and explains the limitations of prior research. Based on this phase, further exploration takes place (*phase 4*) in order to identify and confirm gaps in applied approaches. Stemming from identified theoretical legacy, further steps of planning data collection are considered for a more in-depth analysis of primary data. Therefore, the methodology (*phase five*) organises and demonstrates how the research is been undertaken. In *phase six*, empirical results are provided. *Phase 7* interprets and substantiates the findings of Phase 6. Following on from this, *phase 8* encompasses all phases of the research and

reiterates the implication of the proposed *Framework*. It concludes by validating the contributions and limitations of the research.

The chapter that follows reviews literature related to the research problem and does so through a three-dimensional perspective of academics, practitioners, and regulators.

2. Chapter Two: Literature Review

2.1 Introduction

As traditional businesses have evolved, society's reliance on IT has increased significantly. Organisations are framing their structures and behaviours to prevent risks resulting from the cyber environment. In the past, Risk Management (RM) could counteract threats from the physical environment. Nowadays, the diversity of activities has led organisations to adopt the more comprehensive approach of ERM. Therefore, the first component of this literature chapter focuses on the evolution from RM to ERM. A second essential element is the alignment between CsM and ERM. As previous literature examining the issue is scant, this chapter focuses on the emerging problem of CsM alignment in organisations by focusing on its strategic nature and whether the alignment has a sustainable strategic prospect in both dimensions.

While the investigation initially focuses on general aspects, it later moves from general to specific exploration of the financial industry. As the financial industry is under explicit regulation, the efficiency of the proposed alignment can be determined. This chapter examines a variety of resources and perspectives focusing on the financial industry in particular, drawing on academic peer-reviewed journals and practitioners and regulatory perspectives to explore different facets, insights of research, typologies and evolution. This allows identification of the current state of research, an understanding of the position of the current research and recognition of the research gap. Such an approach is particularly useful to complement literature and add a three-dimensional perspective, and thus assure a more complete and informed research contribution. This approach has also been adopted to overcome the arguments such as theory often omitting some aspects of the field of reality. Such a three-dimensional perspective aims to ensure the validity of correlations in a real context.

2.2 Risk landscape

Academics' viewpoint: The concept of risk is familiar for most researchers as it encompasses a variety of research areas. However, the etymology of the word seems to be unknown, even though the term was initially identified in medieval documents. Some findings suggest that the spread of the term was due to the printing press development (Luhman, 1991). Other authors believe that the term is of Arabic origin, demonstrating that risk concerns have always existed (Klüppelberg, Straub and Welpe, 2014). From analysing

pre-modern societies, there is a clear illustration that risk was experienced in different forms since uncertainties have exposed humankind from early beginning to natural changes, disasters, premature deaths, epidemics, wars, violent politics and many other unexpected events. Although in the past the meanings of risk were apprehended, a multi-faceted focus on risk response appeared late in modern society and through a multidisciplinary approach (Klüppelberg, Straub and Welpe, 2014).

Additionally, whilst its origin is unknown and unclear, the word "risk" appears to have remained fragmented in different connotations. For instance, in Arabic, the word "risq" describes a favourable outcome depending on the actions required. However, in Latin, the word "riscum" represents a challenge. Furthermore, in French, the word "risqué" also means a challenge but usually, one that leads to a negative result and almost never with a positive outcome. In English, the word "risqué" also exists; however, it is used in the context of society and should not be used interchangeably with the English word "risk" as it has an entirely different meaning. The word "risk" is closely related to danger, yet unlike its French counterpart, the outcome is not necessarily expected to be negative; it could be either. In the recent years, the word "risk" has been applied in the context of business' assets (Merna and Thani, 2008). Accordingly, Hopkin (2014) considers that risk in an organisation's environment is something that could hinder the fulfilment of objectives. Nonetheless, Merna and Thani (2008) simply define risk as the likelihood (probability) of something negative or positive occurring at a given time. Furthermore, authors such as Aitchison and Guerin (2014) consider that nowadays the risk semantic has gradually moved from an adventure concept to a more specialised interpretation of RM. Klüppelberg, Straub and Welpe (2014) define *risk paradigm shift* as being determined by a move from traditional to modern society, and thus it is believed that the term's etymological roots have been forgotten. While organisations are exposed to a broad array of emerging risks such as the global financial crisis, extreme weather, terrorism, or cyber threats, based on this exposure, organisations seek to mitigate and manage risks and embrace possible opportunities that appear in organisational processes. Authors such as Web *et al.* (2014a) offer a modern perspective of risk. They consider that innovation conveyed by the development of the Internet, mobile computing, big data, cloud computing technologies and/or the Internet of Things (IoT) have all driven the trend towards the acknowledgement of risk as an opportunity providing it includes adequate oversight. Accordingly, Web *et al.*'s research reflects upon RM approaches for increasing the capability of identifying, prioritising, and controlling an

organisation's vulnerabilities and risks (Web *et al.*, 2014a). Following the same trend, Miller (1992) provides a more strategic description of risk encountered by organisations, as it refers risk as a variation in an organisation's outcome. Thus, the shift from pure risk (traditional view) to opportunity risk (current view) is later viewed by Rosenberg and Schuermann (2006) as an adverse deviation. Moreover, risk perception and evolution from risk adversity to risk opportunity have registered a need for quantification and categorisation. Therefore, authors such as Burnaby and Hass (2009) categorise risks based on their potential as minor, damaging or catastrophic.

Practitioners' viewpoint: In the business context, risk is seen as a vital force for yielding success due to its financial, operational or strategic implications (PwC, 2012). Likewise, Lloyd (2010) is of the opinion that in a global economy, organisations have to adapt and prepare for risk implications on an ongoing basis. Another simplistic viewpoint regarding risk is briefly described by the British Standards Institution (BSI) in BS ISO/IEC 27005:2011 (BSI, 2011a) as a deviating effect on objectives that reveal the downside and opportunistic aspects in a business environment (BSI, 2011a; BSI, 2018). To portray the risk issue, some organisations have categorised and addressed them by type as hazard risks, financial risks, operational risks or strategic risks, and consider that these kinds of risks should be the principal consideration of organisations (Casualty Actuarial Society, 2003; PwC, 2012). Given the implication of risk for organisations and global economy, there is a need to adapt and prepare for risk implications on an ongoing basis. Thus, risk categorisation represents an initial examination of additional steps that should be taken to mitigate, transfer, or avoid or risk (NIST, 2014). This means that organisations can choose to handle risk directly; for example, to identify a means to manage, reduce, avoid it (preventive) or transfer it to a third-party and share responsibility (e.g. insurance, suppliers). Which option would depend on the organisation's strategic, operational, financial, ethical and/or technical capability.

Regulators' viewpoint: Although risks may be defined from different perspectives, historically the value of meaning differs within periods and issuers. Likewise, Her Majesty's Treasury (HM Treasury, 2004) defines business risk from a general and modern point of view, where risk truly represents an uncertainty of outcome that could turn into a convenience or a real danger: "risk is defined as this uncertainty of outcome, whether positive opportunity or negative threat, of actions and events" HM Treasury, 2004, p. 9). Hence, the balance represents the likelihood of the event to come about, through an upward

or downward course. Similarly, the Committee of Sponsoring Organisation (COSO, 2004) and HM Treasury (2004) take into consideration the advent of both effects; a fact still omitted by some. The fact that the term 'risk' has numerous definitions confirms that over time, the meanings of the word have shifted and accordingly several perspectives have been adopted. However, all focus on the result of an action, positive or negative.

Additionally, definitions agree that risk resides in two or more components; the action and what the action entails offsetting the expected result of that action. In other words, there are two aspects to consider - action and the probable consequence.

2.3 Risk Management development

Academics' viewpoint: Organisations encounter risks every day on a variety of levels (Servaes, Tamayo and Tufano, 2009; COSO, 2012) but their ability to manage them dictates the consequence the risk has on business activity. As the business environment is uncertain and volatile, the enhancement of RM carries many challenges and benefits (such as the reduction of organisational overinvestment, an increase in the organisation's debt capacity, good internal communication, and cost) (Castro *et al*., 2008).

Literature has emphasised the appearance of the concept of RM in the early 1950s (Crockford 1982; Dionne, 2013) due to several factors. Firstly, insurance policies became expensive and partially liable. Secondly, changes in the economic environment and market competition led to the introduction of in-house risk procedures (self-insurance) as an alternative precautionary approach to risk mitigation. Lastly, organisational risk culture, triggered additional strategic changes, (Verbano and Venturini, 2011; Schroeder, 2014). Although the interest in applying the RM approach was mostly a business trend during 1950s-1960s (Crockford, 1982), there was a lack of theoretical and practical literature. Crockford revealed that in 1956, some academics informed that during that period, theoretical background and expertise in the field were missing (a lack of textbooks, a lack of academic courses and a lack of trained specialists) and consequently some decisions were taken instinctively. Following this, RM academic articles settled the basics of the theoretical background that aggregated changes in business approaches. In the course of the 1960s, various risk self-protection approaches were adopted and applied across organisations. However, it must not be forgotten that for many years the pure RM approach focused mainly on the insurance market (Dionne, 2013). Formerly, RM was concerned with risk perspective purely as a negative output (loss, harm, accidents, or consequences). To summarise, in the

past, the basic concept of risk failed to take into consideration the opportunities which arose from risk exposure. Likewise, Crockford (1982) explains that for an extended period of time, risk was limited to a single perspective. By this approach, RM had focused on negative risk (pure risk) and did not address the opportunities arising from a risk-taking approach.

Additionally, in 1965 the Insurance Institute of America recognised and developed additional expertise by investing in professional education (Crockford, 1982), a fact that encouraged extension and development of RM. By 1970s, the concept of RM was modernised by the expansion of financial risk management (FRM) due to its innovative approach to risk and opportunities. Continuing the trend, in the 1980s international regulation appeared and many organisations shifted to the new, modern form of RM (Dionne, 2013). Furthermore, the insurance market crisis that followed in the 1980s (Verbano and Venturini, 2011) reinforced the initial 1960s movement towards RM applicability and internal risk frameworks. Moreover, in this phase, the shift was encouraged significantly by risk guidelines, regulation and the new business standards that stimulated the innovative perspective of upside risk (e.g. Turnbul Report, 1992). However, despite the significant changes in RM approaches, organisations continued to rely on insurance services but as a secondary protection practice (Hillson, 2002). Clearly, the move from risk philosophy to a strategic one was the result of the learning that success is not based on luck, but on RM approaches (Clarke and Varma, 1999). In the ensuing years, the principles of the new, modern approach of RM extended globally and subsequently determined the release of new guidelines, regulations, and standards specifically optimised to meet regional prerequisites (Arena, Arnaboldi and Azzone, 2010).

In the early 1990s, RM activity emerged as a policy whose main responsibility was to determine the risk value of investments in business lines (Tilman, 2001). During this period, Schmit and Roth (1990) defined the basic concept of RM as a performant activity able to minimise losses through the accountability of risk and cost.

In the late 1990s, RM started to be viewed as a business discipline (Schmit and Roth, 1990), while a few years later, the empirical evidence of Stulz (1996) criticised the inappropriate practices of RM due to its imperfect correlation between theory and applicability. In conclusion, available evidence seems to suggest that regrettably RM at its beginning was adopted as a risk silo-based concept (risk treated in isolation), a fact that increased cost and resources implied (Servaes, Tamayo and Tufano, 2009).

By 2000, the focus of most studies shifted to the concept of integrated RM that proposed to align organisational strategy, processes, people, technology, and knowledge (Verbano and Venturini, 2011). In recent years, there has been increasing interest in RM, something that has led to the development of the various paths such as strategic risk management, financial risk management, enterprise risk management, insurance risk management, project risk management, engineering risk management, supply chain management, disaster risk management, clinical risk management and product development management, among others. The literature of RM is essential for a broad range of fields, as it represents their roots. The paths mentioned above differentiate themselves through risk considerations, techniques and methodologies applied to the specific discipline (Verbano and Venturini, 2011; Wu, Chen and Olson, 2014). Clearly, RM development has implied different determinants and stages depending on the era; a fact that has led to changes in RM applicability in organisations. Therefore, the launch of the Sarbanes-Oxley Act (SOX) in 2002 was another challenge that facilitated additional improvements in RM.

RM has its roots in multiple disciplines such as economics, finance, management, marketing, sociology, and as a result, the disciplines have become fragmented (Clarke and Varma, 1999). As risk is part of organisations' everyday activity, the approach to risk shifted to effective-taking strategies that imply the development of internal business philosophies, as is the case of ERM (Wu, Chen and Olson, 2014). Aven and Aven (2015) describe RM as a need to explore opportunities and to avoid losses, accidents and disasters through methods such as identification, assessment, evaluation, control and treatment. According to the authors, the main challenge faced by RM is to establish a balance between organisational appetite for seizing opportunities and risk. Additionally, Clarke and Varma (1999) outline that poor RM can destabilise an organisation in many ways or even destroy it. However, an opposite approach might enhance a positive management of risk.

As a result, the consensus view registered over recent years defines RM as a strategy of identification, assessment and prioritisation of risks (Coyle, 2014; Calandro, 2015). By reframing strategy in an organisational context, it relies on an intention to use its vision and core values for its mission - objective attainment (COSO, 2016). Accordingly, RM should include a business continuity process incorporated into an incident response plan (Kouns and Minoli, 2010). Nag, Hambrick and Chen (2007) suggest that strategic risk management continues to be fragmented, hence multiple perspectives have been adopted. As a result, its

definition in the field has varied and been re-conceptualised over the time. Apparently, the clear evidence of global financial failures of 2007-2008 shows that losses can hit even experienced organisations, which have RM strategies fully implemented (e.g. Goldman Sachs, Bear Stearns, JP Morgan, Credit Suisse, Union Bank of Switzerland, and UBS, to name but a few).

In consideration of the above, some contributing factors to global financial failures might be a lack of common language, a lack of common practices, a lack of preparation, a lack of stress tests, a lack of correlation between theory and practice, unethical practices, overconfidence in the system and/or inappropriate implementation of risk oversight or governance (Jorion, 2009). However, in recent years, there have been many assumptions claiming that the financial crisis was an unpredictable event (Servaes, Tamayo and Tufano, 2009). Others believe that many organisations failed to have a strategic RM in place and for this reason were unprepared (Calandro, 2015). In addition, in conjunction to these reasons, market expansion, RM silo approach practices, the lack of a commonly accepted standard and guidance in implementing the RM have all contributed to organisational failures (Clune and Hermanson, 2005; Yaraghi and Langhe, 2011).

Building on from this idea of past failures, RM has extended to become more integrated, respectively ERM. The year 2000 saw the starting point where the need for an integrated strategy changed RM practices again (Viscelli, Hermanson, and Beasley, 2017). Results from earlier studies demonstrate a consistent and robust association between integration and the rigorous method of implementation of RM across organisations (Beasley, Clune and Hermanson, 2005). Thus, working collaboratively with other departments/units assures transparency of processes (as opposed to a traditional RM silo approach), where actions are undertaken by individual departments/units, one by one (subjective prioritisation of risks) and with possible links not being shared and communicated (Grace *et al*., 2015; Viscelli, Hermanson, and Beasley, 2017).

Practitioners' viewpoint: In addition to theoretical views, the practitioners' view on RM is that RM has been determined by global expansion because globalisation determines business expansion and partnerships around the world, leveraging economic growth and technological innovation along with the creation of a common marketplace, which has also rendered fierce competition (Aon, 2015; Deloitte, 2015; PwC, 2015). For this reason, it is believed that a key driving force for yielding and maintaining success is a strategic RM

approach (Aon, 2015; McKinsey and Company, 2016) whereby a lack of RM or partial practices might determine incapacity to innovate and recover after a crisis, financial loss, disruption of business operation, reputation damage, property damage, and many more. The strength of such an approach was determined over time by external and internal factors (e.g. economic volatility, customers', suppliers', vendors' or investor's pressure) and also by substantial losses (Aon, 2015).

The focus of past research shows that along with market challenges, regulations of RM affecting the practices and gradual changes were made based on regulatory requirements (Deloitte, 2015a). Over recent years, the increased regulatory requirements have placed pressure on organisation governance, risk appetite, stress test, operational risk, technology risk, culture risk, and much more. However, the study of Deloitte (2015b) reveals that organisations often struggle to comply with multiple regulatory authorities dispersed globally (in the case of the financial industry, compliance to Financial Stability Oversight Council, Bank of England (BoE), Prudential Regulation Authority (PRA), Financial Conduct Authority (FCA)). The modern organisation adopts RM as it fosters analytical capabilities and develops an ethical business culture along with good practices regarding risk appetite (Deloitte, 2015a). As a result, RM had been reformed, elaborated and scrutinised during these times but, in general, lines RM proposes to 'direct and control' risks (identify, analyse, reduce, eliminate if possible and/or transfer risk (Aon, 2015; BSI, 2018). Nonetheless, the industry literature emphasises that the traditional approach of siloed risks of RM is insufficient and an 'extension' is a forwarding step (RIMS, 2014).

RM through the perspective of regulators seems to be embedded within reactive approaches (AICPA, 2017). Consequently, RM failures have recently registered large organisations demonstrating that risk-taking is deficient and decisions are made post-event. Accordingly, such events have facilitated and readjusted the mandatory organisational strategy with regards risk (Organization for Economic Co-operation and Development (OECD), 2014). Regulators propose to highlight the exponential aspects of risk and determine appropriate governance for a suitable preparation (safeguards) rather than reaction based on due diligence (minimum countermeasure). One example is the Basel Committee on Banking and Supervision (2015), which sees RM as a process that guarantees the identification, measurement, limitation, control, mitigation, and report of risks. For instance, Basel III regulation of the Basel Committee on Banking and Supervision requires an enterprise-wide

RM. Therefore, through the implementation of RM, an organisation quantifies its risks and creates appropriate adjustments to examine risks through mitigation, transfer, avoidance, or acceptance (NIST, 2014). Whilst RM practices provide a useful approach, further studies present arguments in terms of a paradigm extension and its opportunistic use under the enterprise risk management (ERM) umbrella.

2.4 Enterprise Risk Management (ERM)

Academics' viewpoint: Given the increase in the number of organisational failures, previous studies have reported that managing risks has become essential for organisations (Dabari, Kwaji and Ghazali, 2017; Cohen, Krishnamoorthy and Wright, 2017). Additionally, uncertainties in the business environment, competition within industries, political risks, regulatory changes, and stakeholders' expectations articulated the necessity for strengthening a cross-functional risk function (Cohen, Krishnamoorthy and Wright, 2017; Shad, 2018). Accordingly, RM upgraded to a more holistic approach (respectively, ERM) as a new, modern way to manage risks strategically (Calder and Watkins, 2012; Andrén and Lundqvist 2017). Above all, ERM has the capability to take advantage of upside risk (opportunities) and the resiliently to cope with downside risk (Agarwal and Ansell, 2016). In general, this demonstrates that the traditional approach of RM seems outdated as it used to focusing mainly on risk minimisation as well as minimising the validity of return on investment (Stoll, 2015; Andrén and Lundqvist, 2017; Bogodistov and Wohlgemuth, 2017). The management of risks in silos (divided into finance, marketing, human resources, IT, distribution systems, audit, and global supply chains) seems an inappropriate and inefficient method to adopt. Prior research evidenced that traditional RM fragmented organisations into departments that were used to dealing directly with all ranges of risks (Hardy and Runnels, 2014; Cohen, Krishnamoorthy and Wright, 2017). Consequently, risks were considered unique, with each in isolation to the other. This led to a lack of departmental communication that in turn, resulted in reduced identification of organisational risk exposures; in other words, a siloed approach. Over time, this matter evolved significantly, leading to a more integrated need to address issues of risks more holistically across an organisation. Overall, the paradigm shift towards ERM supports a change from tactical to strategic emphasis (Dabari, Kwaji and Ghazali, 2017). Moreover, it provides organisational effectiveness and preserves shareholder value on a continuous basis (Dabari, Kwaji and Ghazali, 2017; Majdalawieh and Gammack, 2017).

On a practical side, the first sign of change started to transform partly due to the launch of the COSO report in 1992 and was subsequently enhanced over the years by other guidances and frameworks (Rubino and Vitolla, 2014). Literature emphasises the importance of the transitions of RM to ERM through numerous investigations that have considered the effects of a *paradigm shift* (Beasley, Clune and Hermanson, 2005; Gordon, Loeb and Tseng, 2009; Eckles, Hoyt and Miller, 2014; Arena, Arnaboldi and Azzone, 2010; Farrel and Gallagher, 2019). Thus, the previous research investigated ERM through many perspectives: accounting, financial, marketing and management; facts that broadened ERM literature. Other authors questioned the literature of ERM implementation based on analysis of organisations that appoint a Chief Risk Officer (CRO), considered to be a first external sign that an organisation adopts a holistic approach to risks (Lienberg and Hoyt, 2003; Beasley, Pagach and Warr, 2008; Pagach and War, 2011). Furthermore, McShane, Nair, and Rustambekov (2011) described ERM as a coordinated process that manages the portfolio of risks addressed to different departments.

Furthermore, regarding its applicability, Nair *et al.* (2014) perceive ERM as a dynamic capability for organisations since its ability to foresee, avoid, respond, and manage risks promises a much faster recovery (should a crisis emerge) compared to organisations that choose a silo approach. Lin, Wen and Yu (2012) refer to ERM as a fundamental shift of risk practice that adapts and determines a complete picture of the risk portfolio.

Moreover, the allocation of resources, cost-saving, and operational efficiency are just a few more determinants that encourage organisations to change their approaches in managing risks. In support of this view, there are indicators that the benefits represented another important factor that encouraged the shift to ERM (Lin, Wen and Yu, 2012).

The early adopters of ERM, for example, Australia and New Zealand Banking Group Limited (ANZ), Goldman Sachs and Barclays, are positive examples that reconfirm its applicability among industries. However, most likely negative examples such as the American International Group (AIG) demonstrate and reflect that ERM implementation does not adequately assure complete organisational success (Lin, Wen, and Yu, 2012). Nonetheless, determinants such as industry-specific standards, internal control, organisational culture, board implications, and regulators or shareholders influence the further adoption of ERM (Kleffner, Lee and McGannon, 2003). Additionally, there was an open dialogue during and after the global financial crisis of 2007-2008. On this basis, the

failures of organisations revealed the inefficiencies of RM and led to the direct implication of the government, regulators, and practitioners in the promulgation of ERM as a long-term investment (Nair and Rustambekov, 2011; Cohen, Krishnamoorthy and Wright, 2017; McShane; McShane, 2018). As a result, ERM adoption was triggered by multilateral pressure on regulators, standard setters, executive boards, rating agencies, competitors, and auditing organisations that in turn encouraged a more effective management of risks in order to cope with the volatile market and become more resilient (Lundqvist, 2015; Cohen, Krishnamoorthy and Wright, 2017; Bogodistov and Wohlgemuth, 2017; Bohnert *et al.*, 2019). Another consensus among researchers is that RM also changed due to SOX 2002. In support of SOX, Arnold *et al.* (2011) later argued that organisations that had implemented ERM before SOX's release occurred low levels of impediments from applying the new requirements. For instance, one of the first adopters of ERM was the financial industry (McShane, Nair and Rustambekov, 2011). The financial industry's specific regulations posed a higher pressure and encouraged the early adoption of risk management safe practices compared to other industries (Mikes, 2009).

Henceforth, regulatory and industry scrutiny (i.e. rating agencies as Standard and Poor, Moody's, Fitch) provided a similar trend for other industries (non-financial) to implement ERM (Lundqvist, 2014). Rating agencies have proposed to sustain the regulatory compliance since their primary role is to evaluate the quality of ERM through a credit rating analysis that assesses whether the RM culture, risks controls, or strategic management are at acceptable levels (Bohnert *et al.*, 2017). In addition, Schiller and Prpich (2013) reconfirm that ERM has strong roots in finance and the insurance sector. Correspondingly, the benefits registered have been transferred to other business sectors and governments.

Beyond its benefits and wide applicability to other sectors, such variations determine a fragmented and uncorrelated ERM literature and practice over the years (McShane, 2018). Academic literature evidence suggests that the first paper that used ERM terminology was by Dickinson (2001), a fact outlined by Bromiley *et al.* (2015). As scholars and practitioners disagree on ERM's definition, COSO's definition appears to be largely used as a point of reference in academic investigation (Beasley, Clune and Hermanson; 2005; Arena, Arnaboldi and Azzone, 2010; Tekathen and Dechow, 2013; Hopkin, 2014; Taylor, 2014; Hayne and Free, 2014; Tricker, 2015). Since 2002, the attention paid to ERM has increased (Lundqvist, 2014) and multiple frameworks have been launched in order to guide, support,

and sustain its implementation. Although there are various sources of frameworks developing the consistency of ERM, the Researcher of this paper has identified a lack of consensus regarding its implementation. Some authors, such as Hayne and Free (2014), suggest that the COSO framework bears the most substantial influence on business practice. Although the findings of Paape and Spekle (2012) sustain that COSO framework is just an initial approach in dealing with risk in a holistic way (it provides a brief guidance and principle), the responsibility of developing and adapting the framework remains an ongoing task for organisations.

Further research in this area demonstrates that despite onerous regulations and barriers, organisations have also registered positive effects post-implementation (increased shareholder value, improved risk-return, enhanced decision making, and a holistic approach to all risks) (Farrel and Gallagher, 2014, 2019; Dabari, Kwaji and Ghazali, 2017). Despite these benefits, organisations have had differing results since each organisation has its industry-specific culture, internal factors and ownership, and its performance is correlated with all factors and the ability to adapt a framework to its individual needs (Gordon, Loeb and Tseng, 2009; Paape and Spekle, 2012). Consequently, the study of Lundqvist (2014) outlines that organisations rely on more than one framework, suggesting that the use of a unique framework is an inappropriate approach.

Alternatively, overseeing organisational needs can lead to the creation and implementation of an internal framework based on organisation-specific requirements and practical issues (Kleffner, Lee and McGannon, 2003). Based on these determinants, ERM frameworks share common features, acknowledging that the implementation of the frameworks differs among organisations' practices due to unique particularities. In addition, that despite the fact that good practices are adopted, this does not mean that the best practices are generated. Taking into consideration that in theory, organisations know how to deal with risks (due to guidelines, frameworks, scholarly literature, and legislation) whereas the reality of the last decade confirms that this may not be a reality as issues are only partly resolved.

As a synthesis of the above, Table 2-1 below illustrates ERM determinants, implications, and barriers.

Table 2-1 ERM determinants and implications

Regulators' requirements	**Practitioners' requirements**	**Market pressure**	**Stakeholders and Shareholders**	**Insurers' requirements**
Sarbanes-Oxley Act; New York Stock Exchange; Toronto Stock Exchange; The Combined Code; Dodd-Frank Act; Basel III.	Rating agencies; Organisational audit; Trade associations; Third-party.	Past failures /mismanagement; Market development; Technological development; Economic downturn; Market competition.	Earning volatility; Board pressure.	Stringent expectations; Contractual requirements.
ERM advantages		**Disadvantages**	**Barriers**	
Strategic oriented; Sustain compliance; Optimised risk appetite; Determine a common language; Reduce costs by mitigating losses; Proactive strategy versus reactive strategy; Stability and continuity assurance (resiliency); Assure response and recovery adjustment; Assure holistic governance to risks; Gain competitive advantage/performance; Avoids duplications (resource allocation); Determine in-house expertise development; Reduce costs by reducing overlapping processes; Determine an increased ability for value protection; Increase firm value (rating credit); Increase the quality of decisions (by information); Consider threats and opportunities; Governance applied enterprise-wide; Increase accountability, transparency and agility; Creates value (optimised risk for shareholder return); Links strategy and organisational objectives;		Cost; Time length; Bureaucracy; Ongoing activity; Regulatory mandate; Needs to be tailored; Accountability of pitfalls; Supplementary resources; Residual risk (variations).	Pitfalls; Fund allocation; Integration variables; Unethical practices; Documentation deficiencies; Employees skills deficiencies; Unappropriated governance; Stress test unpreparedness; Dispersed compliance settings; Plethora of guidance's/practices; Silo approach /overlap of functions; Heightened regulatory expectations; Unclear policy and risk statements; Organisational cultural deficiencies; Uncorrelated theory with applicability; Inappropriate alignment/low maturity; Preparedness to overcome deficiencies; Uncoordinated efforts of staff involved; Overconfidence in systems and procedures; Inconsistent regulations (national specific vs. global).	

Source: The Researcher

As shown in Table 2-1, ERM practices have significant economic results and thus its application can be an introductory guide for organisations and could yield benefits such as defining risk setting and business response (Taylor, 2014). Unfortunately, it seems that it still needs development as it is considered immature by some (Paape and Spakle, 2012; Eckles, Hoyt and Miller, 2014; Grace *et al.*, 2015; Andrén and Lundqvist, 2017). The implementation might be seen by some authors as a "tick-box approach". Further evidence of Unger (2015) claims that literature has developed findings which suggest that taking measures to protect assets is not an option for organisations. Therefore, the present organisational strategies are proving to be susceptible to vulnerabilities and barriers. Thus, the Researcher believes that planning risk control and oversight through the governance of ERM would ensure minimisation of potential loss. whilst aligning 'governance, integration, and strategy' (Andrén and Lundqvist, 2017).

Returning to the applicability of the research problem, the financial industry is a complex mechanism that most often encompasses multiple structures, labelled by Oldfield and Santomero (1997) and Simeon (2012) as:

- depository institutions (e.g. retail banks, commercial banks, private banks, savings banks, postal saving banks, building societies, community banks, credit unions);
- insurance and pension fund institutions (e.g. insurance organisations, pension fund management organisations);
- brokers and investments institutions (e.g. asset management, investments banks, corporate finance, mutual funds, hedge funds, mortgage brokers, clearinghouses, finance organisations, investment organisations) and more (Oldfield and Santomero, 1997; Simeon, 2012).

Although the industry involves a diversity of players, it is indisputable that they all encounter similar risks. The risk associated is underpinned with the organisation's size, main activity, and time established. While risk is specific, the financial industry is exposed to additional risks such as systematic risk, credit risk, counterparty risk, operational risk and legal risk (Oldfield and Santomero, 1997). The financial industry is a major component of the global economy and plays a vital role in sustaining society (Lenssen, Dentchev and Roger, 2014).

For this reason, organisational responsibility in this sector is strictly regulated due to its sustainable role. For example, in the USA, it is mandatory for financial and governmental organisations to adhere to ERM practices (Whitman, 2015). A fact, that reminds the official implication and acknowledgement of ERM as a baseline to ensure deployment of deterrent practices. Thus, past failures (e.g. Lehman Brothers bankruptcy of 2008, Countrywide Mortgage of 2008) reiterate the strong need for prudence and holistic RM. They also raise an intriguing question as to why organisations still fail to employ good risk practices.

As a matter of fact, banks were one of the first sectors to adopt ERM (based on global regulations of Basel). There is an ongoing discussion among some critics that suggests ERM efficacy had a low capacity during the global financial crisis of 2008-2009 (Hopkin, 2014; Bromiley *et al.*, 2015). Some argue that it might be due to possible ill-implementation of ERM, aggressive risk-taking, lack of knowledge, and unfair business practice. The Researcher argues that ERM was not ill-implemented because evidence suggests how ethical

organisational responsibility towards good ERM practices is particularly influential; particularly in terms of following known practices.

Such failures are considered sensitive for global economy (Alcaraz and Zeadally, 2015) due to the interdependent nature of the financial industry. Critical infrastructures (e.g. water, food and agriculture, transportation systems, chemical industry, nuclear industry, energy industry, information technology, financial systems, and many others are at the heart of today's economy and a problem one could trigger a "cascading effect" due to their interrelated and inter-dependent functions (Kauspadiene *et al*., 2017). Henceforth, a potential financial catastrophe might affect customers' or an entire country's financial system since society and business activity depend on monetary flow on a global scale. The post-reality of the financial crisis 2007-2008 exposed key faults in business practice that reiterated changing organisational behaviours towards threats, vulnerabilities, and risks (Crouhy, Galai and Mark, 2014; Oliveira *et al*., 2018). Cases such as HBO bank or British Northern Rock bank were among a few examples of over-exposure to risks (Tricker, 2015) and thus organisations should move towards a new approach, rethinking, and safeguarding their stratagems in regard to unanticipated and unknown risks in order to ensure the protection of tangible and intangible assets in a responsible way. In addressing the issue of security, organisations from the financial industry must take into consideration new ways to meet consumer demands in addition to the new trends in the banking sector such as Internet banking or mobile banking which increases new fraud patterns (Schiavone, Garg and Summers, 2014).

Practitioners' viewpoint: When referring to practitioners' views, two types of literature categories are included: (1) advisory entities, which include reports, white papers and guidance for industry vendors, and (2) industry recognised entities (non-profit), which promote good practices through specific frameworks and standards.

It can be observed that a shift of approach is occurring when studying research problem. There is a change from a micro approach (i.e. existent in the silo approach) to a macro approach, whereby risks are considered from a wider perspective (i.e. collective versus individual strategy) of strategic, operational, and financial hazards (Casualty Actuarial Society, 2003; Institute of Management Accountants (IMA), 2011). ERM is predominantly seen as a discipline (Accenture, 2013; Risk Management Society (RIMS), 2015; Thomson Reuters, 2015), as a programme (Tower Watson, 2014, PwC, 2015; McKinsey and Company, 2016), as a process (KPMG, 2009; EY, 2016) and also as an approach (Deloitte,

2009; EY, 2015), yet within all views, it is seen with the purpose of sustaining the common achievement of organisational objectives. As an example, Casualty Actuarial Society (2003) define ERM as "…the discipline by which an organisation in any industries assesses, controls, exploits, finances, and monitors risks from all sources for the purpose of increasing the organisations' short and long-term value [benefits] to its stakeholders" Casualty Actuarial Society, 2003, p.6) The approach outlined by Casualty Actuarial Society is based on ERM intentions to create value and to mitigate risks, but there seems to be no compelling reason to argue that organisations understood the potential of ERM.

Additionally, in a more simplistic manner, ERM presumably should be able to anticipate an event, likelihood of risks, and assure minimal disruption or loss in accordance to proposed organisational objectives, risk appetite, and risk tolerance (KPMG, 2009; EY, 2016). In addition, ERM shall improve the prospects of success for organisations hence they stand more prepared, informed, and resilient in dealing with the occurrence of risk and its impact (RIMS, 2011; RIMS, 2014). As a result of strategic internal control, risks are aggregated and reported holistically in order to support business decisions (KPMG, 2009; KPMG, 2017a).

Thus, in contrast to RM, ERM proposes a unified management that acts holistically (i.e. it grasps the concept that risks are inter-related) without overlapping or duplicating a risk control function of another managerial department (compartmentalised) (RIMS, 2015) and with the aim to create better value, sustainability (COSO, 2016), and value protection (Grant Thornton, 2006) and measurement. Moreover, ERM seeks to anticipate possible events before they occur and in turn prevent or at the very least minimise their effects through a plethora of strategic alternatives to counteract the exposure to risks (COSO, 2016). As ERM is seen by practitioners in various perspectives, for the purpose of this research, the 'approach' terminology seems to complement and align itself with the terminology used by academic contributors.

Apart from classification variations, there are many prescribed behaviours for organisations and implementation recommendations for ERM, but the evidence indicates that organisations struggle to cope with such variations (Casualty Actuarial Society, 2003; Ponemon Institute, 2011). The most compelling evidence of ERM frameworks is the COSO, Risk Management Society Standard, the Institute of Risk Management Standard (IRM Standard), the International Organization for Standardization (ISO standard), Control Objectives for Information and Related Technology (COBIT), British Standard, Joint Australia/New Zealand 4360:2004 Standard (AS/NZS, 2004), the Turnbull Guidance, the

Casualty Actuarial Society Framework, among others. Per total, the promulgation and utilisation of ERM good practices and baselines (COSO, 2016) is at the basis of all these frameworks and standards of risk oversight.

In addition to the industry-recognised entities' viewpoint, advisory organisations sustain that the best approach to tackle risk is to adopt a strategic, holistic, and proactive approach (McKinsey and Company, 2013a; McKinsey and Company, 2016). However, there might be subjective interest due to the incentives involved. Whatever type of support it is, it is clear that organisations need to adopt and sustain ERM practices in order to demonstrate to parties (e.g. regulators, customers, collaborators, and shareholders) that risk detection, mitigation, and prevention are of primary concern for the organisation and as such the organisation is duly prepared.

The study of PwC (2013) supports the same line and accordingly confirms that previously ERM capabilities were developed and tested across multiple industries and seemed to have a low maturity in their implementation. The foregoing discussion implies that inhibitors and emerging risk challenges to ERM can be lessened if organisations accelerate their capabilities from reactive to proactive risk practices in order to assure appropriate measures that safeguard organisations from potential risk in advance (PwC, 2009, RIMS, 2014). The landscape of risk is more profound in the financial industry because losses in this sector could have ripple effects on national or even international economics and politics (PwC, 2014; Verizon, 2018). Moreover, in the light of evidence from 2015, the third most affected sector appears to be the financial industry. The financial industry seems to be ahead of many industries due to its attractive characteristics as a high-reward area. Cases such as JP Morgan, Fidelity, HSBC, Bank of America, Citigroup, PNC Bank, US Corp, Well Fargo, and Citi Bank are just a few examples that highlight the threat's maturity (Verizon, 2015; Websense Security Labs, 2015).

In regards to Table 2-1 (above), Accenture (2009) explain that due to the increased organisational risks, an effective risk oversight implies a higher cost. Despite the fact that ERM reduces cost, its maintenance and applicability is affected by increased regulatory and market constraints. To summarise the main focus of practitioners, Table 2-2 below articulates the fragmented practices of the industry that varies between a top-down (strategy, objectives, appetite, leadership, value creation, strategic risk oversight and compliance) and bottom-up approach (infrastructure, processes and culture).

Table 2-2 Literature variations among consultancies organisations

Focus	Key considerations	Entity/year
Strategy	ERM is a strategic capability. ERM is still immature developed.	Grant Thornton (2013); McKinsey and Company (2013a); Tower Watson (2014).
Objectives	The objectives are aligned with risk appetite, tolerance and organisation strategy.	Thomson Reuters (2015)
Appetite	Risk appetite is aligned with organisational objectives and exposure. Risk appetite determines the strategic directions. Risk appetite represents the acceptable risk parameters. A risk appetite statement it considers organisation risk profile, capacity, tolerance and oversight. Risk appetite statement needs to be acknowledged by all.	Manigent (2009); Deloitte (2009); Manigent (2011); COSO, 2012; Protivity (2012); Deloitte (2014a).
Leadership	Embedding ERM relies on leadership, culture, risk appetite, risk strategy, communication and education. RM efficiency is strengthened by leadership and its alignment to business functions.	Tower Watson (2010); PwC (2015).
Value	ERM enhance and optimise organisations. ERM add value to an organisation. Return from RM is significant.	KPMG (2009); RIMS (2014); Accenture (2015); McKinsey and Company (2016).
Performance	RM main purpose should be performance attainment.	Accenture (2009)
Risk oversight	RM capabilities needs supported improvements	KPMG (2013b)
Compliance	Internal framework as compliance to regulatory demands. A heightened regulator demand has reshaped RM. The effectiveness of an organisation RM is intensively challenged.	Ponemon Institute (2011); Deloitte (2015); AON (2015).
Risk culture	ERM is effective based on an integrative approach.	Ernst and Young (2014)
Structure/Architecture	ERM implies a top-down and bottom-up approach.	McKinsey (2010)

Source: The Researcher

Table 2-2 above shows that practitioners' literature significantly emphasises the importance of the alignment of risk oversight to business strategy due to the fact that such practice assures organisational achievement of 'mission' and 'vision' (COSO, 2016). However, risk alignment, although identified in literature as being necessary, omits to specify how it should be accomplished. In other words, it is necessary, but through what mechanisms should it be applied (Tower Watson, 2014).

Although in academic literature ERM is defined as an 'approach', by many industry experts it is considered a 'programme' (KPMG, 2009; Accenture, 2009; KPMG, 2013a; Deloitte, 2015). Furthermore, as a programme, it is believed to determine value through its ability to provide stability due to its determination of informed business decisions and appropriate risk oversight aligned with risk appetite and thus assures a reduction in cost. Moreover, ERM helps to anticipate and mitigate risks together with an increased ability to overtake opportunities (informed decisions), therefore leading to an increased organisational performance (PwC, 2015).

Manigent (2009) highlights that at the basis of every strategy, risk appetite should be defined and aligned with organisational objectives and exposure. Accordingly, the organisation would expose itself to consequences proportionate to achieving its objectives (Manigent, 2009). Moreover, Deloitte (2009) argues that a risk appetite statement (documentation) is often used as a strategic direction since it provides a formal standpoint which articulates, clarifies and communicates the maximum acceptable 'parameters' regarding risks. Additionally, it offers provision for decisions due to the acknowledgement of risk actually existing, and it assures that risk remains within an acceptable limit (Protivity, 2012; Deloitte, 2014a). A risk appetite limit (parameters) should be in harmony specifically with risk profile (exposure) as well as risk universe (all risks), governance, RM, culture, and infrastructure (Manigent, 2011; Deloitte, 2014a). It should also ensure that as long as limits are acknowledged and maintained, the pursuit of value is ensured (Tower Watson, 2010). Unfortunately, few organisations develop an appetite framework and embed it across their internal environment (PwC, 2015); something that reinforces the actuality of the concept of mismanagement and lack of preparation regarding risk oversight.

Organisational culture is certainly a significant component of ERM (COSO, 2016) and in turn, the organisational strategy, mission, and vision involve interaction with a human component. Thus, the Researcher believes that human impact needs to be considered and promoted across organisational divisions to assure comprehension of organisation objectives. Therefore, considerations of the need for an improved risk oversight and management suggest that these actions should have a top-bottom approach, where executives deploy further imperatives. Moreover, its integrative approach should incorporate board oversight, organisational culture, risk appetite, risk ownership, risk transparency oversight, infrastructure, and operation in one main strategy (Grant Thornton, 2013, KPMG, 2013b; Ernst and Young, 2015). Thus, the ERM expected effectiveness depends on its ability to align its risk strategy with its objectives, appetite, risk tolerance (Thomson Reuters, 2015), and objectives/strategy communication across the organisation.

Regulators' viewpoint: Although the adoption of RM industry practices has various voluntary determinants (e.g. organisation's decisions, the use of sound practices of security, shareholders' pressure, to name but a few), there are also some imposed and mandatory aspects that empower the use of ERM. Given the sensitive dimensions of the financial industry, the regulator's viewpoint section refers to written and peremptory norms of

organisational practices. Since economic stability works in close relationship with the financial industry, correct management, in turn, influences other industries. For this reason, financial industry practices were strengthened by regulators (e.g. Financial Stability Board, 2010) to balance exposure and possible influence. As the financial industry is continuously exposed (due to its incentives, participants, and channels), ongoing compliance is prescriptive and mandatory. Through the process of identification and measurement of practices, the financial industry maintains its status (Basel Committee on Banking Supervision, 2015). The post-crisis regulatory reforms (e.g. Basel II, Basel II.5, and Basel III) illustrate implications of supervisory effectiveness and provide sound advice for the financial industry (Basel Committee on Banking Supervision, 2014).

In addition to its strategy, the financial industry encourages the development of an organisational culture that needs to constantly reinforce ethical and efficient risk appetite. Expanding rules pre-supposes the recommendation of best approach; i.e. that risk should be identified, monitored, and controlled continuously. Moreover, an organisation must comply with law and regulations but it must also adjust the external requirement to its internal policies (Basel Committee on Banking Supervision, 2015).

While the issues stated have a potential to be addressed globally, organisations are currently advised to comply with minimum standards of country-specific security regulations. Since early 2014, the Office of the Comptroller of Currency (a primary financial regulatory agency for national banks, USA) has been drawing attention to the fact that financial industries are registering weaknesses when adopting minimum standards of RM practices yet at the same time are compelled to "heightened expectation" (USA Department of Treasury, 2014). Examples such as Barclays Bank, Zurich Insurance, Global Payment, MasterCard, and Visa continue to prove that managing information systems is more complicated than ever. A clear illustration of the issue is also the case of JP Morgan and Chase, who were considered to have the highest RM culture in the banking sector. The events from 2014 proved that challenges are more complex than expected.

Moreover, financial failure has reiterated the need for strict rules such as those of SOX, the New York Stock Exchange (NYSE) and the Toronto Stock Exchange (TSE), all of which set new security parameters for publicly rated organisations. For instance, the Corporate Governance Guide of NYSE expects organisations to embed risk governance practices

across the whole organisation through mechanisms such as culture, communication, leadership, and RM (NYSE, 2014). Such an approach promotes awareness and acknowledgement of organisational risk exposure and fosters individual responsibility for mutual welfare. Therefore, compliance with rules and proactively taking steps to meet the security requirements of the competitive market is enforced via the pressure of governmental regulatory demands (e.g. SOX's Section 404, 2002, Gramm-Leach-Bliley, Fair Rating Reporting (FCRA)). For example, the Combined Code of the Committee on Corporate Governance (also known as Turnbull Guidance) reinforces the value of internal control in organisations to assure quality, compliance, and efficient operations (Financial Reporting Council, 2005). Its content emphasises the accountability and monitoring responsibility of management (typically, boards of directors) in order to assure, improve and promote good practices regarding risk.

Consequently, it can be seen that each Act focuses on something different. It can, therefore, be concluded that the actual points covered by an Act affect how risk control is dealt with. In other words, one Act cannot be followed without the other as they each cover different aspects and in turn, yield different results.

The Gramm-Leach-Bliley Act (GLBA) (1999) introduces baseline and safeguarding rules for the financial industry with regards to customer data protection as well as advancing risk documentation and staff training. On the other hand, the Sarbanes-Oxley Act (SOX) introduces the internal audit requirements and quality controls and adds ethics for organisations based on the initial Security Exchange Act of 1934 (SOX, 2002). From the outcome of disclosure of proper organisational governance, this Act enforces responsibilities and punishments for those that fail to comply. This Act can be considered as an originator of current practice among organisations.

Apart from focusing on the financial industry, Dodd-Frank Wall Street Reform and Consumer Protect Act of 2010 suggests that non-financial organisations should also be prudent about risk oversight in order to assure overall economic stability (Dodd-Frank Act, 2010). The prominent requirement of the Act is to identify accountability and any transparency of internal procedures. The general obligation for organisations entails official statements of financial results as well as risk oversight procedure and results so as to assure applicability of prudential measures. Likewise, the UK Corporate Governance Code of 2016 addresses similar lines and initiates formal planning for the long-term. Similar to the Dodd-

Frank Act's principles of accountability and transparency, the guide goes further and facilitates an understanding of current organisational challenges. Apart from initial principles, it promotes leadership for effectiveness, remuneration, and mutual understanding. Thus, this guide is based on the belief that to improve the risk oversight, maintenance and control, executive involvement is essential (Financial Reporting Council, 2016).

The middle-ground position, which states that the adoption of ERM is a sign of an organisation's compliance with the regulatory demand (Standard and Poor, 2008), is worthy of consideration. Adoption and implementation of ERM is a starting point that requires ongoing personalisation, optimised to a specific sector and the organisation's specific risk appetite, specific risk profile and specific business model. However, it should be noted that mandatory compliance for the industry can sometimes limit the business model; for example, implementation of privacy policies for customers based on the Gramm-Leach-Bliley Act or the Dodd-Frank Act.

2.5 Cyber exposure

2.5.1 Cyberspace

Although many studies have attempted to explain the terminology and the definition of the word 'cyberspace', over recent years the term has yielded limited consensus regarding its etymology and meanings. Consequently, the term is facing an undefined explanation of what exactly it semantically represents. It seems that over time, the terms have been associated or confused with 'virtual world', 'virtual environment', 'cyber environment', 'cyber domain', 'online world', 'online domain', 'online realm', 'cyber ecosystem', 'electronic space', 'digital world' or 'wired world', among others. Often, these terms have been used interchangeably and as equivalents to 'cyberspace'. However, they are not necessarily similar in all cases and can imply multiple meanings (Cicognani,1998; Min, Chai and Han, 2015). For example, 'virtual world' refers to the electronic environment, as a three-dimensional reality, where people can interact/experience (e.g. video games, interactive learning) with an artificial environment based on human-computer-interaction. It is similar to real-life experience, although intangible (Bainbridge, 2007; Gartner, 2016). Thus, 'cyberspace' is an impartial term to define and represents only some aspects of it.

Henceforth, Internet developments have led to the creation of ‘cyber ecosystem’ where multiple elements interact (EY, 2014). Such perspective outlines that the perimeters and the volume of interaction divide the term into two: cyber and space.

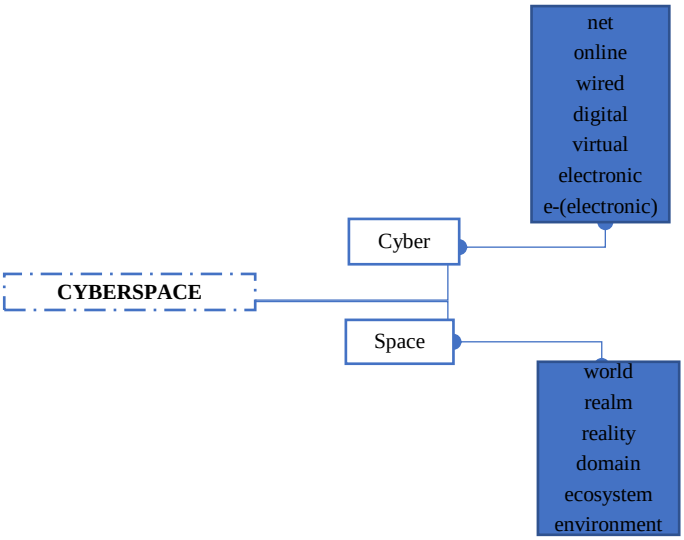


Figure 2-1 Ambiguity of cyberspace terminology

Source: The Researcher

While cyber terminology and its etymology are an open discussion, the evidence of definitions supplements a deeper understanding of variations and Figure 2-1 above illustrates some of its derivations, which are often used mistakenly in an interchangeable manner. On the whole, Figure 2-1 briefly summarises an etymology analysis that shows how the term has been emphasised within the literature under the form of an ‘etymological map’ (Hart, 2014). While ‘space’ can clearly be defined as a setting/place, the word ‘cyber’ describes the type of setting/place (namely that it is an online place). Consequently, the word ‘cyber’, incorporates the principles of cybernetics (i.e. human-computer-interaction), where interconnected computer systems embrace extensive technologies that are capable of facilitating, reshaping, and exchanging electronic information and communication by connecting to an “imaginary world” (Mindell, 2000; Mitra and Schwartz, 2006) and relying on “the principle [of] governing or directing a technology or system” (Mindell, 2000, p.3). In most cases, ‘cyber’ forms part of a compound word, as do the words ‘online’, ‘digital’, ‘virtual’ or ‘electronic’ and the word ‘space’ has equivalents: ‘world’, ‘realm’, ‘reality’, ‘domain’, ‘ecosystem’ and ‘environment’.

In short, ’cyber’ and ‘space’ refer to perimeters/boundaries and the type of technology involved, and this technology is handled on the whole (Henderson, 2009). In particular, ‘cyber’ refers to control/governing aspects (Gibson cited in Kurbalija, 2014) and articulates

interaction with the Internet, computers or even robots as machine learning (Henderson, 2009; Burgess, 2010; DeFranco, 2013). Consequently, it relies on feedback, control and communication (Mindell, 2000; Henderson, 2009).

Table 2-3 Alternative meanings of cybersecurity

Terminology	Definitions
cyber world	"… the cyber world is an amalgamation of the Internet, other physical networks, digital services and virtual reality: it is a multi-user virtual environment." (Lehto and Neittaanmäki, 2015, p. 7). "Cyber-world is the network of computers is simple definition." (Gavrilova, Tan, and Sourin, 2016, p. 25).
cyber space	"…is a global domain within the info environment whose distinctive and unique character is framed by use of electronics and electromagnetic spectrum to create, store, modify, exchange, and exploit via interdependent and interconnected networks using information communication technologies." (Tyagy, 2014, p. 11).
cyberspace	"…cyberspace can then be defined as the diverse experiences of space associated with computing and related technologies" (Strate, 1999, p. 383). "…cyberspace describes the human-made domain for action that exists as a consequence of an interconnected and interdependent global communications and computing infrastructure." (Deibert and Rohozinski, 2010, p. 16). "The Cyberspace is a complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form." (BSI, 2012, p. 4). "A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." (Committee on National Security Systems, 2010, p. 25). "Cyber space encompasses all forms of networked, digital activities; this includes the content of and actions conducted through digital networks." (UK Cabinet Office, 2009, p. 7). "Cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies." (Kuehl, 2009, p. 4). "A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." (USA Department of Defence, 2016, p. 69).
cyber ecosystem	"Cyber ecosystem: a complex community of interacting devices, networks, people and organisations, and the environment of processes and technologies supporting these interactions." (EY, 2014, p. 1). "Like natural ecosystems, the cyber ecosystem comprises a variety of diverse participants – private firms, non-profits, governments, individuals, processes, and cyber devices (computers, software, and communications technologies) – that interact for multiple purposes." (USA Department of Homeland Security, 2011, p. 2).

Source: The Researcher

Table 2-3 above emphasises some terms while also identifying commonalities. It must be noted that all definitions reiterate that cyberspace greatly relies on computers and technologies. It encompasses various spectrums of technology, devices and networks to

facilitate interaction among many stakeholders for various purposes. As the term ‘cyberspace’ corresponds to this research problem, the Researcher adopts this term throughout.

2.5.2 Cybersecurity challenges

Academics’ viewpoint: In the early period of the Internet, computer security was considered a particular technical risk. Due to the Internet’s lack of built-in security regarding information protection, most organisations had to develop their own strategy to counteract risks. In this trend, Singh *et al.* (2014) believe that despite numerous technical solutions, information security (IS) is complete when in combination with management directions. Nonetheless, over the years, this mentality has changed dramatically and shifted to a non-technical perspective where strategic solutions are considered (Maynard *et al*., 2018).

While the term is known under numerous appellations, a common definition of “cybersecurity” fails to be adopted. Nevertheless, the term is being employed more frequently, and thus this research adopts the same terminology. Additionally, authors such as Von Solms and Van Niekerk (2013) indicate that the shift of names represents, in fact, an evolution of change. Von Solms and Van Niekerk justify their claims through assessing the developments in the field. In the past, IS has referred to information protection, whereas nowadays cybersecurity operates beyond these limits and intends to protect humans and various assets. In short, it has become a more complex mechanism, implying multiple aspects of the cyber and traditional environment.

Whereas in the 1980s computer crimes were represented by viruses transmitted through floppy disks (Blyth, 2008), cybersecurity is currently perceived in a multifaceted perspective. For instance, Singer and Friedman (2014) have predicted a negative scenario of Internet-based attacks and their research suggests that mankind is inclined to *react* (to defend) rather than *act* and install vital preventative in advance (offensive). For example, measures taken *after* an unprecedented disastrous attack occur is a reactive approach, respectively a countermeasure post-event; whereas a proactive approach is a prior approximation of an event and thus an earlier preparation; it is a safeguard that aims to assure that organisational losses are capped to minimum levels.

Hence, cybercrime has not only had the opportunity to increase in sophistication and frequency but has indeed done so. One merely needs to look at cases

such as Stuxnet, Flame, Gaus, Sony Pictures or Saudi Arabian Oil, all indicating that cybercrime, industrial espionage, "black swan" (unpredictable events) and cyber sabotage are more prevalent in today's society.

To sum up, Figure 2-2 below briefly covers some generalised risks, threats and vulnerabilities in the form of criminal acts, basic motivation, and impact with the purpose to demonstrate that the intersection of them can be a potential risk for organisations. Ranging from business, financial, military, thrill or grudge attack (Stewart, Chapple and Gibson, 2015) there are many potential risks addressed in the direction of organisations.

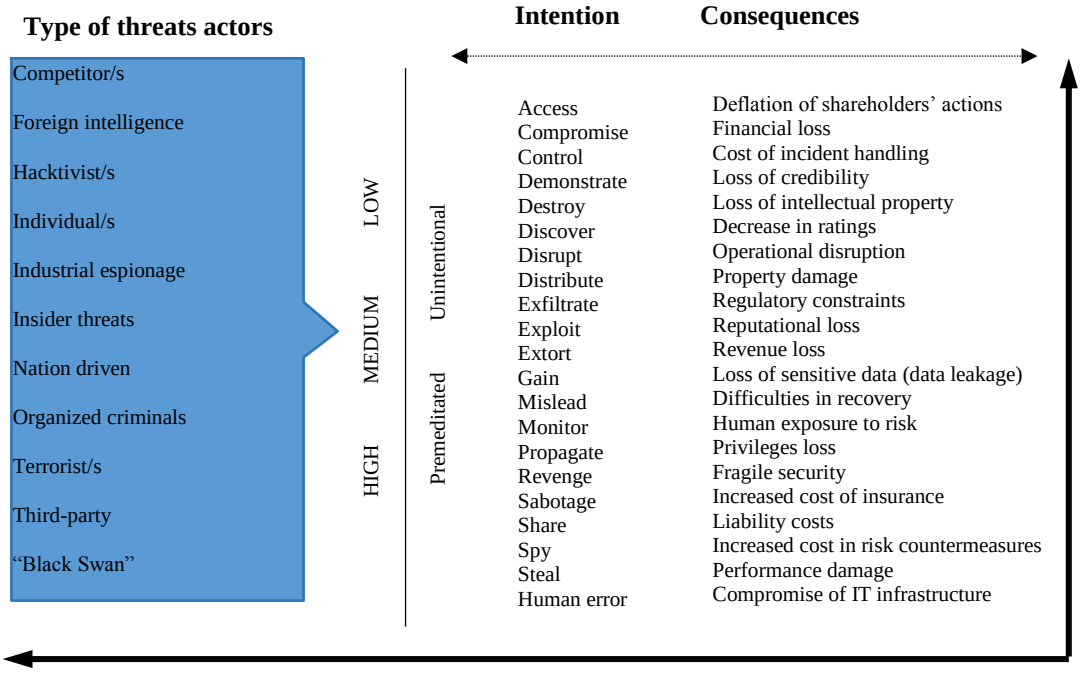


Figure 2-2 Cyber-criminal categorisations

Source: The Researcher

The bottom line of Figure 2-2 is the general pattern of threats actors, threatening acts, intentions, and consequences. Taken together, the synthesis of Figure 2-1 highlights the risk dimension for organisations and the importance of implementing safeguards instead of countermeasures (reactive) as post-event response which presumably might be overpriced; the latter being overvalued.

Practitioners' viewpoint: The literature of academics and practitioners abounds with examples of terminology used interchangeably. However, the fragmented state of terminology fluctuates between the domains of information security and cybersecurity (BS ISO/IEC 27032:2012). Thus, it fluctuates between synonymously and similar meanings but

with different objectives. Whether terms are synonymous is clarified by their scope, hence IS aims to protect confidentiality, integrity and authenticity of information (BS ISO 27032:2012, BSI, 2012) while the domain of cybersecurity considers protection of people, assets, process and technology.

As cybercrime represents an illegal digital activity/action with potential damage, financial loss, and/or operational disruptions, KPMG (2013a) suggests that the current reliance on the Internet for businesses, governments, and consumers will also continue to yield a negative return. Similarly, the McAfee report (2014) outlines that cybercrime has become an 'industry' since losses encountered in 2014 were around $400 billion. McAfee estimated in 2014 that losses would continue in this trend because prognoses about further business movements to the digital environment are expected. Cybercrime becoming a more sophisticated entity/force was reconfirmed in 2018 when the report showed an increased cost, reaching almost $600 billion (McAfee, 2018). The trend in cybercrimes varies from technical breaches in 2016 to social attacks in 2017 and 2018. What is clear is that there are losses that need to be considered and as much as possible reduced. Though real and potential damages to the global economy owing to cybercrime are calculated/estimated, McAfee considers that it is an incomplete picture because there is a belief that significant numbers of incidents remain unreported. Furthermore, Verizon reports in 2015, 2016, 2017, and 2018 provide compelling evidence that cyber incidents have increased, thus creating challenges for organisations (Verizon, 2015; 2016; 2017). The reports show that financial motivation remains one of the main drivers for cybercriminals and/or threat agent (89% in 2016; 76% in 2018).

The research of The Institute of Chartered Accountants in England and Wales has reiterated from early 2014 that cybersecurity is such an enormous challenge that combating it has almost become a *business* for organisations and governmental bodies (ICAEW, 2014). Although cybersecurity appears to be a new risk, in reality, it is a modification and a shift from previous information security to a more complex one. In other words, it is an old risk existing in a new and more complex way. Types of risks have evolved as the landscape of threats has migrated from simple viruses spread with unauthorised access and social deception (social engineering, social attacks) to substantial financial losses, disruption of business operations, loss of reputation, intellectual property loss, and loss of clients, among many other ramifications. While awareness campaigns are conducted by different organisations and governmental bodies (e.g. UK National Strategy, US Homeland Security,

National Institute of Standards and Technology (NIST), Computer Emergency Response Team (CERT), Europol, North Atlantic Treaty Organization (NATO), cyber threats still continue to be addressed by individuals, organised crime networks, competitors, nation-states, hackers, and, in some exceptional cases, from employees or contractors (ICAEW, 2014).

Likewise, a report from the Georgia Tech Information Security Center (2013) emphasises the fact that cybercriminals develop new strategies according to innovations in the field. As can be expected, practitioners have released different definitions on the topic, mainly because the subject is interrelated with various stakeholders and shareholders. For instance, KPMG (2014a) considers that cybersecurity represents an attitude towards cybercrime. Capabilities to prevent, detect, and respond to different illegal digital activities are essential. Similarly, Ernst and Young's study found that cybersecurity requires a 'multi-tiered approach' (Ernst and Young, 2014b). Later on, in 2018, Ernst and Young recommended a 'de-novo approach', meaning that due to an increase in volume and sophistication of cyber-attacks, organisations should adopt an integrated approach of strategy and culture, and they should advance towards an approach that combines the capabilities of IT and IS (Ernst and Young, 2018a).

Although cyberspace has changed the attitude of users, organisations, and governments in regard to protection, recent highly publicised online incidents confirm that more preparation against cyber threats is needed. Therefore, a continuous and active cybersecurity strategy is imperative for organisations because it would clearly draw the line between success and failure regarding the protection of both tangible and intangible assets.

Additionally, active cybersecurity management encourages boards to make riskier but more informed decisions, and accordingly, opportunities are not lost. In short, cybersecurity's role is to protect an organisation from various threats, both from the inside and outside. As has been noted in PricewaterhouseCoopers' (PwC) report, cybersecurity represents a capability to protect the "crown jewels", which embodies the revenue streams, business processes, resources, facilities, trademarks, and reputation (PwC, 2014; PwC, 2017). Proposing to minimise potential damages, organisations are advised to organise security activities in an economically effective manner (PwC, 2014). Additionally, PwC (2013a) outlines the fact that the diverse background of organisations could impede the adoption of standards/ guidance because the selection process represents a test in itself due to compatibility issues.

Regulators' view: The dynamic of cyberspace implies the involvement of participants from many sectors. Accordingly, cyberspace is a wired environment that attracts criminals, terrorists, hackers, and foreign intelligence, among other threats. As a response to such threats, organisations and governments have developed cyber strategies. For example, through its National Cyber Security Program, the UK government demonstrated from early 2011 its ability to foresee the upcoming developments of the threat landscape (UK Government, 2011). Similarly, the USA proposed to assure a safe place for online businesses and accordingly recommended the National Institute of Standards and Technology (NIST) framework as a minimum strategy for critical infrastructures (NIST, 2014).

Since UK National Security, USA Defense, Europol, and NATO are developing diverse strategies in dealing with the threats, such approaches are an explicit declaration that cyber risks are emerging in a negative dimension. The current literature abounds with debates about the volume of the development of the Internet-based attacks.

Table 2-3 below illustrates the available institutional and regulatory support among various entities from different geographical establishments.

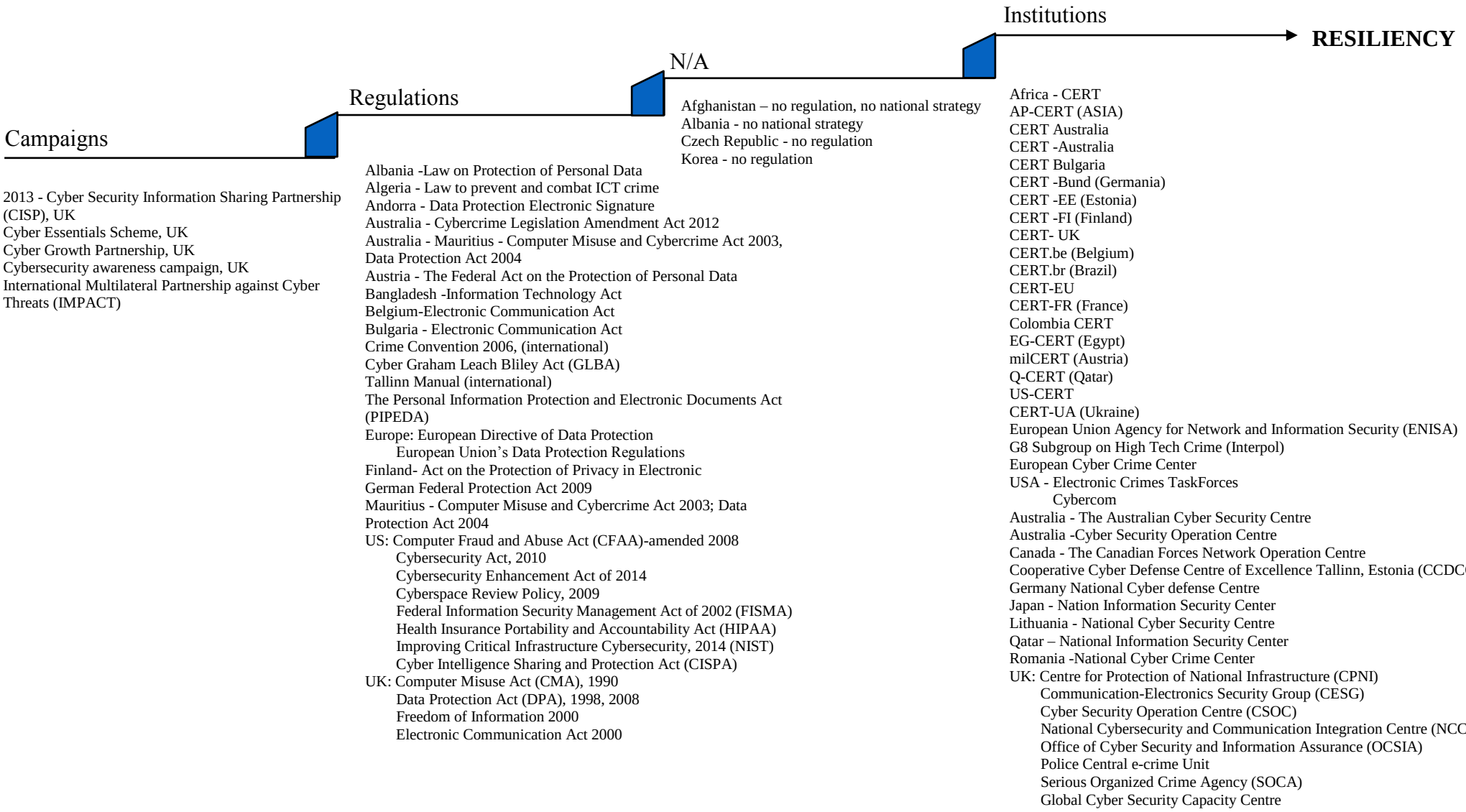


Figure 2-3 Regulatory support for cybersecurity

Source: The Researcher

N/A-not applicable, lack of regulations

As can be seen in Figure 2-3, legislation has evolved over recent years, and some national laws have been upgraded to multilateral treaties. For example, in the USA, a majority of states have adopted cybersecurity laws. The Alabama, Kentucky, New Mexico and South Dakota states are exceptions since, at the time of writing this research, regulations are still missing (Mohamed, 2015). Additionally, few more countries failed to adopt clear cybersecurity law (e.g. Afghanistan, Czech Republic, Korea), as can be seen in Table 2-3 above. In general, organisations must comply with different regulations and the lack of international laws that countries would have in common is an additional hindrance for organisations with international activities.

2.6 Cybersecurity Management

Academics' viewpoint: Recent years have shown that sophisticated technologies, Internet dependency, and cyberspace have extended perimeter for organisations and have made the handling of cyber risks a considerable challenge (Korovessis *et al*., 2017; Armenia *et al.*, 2018; Marotta and McShane, 2018). Despite significant research, there are still siloed practices in managing risk (e.g. technical silo, information security silo, departmental silos). Therefore, literature is separated into a various school of thought regarding the definition of cybersecurity.

For instance, a significant part of literature refers to cybersecurity through the lenses of information security while another part is still grounded on a technical view of IT. The view is that information is a valuable asset and must, therefore, be handled and protected appropriately. While such an asset brings advantages, it can expose organisations to various risks (Borek *et al*., 2013).). To focus only on the protection of information and information systems might also be explained by the publicised security failures of organisations that mainly referred to the assurance of information security (e.g. loss/compromise of key business data, loss of customer and employees data, loss of intellectual property, among others) (Calder and Watkins, 2012; Korovessis *et al*., 2017). Whilst some academics even advance the view that actually cybersecurity is a 'sub-set' of Information Security, respectively cybersecurity should sit under the IS umbrella (Von Solms and Von Solms, 2018).

Accordingly, some prior literature defines cybersecurity through lenses of information security and rests on assumptions made under the CIA triad (Calder and Watkins, 2012; Saleh and Alfantookh, 2011; Web *et al.*, 2014). While the additional viewpoint of Tashi and

Ghergnouti-Hélie (2009) emphasises a more complex definition of CsM. Given the increasing velocity, diversity, and volume of cybercrimes over recent years, securing information has shifted from being an IT security problem regarding the protection of information assets to a strategic challenge and respectively advancing towards Cybersecurity Management (CsM). Tashi and Ghergnouti-Hélie define information security from a more wide-ranging perspective: to achieve and maintain confidentiality, integrity, availability, accountability, authenticity and reliability of planning, organising, commanding, coordinating, and controlling through an on-going process. Hence, this continuity contributes to the identification of risks and assesses their consequences in the light of occurrences. Accordingly, businesses would be able to establish risk priorities, leading to an organised model able to reduce exposure by undertaking certain actions. Similarly, existing research of Nazareth and Choi (2014) confirms that online risks are a real issue for organisations and could render detrimental losses. The 2012 case of Saudi Aramco, a national oil producer of Saudi Arabia, is clearly an example where a lack of cybersecurity strategies disrupted all organisational activity due to the wipeout of 30,000 computers (Nazareth and Choi, 2014); RM and mitigation measures for Internet-based attacks were omitted in this case. They succeeded to prove that a close relationship between RM and CsM is required for survival. Internal coherence appears to be a hard task, and the option to stop fighting against attacks is simply unacceptable. The hypothetical scenario of consciously leaving doors open and letting attackers run free would be like writing a declaration of surrender (Reuvid, 2014). Therefore, CsM appears to be more comprehensive, inclusive, and thus far more preferable for the protection and handling of risk oversight. In this manner, the possible vulnerabilities of software, hardware, networks, and processes are acknowledged and addressed as a whole (Calder and Watkins, 2012).

Although extensive research has been carried out on cybersecurity management, many analyses were addressed under the numerous appellation as Information Security, Information Security Risk Management, Information Security, IT management, IT governance, Information Computer Technology Security, Information Technology Governance or Cyber Risk Management (Bojanc and Jerman-Blažič, 2008; Calder and Watkins, 2010; Laudon and Laudon, 2010; Turban and Volonina, 2010; Kouns and Minoli, 2010; Web *et al.*, 2014a; Fenz *et al.*, 2014; Rubino and Vitolla, 2014; Gupta and Oija, 2014; Nazareth and Choi, 2015), among others.

Figure 2-4 below offers some examples of the interchangeable use of terminology and its variation between technical and strategic reference; in some cases, the terminology differs.

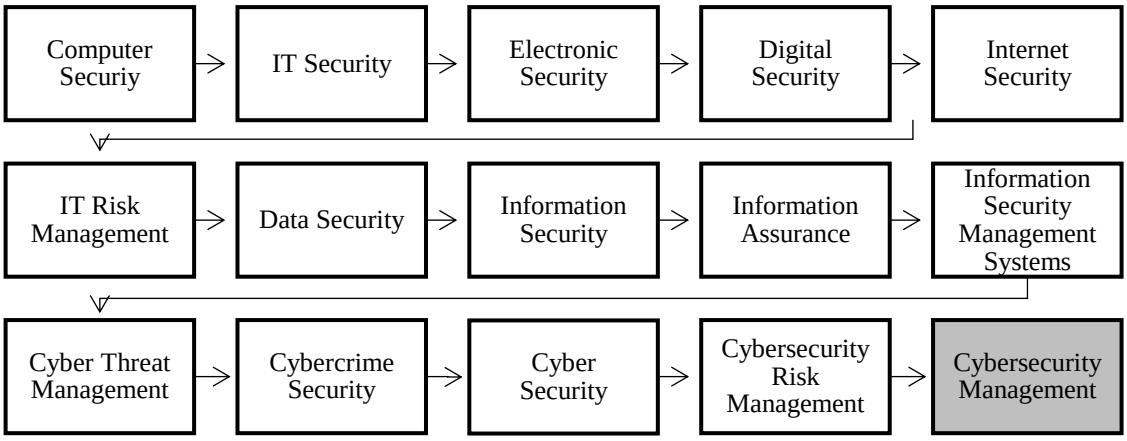


Figure 2-4 Terminology fluctuation of cybersecurity term

Source: The Researcher

Figure 2-4 above shows that the domain registers significant fluctuation in its terminology semantic and scope. This also involves an unclear definition and even conflicting and uncorrelated perspectives. Henceforth, many of them have only similarities and still seem to be used for the same purpose or context despite being different domains. Their apparent identical meanings express a partial perspective (e.g. information security, security of computers). Nevertheless, a precise definition of each term would be beyond the purpose of this research and the illustration is intended merely to outline the abundant diversity.

However, some evidence (as already discussed in Subsection 2.5.1) demonstrates that in the digital age the term *cyber*, respectively cybersecurity, is more appropriate (Hampton, 2015). Gaining cyber resilience contributes to identification of reaction to, and recovery from cyber risks with a proactive strategic mindset (Raban and Hauptman, 2018). For this reason, the Researcher will analyse the issues under the 'cybersecurity' umbrella, respectively cybersecurity management, even though in the literature examined the term is used interchangeably and could cause confusion. Apart from terminology confusion, another problem is that it has been suggested that despite the wider practice of specific guidelines and standards, in reality their implementation does not necessarily guarantee that they are the best solutions tailored to the environment and operations (Siponeh and Willinson, 2009; Maynard *et al*., 2018).

Practitioners' viewpoint: Cybersecurity threats are increasing, and organisations are concerned about resolving these challenges (Cisco, 2014; Oliver Wyman, 2018b) due to potential of disruptions, damage, and cost caused by cybercrimes. The nature and large scale of cybercrimes have become more intrusive, sophisticated, complex and severe concluding that it is a "convenient" business for cybercriminals and/or a threat agent (McAfee, 2013; CISCO, 2014; Deloitte, 2018; PwC, 2018b), and unbeneficial for the global economy.

Hence, the value of information has changed together with intensification of threats and vulnerabilities (multiple cases of failures), attackers have become more skilled and more organised, and thus strategic and technical approaches must be considered altogether. Organisations are found to be dependent on IT and Internet, and thus, risk exposure of organisations has increased (PwC, 2016; PwC, 2018b). The need for an optimised approach for risk control and risk oversight might be due to organisations' increased risk appetite. Furthermore, customer expectations (public mandate) regarding security and cyber resiliency are higher due to the increase in sophistication of technologies (Accenture, 2016; Deloitte, 2018; Accenture, 2018a). Competition is another contributor to the necessity of security. Technology evolution (velocity) as mobile technology (as new means and vectors for weaknesses) triggers increased surface of attack and multiple layers for attackers (Deloitte, 2015f; Accenture, 2018a). Moreover, the complexity of the financial system and its interconnectivity expose organisations more (Oliver Wyman, 2018b).

Subsequent studies (Ernst and Young, 2014; Marsh, 2015; Thomson Reuters Accelus, 2014; KPMG, 2014a; Websense Security Labs, 2015) re-confirm that the duty of care for cybercrime advanced together with innovations in mobile devices, the web and mobile applications, social media, web browsers, home computers, cloud computing, and the Internet of Things (IoT). In short, the viability and profitability of organisations is in strict connection to the ability to tackle and update protection on an ongoing basis (Cisco, 2014). Similarly, other practitioners expressed concerns regarding the way in which IT issues are handled. Cyber risks remain a complex challenge for organisations, and it is believed that the engagement of executive management can foster a more resilient position (PwC, 2014; Accenture, 2018b). Recommending a top-down strategy appears to be the first step when advising how to assure holistic protection against malicious cyber activities (IT Governance, 2015; KPMG, 2015). However, not all organisations show that they are adhering to holistic management of cyber risks (Ernst and Young, 2018). Some evidence

agrees that half of organisations fail to integrate cybersecurity in strategic planning, respectively organisational strategy (Ernst and Young, 2018b).

As the threat spectrum has changed over the years, likewise the global business environment has tried to respond adequately. For example, Ernst and Young's report of 2014 looked at multiple sectors in regards to the current state of cybersecurity and concluded the effects of aligning cybersecurity departments as not fulfilling the organisation's function; the study proposes that a managerial approach might fortify its functions (Ernst and Young, 2014a). In particular, for financial organisations the reality of risk has always existed, ranging from robberies, fraud, theft, and many other criminal activities. However, emerging technologies have brought new challenges, and the reality of cybersecurity threats impose additional actions failing to protect revenue, business activity, assets, and reputation. Nonetheless, such an issue requires long-term investments of money, resources, and employees (Thomson Reuters Accelus, 2014).

Although a lot of guidance and regulations have been released, the silo approach seems to continue (Marsh, 2015). On these grounds, an organisation manages risks in a variety of ways, depending on a silo or holistic approach regarding probable losses (e.g. intellectual property, business interruption, reputation, customer trust, loss of sensitive information, financial loss, etc.). The issue of global cybersecurity losses is almost incalculable due to the fact that estimation/prediction often relies on surveys (McAfee, 2013; Websense Security Labs, 2015). Losses were estimated in 2014 to approximately $400 billion and later on in 2018 to be $600 billion (McAfee, 2014, 2018). Nonetheless, it seems that 'biased' surveys and unreported cyber malicious incidents (i.e. events that were maybe not realised in full yet had criminal intention) contribute to the inability to understand the implications of cyber threats at a global level (Marsh, 2015).

Over time practitioners' efforts have expanded to knowledge orientated towards various aspects of CsM, fluctuating among strategy, value creation, risk oversight, maturity assessment, or organisational risk culture.

Table 2-4 CsM literature focus fluctuations amongst practitioners' reports

Focus	Key considerations	Entity/year
Strategy	• Cybersecurity should be tackled strategically; • Cybersecurity strategy should be aligned with organisation strategy; • An organisation should comply with the security of industry standards guidelines.	KPMG (2013a); PwC, 2013a); PwC (2014); KPMG (2014d).
Value	• Management, RM and audit are responsible for value creation and its measurement.	Deloitte (2015e); McKinsey (2015); BSI (2018a).
Performance	• Strategic alignment sustains business performance.	Ernst and Young (2014b); BSI (2018a).
Risk oversight	• Risk oversight is significantly challenged; • Cybercrimes losses are significant across globe; • Cyber resilience is increasingly difficult to achieve; • Cybersecurity needs a top-bottom approach.	KPMG (2013b); Ponemon Institute (2013); CISCO (2014); PwC (2014); KPMG (2014b); McAfee (2014); Thomson Reuters Accelus (2014); Verizon (2015); Websense Security Labs (2015); Oliver Wyman (2018).
Maturity	• Organisation cybersecurity maturity needs to be identified.	Deloitte (2012); KPMG (2015); Deloitte (2018).
Risk culture	• The culture should assimilate the CsM framework.	KMPG (2014a).

Source: The Researcher

As can be observed in Table 2-4 the practitioners' reports focus on top-down and bottom-up approaches (strategic and operational) as well as the enumeration of key considerations, demonstrating that multiple factors (e.g. strategy, value, performance, risk oversight, maturity, risk culture, resources and capabilities, objectives and finally, planning) compound together. Thus, all of the elements are dependent on reaching a business overall strategy, resiliency and effectiveness.

Regulators' viewpoint:

The financial industry has unique challenges and interrelated implications within national economies, thus the regulators' scope is to determine and shape the financial sector's behaviour in minimising losses due to cyber risks (Basel Committee on Banking Supervision, 2018). Of much more concern is that the type of risk broadened as well as sophistication and severity (Basel Committee on Banking Supervision, 2018). Despite various benefits brought by innovations in technology, it also determines rises in vulnerabilities (Financial Stability Board, 2017; Financial Conduct Authority, 2018). Specific to the financial industry is that apart from cyberspace exposure and technology use, interconnections between financial institutions and related third parties represent another avenue of risk exposure (Financial Stability Board, 2017). Besides, factors as changing

consumer behaviour. The complexity of technology or exposure to a different type of threat (treat intelligence), place more pressure on the financial industry to prepare proactively and provide risk resiliency (Bank of England, 2018). Another particularity is that instability or even outage of financial organisations affect the financial system, other organisations, market participants and even consumers through ripple effects (Financial Conduct Authority, 2018; Bank of England, 2018).

Looking beyond the trend of poor adoption of cybersecurity principles as seen in academic papers and similarly in business practices, the regulators' viewpoints alternate correspondingly. The most significant limitation within the industry is that cyber is managed through the lenses of IT or operational risk (Basel Committee on Banking Supervision, 2018), thus failing to address the CsM strategically. For instance, some legislation refers only to security/assurance of information (e.g. Data Protection Act 1998; Federal Information Security and Management Act of 2002; EU General Data Protection Regulation, General Data Protection Regulation (GDPR, 2016)) versus regulation that refers to a more inclusive security of assets, people, information, practices, processes, and technology (e.g. Cybersecurity Act of 2012). Such discrepancies in terminologies and meanings are present in various industry standards and guidelines (i.e. NIST used the term *cybersecurity* while BS ISO 27000 and its series refers to it as *Information Security*). The question of variation in terminology and semantics need to be addressed urgently as it affects theoretical legacy and industry practices as well as regulatory applicability along with organisational behaviours.

Adhering to the applicability of regulatory recommended good business practices typically specifies baseline practices for assuring a minimum level of cybersecurity to avoid careless practices. For instance, in the UK as a proof of due diligence and preventative practices, organisations are required to evaluate partners' collaborators, and/or third-parties' cyber-risk good practice (HM Government, 2015a). This is due to the fact that in the past many incidents were identified to have been caused by a third-party's lack of cyber risk controls. In a report of 2015, HM Government evidenced that less than 50% of organisations have adopted legal and practical measures for cyber risks (for example, contract clauses, third-party audit, pre-contract due diligence, third-party self-assessment) (HM Government, 2015a). Additionally, it was found that few organisations require endorsement and certifications from third-parties (e.g. Cyber Essential Scheme, Innovation Voucher Scheme).

As these arguments suggest, safeguarding the financial industry is pivotal. In the 2018 Financial Conduct Authority report, it was concluded that challenges are much higher—a significant increase of 138% in the number of cyber incidents (Financial Conduct Authority, 2018) was concluded. Consensus amongst regulators is that to counteract challenges of cyber risks, a closer relationship between industry, academia, and government should be formed. An example is Cyber Security Information Security Partnerships (CiSP) available to bring implied mutual benefits to all parties (CERT-UK, 2015). Additionally, regulatory requirements are in most cases in line with industry standards/practices (Basel Committee on Banking Supervision, 2018).

Moreover, such initiative was also considered by the UK London Chamber of Commerce and Industry back in 2014, which outlines that the expansion of the Internet over the last few years has succeeded to unveil new security challenges for organisations (UK London Chamber of Commerce and Industry, 2014). It is estimated that every year organisations spend millions of pounds on counteracting this issue (UK London Chamber of Commerce and Industry, 2014). While cybercriminals continue to target organisations due to their valuable trade secrets, intellectual property, credentials or customer financial data, regulations are unable to stop this trend and only propose worthy practices to lessen damages to organisations as well as indirectly to society.

It is becoming increasingly difficult for organisations to comply and to assure transparency, hence increased regulatory demands tend to change from voluntary to prescriptive, and mandatory standards are centred and generally accepted rules within organisations.

Conversely, there is a general belief that to apply past lessons and to move from a stationary to a more dynamic approach encompass challenges in practice, information confirmed by many exposed organisational resiliency failures (i.e. the case of Bangladesh Bank, 2016).

2.7 Alignment paradigm

Academic's viewpoint: Alignment is considered a process worth achieving due to implications of effectiveness and efficiency on integrating managerial and administrative internal controls (Luftman, Papp and Brier, 1999). After years of research, the alignment is currently criticised as being a fragmented paradigm, separated in various streams (Volk and Zerfass, 2018). For instance, some authors, outline the process of alignment through **the lense of strategic fit.** Others such as Salaheddine and Ilias (2017) emphasise alignment as being a continuous strategic process of integration based on the well-known PDCA (plan-do-check-act) circle and it is thus believed that culture and leadership are critical (a top to

bottom approach). Likewise, other academics focused on **alignment benefits.** Jevtić *et al.* (2018) concentrate on performance, measuring internal alignment. For that reason, there are clear indications demonstrating that interest in achieving alignment has been continuously maintained over time. The research of Smaczny (2001) explicitly indicates that a possible explanation for alignment benefits and determination is the fact that organisations have acknowledged the importance of integration and any adverse outcome of un-aligned business strategies (for example, low returns).

Some research studies suggest that by achieving alignment, an organisation is less vulnerable to market changes and internal inefficiency because the alignment creates a standard and centric/unified solution (Bergeron, Raymond and Rivard, 2004) in handling risks with all available resources and capabilities. Such an approach is similar to the initial research of Henderson and Venkatraman (1990), who outline the value of a unified approach towards the achievement of organisational goals and missions (i.e. alignment is driven to prioritise decisions in correlation to organisational goals and missions instead of CsM or ERM priorities). Noticeably key literature validates the fact that Henderson and Venkatram were the initiators of strategic alignment research and created the platform for subsequent work (Henderson and Oldach 1993; Campbell, Kay and Avison, 2005; Gutierrez, Orozco and Serrano, 2009; Preston and Karahanna, 2009; Mekawy, AlSabbagh and Kowalsky, 2014; Reynolds and Yetton, 2015; Hinkelman *et al*., 2015).

Another stream of alignment is the one that focuses on the **challenges of alignment.** A significant body of research indicates that the achievement of the alignment is one of the biggest concerns and challenges of IT/IS executives and boards since early 2000 (Reich and Benbasat, 2000; Avison *et al.,* 2004; Chan and Reich, 2007; Chen, 2010; Corsaru and Snehota, 2011; Reynolds and Yetton, 2015; Preston and Karahama, 2009; Wu, Straub and Liang, 2015; Yarifard, Taheri and Zafarzadeh, 2016); but one worth striving for due to its benefits. For instance, Volk and Zerfass (2018) study outline communication as a critical element for achieving alignment. However, Baets (1992) formally confirmed that the theory applied has faced significant challenges over the last years. Additionally, other studies provide evidence about constant challenges in alignment.

Furthermore, some investigations have focused mainly on alignment dimensions whereas other studies have concluded that strategic alignment could be accomplished from the following perspectives: IT-business alignment, IT-RM alignment, or CsM alignment with

ERM. Conversely, another stream of research is the **cultural alignment** that has been researched by authors such as Shao (2018), who argues that culture is a moderator for effective implementation. Shao's research findings emphasise that culture should be a controlling mechanism that moderates potential internal misalignment.

Research regarding the antecedents and consequences of non-alignment is of constant interest (Hung and Hu, 2007; Taradfar and Qrunfleh, 2009; Walter *et al.*, 2013; Coltman *et al*., 2015; Volk and Zerfass, 2018) hence alignment ensures proactive and continuous practices in the direction of the strategic alignment. Although variations of terms appear in literature, in general, the meanings are common and might be defined as a fusion of strategies to achieve effectiveness and efficiency across an organisation (Luftman, 2000).

Based on the review of preceding literature, the term *aligned* appears to be hidden under different terminology such as 'fit', 'co-aligned', 'linked', 'congruent', 'contingent', 'matched', 'harmony', 'fusion', 'synchronisation', 'integration', 'synergy', to name but a few terms. Furthermore, alignment has been investigated from distinctive social, strategic, structural, technical and intellectual perspectives (Reich and Benbasat, 1996; Yarifard, Taheri and Zafarzadeh, 2016), whereas the strategic alignment has registered a more significant number of studies by scholars and practitioners.

However, Cragg, King and Hussin (2002) point out that most authors have been discussing alignment without a clear indication as to how it can be achieved. Many other authors have consequently reviewed this issue, and Table 2-5 below summarises some of the research that has enabled the development of the paradigm through a three-dimensional perspective – adoption, implementation, and assessment.

Table 2-5 Three-dimensional perspective of the alignment literature

Fluctuation of alignment literature focus	**Authors**
Alignment adoption	Baets (1996); Luftman (2000); Cragg, King and Hussin (2002); Avison *et al.* (2004); Sledgianowsky and Luftman (2005); Huang and Hu (2007); Preston and Karahanna (2009); Johnson and Lederer (2010); Rahman and Donahue (2010); Saleh and Alfantookh (2011); Volk and Zerfass (2018).
Alignment implementation	Luftman, Papp and Brier (1999); Kearns and Lederer (2000); De Haes and Van Grembergen (2009); Shao (2018); Volk and Zerfass (2018).
Alignment assessment	Luftman (2000); Burn and Szeto (2000); Reich and Benbasat (2000); Chan, Sabherwal and Thatcher (2006); Gutierrez, Orozco and Serrano (2009); Yarifard, Taheri and Zafarzadeh (2016); Salaheddine and Ilias (2017); Jevtić *et al*. (2018); Joshi *et al*. (2018).

Source: The Researcher

Compiling this evidence demonstrates that literature consists of different phases of alignment yet multiple studies addressing all phase are scarce.

Practitioners' viewpoint: The alignment of IT with ERM is a common practice among organisations, and although it considers the alignment in a traditional silo approach, it is part of the legacy. Often the organisational effectiveness is measured by key risk indicators (KRI), which assure that necessary measures are yielding results as anticipated. Thus, it comprises of a three-dimensional perspective: align, integrate and measure (KPMG, 2014; Grant Thornton, 2016). Even so aligning organisational strategy, with RM and culture currently remains a current challenge (PwC, 2018).

2.8 Literature key findings

From its early beginning, alignment has been identified as necessary, but literature is scarce regarding methods that could achieve and sustain it (Sledgianowsky and Luftman (2005). The Strategic Alignment Maturity (SAM) of Henderson and Venkatraman (1993) is viewed by several academics (Smaczny, 2001); Avison *et al*., 2004; DeHaes and Van Grembergen, 2009; Gutierrez, Orozco and Serrano, 2009) to be an initial framework for identifying, sustaining, achieving, and maintaining alignment. However, organisations are still none the wiser how to achieve alignment in practice (Preston and Karahanna, 2009). Therefore, impediments of alignment such as culture gaps (e.g. between IT and business boardrooms, IT and business departments), the lack of communication, inadequate knowledge sharing, and many other reasons maintain a miss-alignment among industries (Huang and Hu, 2007). Although in practice some organisations seek to align their RM with ERM, others indirectly discourage the action due to their own organisational culture that encourages (in some cases) departmental competition (Cambell, Kay and Avison, 2005).

Additional evidence outlines that despite extensive research, alignment remains a top issue; a fact confirmed by other authors such as Cragg, King and Hussin, 2002; Avison *et al.*, 2004; Preston and Karahanna, 2009; Johnson and Lederer, 2010; Chen, 2010; Rahman and Donahue, 2010; Reynolds and Yetton, 2015. Alignment has become a more challenging issue in the view of emerging technology developments, regulatory demands, market volatility, and competition in comparison to its early beginnings. Chen (2010) suggests that there are many organisations that fail to align their strategies due to their size (large

organisations versus multinational organisations), yet a broader strategy would most likely yield success. While most authors have focused on strategic alignment and discussing internal strategic alignment, some other studies (Siponen and Willinson, 2009; Walter *et al.*, 2013) propose an alignment that also considers the external environment. As such, the environment and the strategy could 'co-align' and lead to a consensus on strategies that would prevent possible failures of alignment.

In early stages, past literature that investigated alignment (Raymond and Rivard, 2004) proposed to focus on IT/IS alignment without specific interest paid to information security. This demonstrates that the literature related to alignment is scarce when researching the CsM alignment to ERM and is more oriented to IT. It is not surprising that some authors believe that alignment represents a complete picture of maturity exposure since it unifies all the organisation's risks and in particular management activities to build common goals for business and IT (Huang and Hu, 2007).

Figure 2-5 below outlines the findings mentioned above

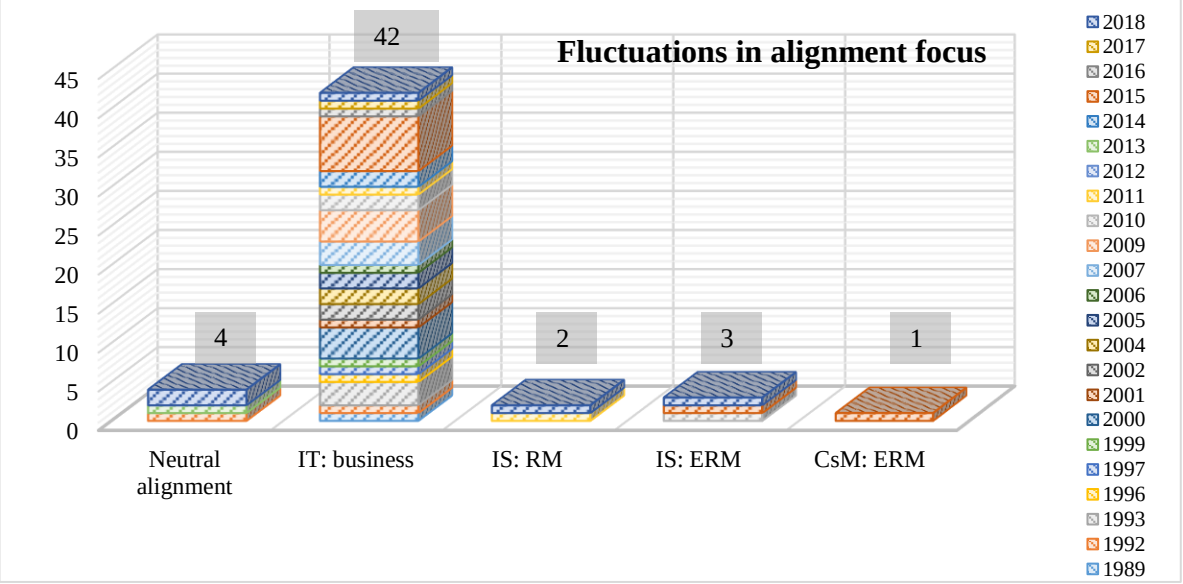


Figure 2-5 Progression of alignment literature across domains

Source: The Researcher

As can be seen in Figure 2-5, previous studies relating to alignment do not represent a new area. Although scholars and practitioners have investigated the topic, it seems that research is insufficient and concentrates specifically on the alignment of CsM with ERM. Based on literature examination of prior research on alignment, it appears that literature significantly

focused on IT alignment with business strategies (42 journals) rather than other alignment domains, which were left on the side as suboptimal research.

Seeing that alignment entails various types (neutral, IT strategy alignment with business strategy, IS wit RM, IS with ERM), the research problem is justified hence CsM alignment with ERM is scarce, if not non-existent. Additionally, following the research background, Table 2-5 acknowledges the importance of shifting from the traditional management of IT to a more complex strategy of CsM.

In view of that, Table 2-6 illustrates the actual focus and the prospect of cybersecurity among academics, practitioners and regulators. Accordingly, the structure is separated into four quadrants so as to explain various empirical and conceptual literature.

Table 2-6 Paradigm shifts (transitions) of cybersecurity literature

Key literature paradigm shifts	**Key authors**
Cybersecurity neutral state	Siponen and Willison (2009); Von Solms and Van Niekerk (2013); Robinson, Jones and Janicke (2015); Min, Chai and Han (2015); PwC (2013a); Oxford Economics (2014); Thomson Reuters Accelus (2014); McAfee (2014); Ponemon Institute (2015); World Economic Forum and Deloitte (2015); Verizon (2015); Bank of England (2013); Conference of State Bank Supervisors (2014); Ponemon Institute (2013); Department of Homeland Security (2002); UK Cabinet Office (2011); European Network and Information Security Agency (ENISA) (2012); Europol (2014); UK London Chamber of Commerce and Industry (2014); CESG (2015a,b); CCDCOE (2015); USA Department of Treasury (2015).
Cybersecurity from IT perspective	Singh, Gupta and Oija (2014); Nazareth and Choi (2015); Websense Security Labs (2015); Oliver Wyman (2018); Rubino (2018).
Cybersecurity from RM perspective	Bojanc and Jerman-Blažič (2008); Saleh and Alfantookh (2011); KPMG (2014d); Ernst and Young (2014b); ICAEW (2014); Fenz *et al.* (2014); Webb *et al.* (2014a); Reuvid (2014); Marsh (2015); HM Government (2015b); Mohammed (2015).
Cybersecurity from ERM perspective	PwC (2012); Rubino and Vitolla (2014); Stoll (2015).

Source: The Researcher

Additionally, following the research background variations identified in Table 2-6, the following table, Table 2-7, acknowledges the importance of shifting from the traditional management of IT to a more complex strategy of CsM. Thus, alignment of CsM with ERM yields an elimination of risk siloed approaches and reduces organisational exposure owing to a single, unified mechanism (Deloitte, 2014b) that can deal with all risk portfolio (RIMS,

2014). Table 2-7 provides more detail regarding traditional and recommended approaches of collaborative departments and functions.

Table 2-7 Pro' and cons' of cybersecurity affiliation matrix

Cybersecurity with IT		**Cybersecurity with ERM**
Advantages Ability to propose technical solutions; Control on software and hardware; Departmental level of control; Independence of decisions; Informed cybercrime trends; IT-centric to security; Technical risk prediction.	+	**Advantages** Business productivity; Common governance; Common technology platform; Competitive advantages; Compliance; Cross-domain knowledge; Derive value from IT (strategic use); Effective strategic prioritization (operational efficiency); Increase in business performance; Increased resiliency; Integrating governnace; Lowering costs/reduce the double effort; Maintenance of shareholders and stakeholders trust (strategic); Minimization of loss; Organizational awareness; Pro-active, continuous; Real-time visibility in business performance; Shared communication; Support business strategy and objectives; Sustained alignment.
Disadvantages Disconnected databases; Double supervisory functions; Duplication of resources and infrastructure; Focus on technical aspects (hardware software); Focus on vulnerabilities, not opportunity. Fragmented governance; Lack of accountability (how effective is); Lack of common language; Lack of communication; Lack of consensus in IT strategy and ERM strategy; Lack of security awareness among organization; Lack of strategic use of IT; Late risk identification; Misalignment to organizational strategy; Silo strategies (double effort, cost, and time consuming); Uncertain return on spending; Weak support of management (organizational dysfunctions).	-	**Disadvantages** Bureaucracy; Compliance to standards; Cost (balance of investment and return); Difficulties in adjusting IT strategies to ERM strategies; Difficulties in implementation (barriers); Focus on opportunity rather than risks; Hard to quantify risks; Increased budgets; Management based on assumptions; One size fit (unspecialized focus on departments); On-going alignment; Outsourcing certifications; Personalisation of standardized approaches; Prioritization of risk; Undermined IT managerial capabilities (under ERM management).

Source: The Researcher

It can be seen from the data presented in Table 2-7 that indeed, the advantages yielded by the traditional approach are noticeable but limited to responsibilities relating to software and hardware issues. On the other hand, an alignment with ERM provides support and guidance for the whole organisation and risks are mainly undertaken in accordance to business performance goals (Grant Thornton, 2016). In conjunction with technical responsibilities, the new approach widely improves the efficiency of organisational security. Hence, ERM successfully incorporates IT security and business risks and sustains common governance.

Additionally, the following table outlines the literature review (312 documents), which is related to the research problem.

Table 2-8 Identified literature based on the research paths

Domain	No.	Author/s
RM		
Academics'	23 journals	Crockford (1982); Schmit and Roth (1990); Smith (1995); Stulz (1996); Oldfield and Santomero (1997); Clarke and Varma (1999); Tilman (2001); Hillson (2002); Raz and Hillson (2005); Nag, Hambrick and Chen (2007); Jorion (2009); Servaes, Tomayo and Tufano (2009); Borison and Hamm (2010); Verbano and Venturini (2011); Yaraghi and Langhe (2011); Pirson and Turnbull (2011); Chang *et al.* (2011); Aebi, Sabato and Schmid (2012); Dionne (2013); Lenssen, Dentchev and Roger (2014); Schroeder (2014); Calandro (2015); Falkner and Hielb (2015).
Practitioners'	6 reports	Australian/New Zeeland Standard (2004); Aon (2015); IRM (2002); Ponemon Institute (2011); PwC (2012); AICPA (2018).
Regulators'	8 reports	FERMA (2003); HM Treasury (2004); Financial Reporting Council (2005); HM Treasury (2009); OECD (2014); USA Department of Treasury (2014); Basel (2014); Basel (2015).
ERM		
Academics'	53 journals	Miller (1992); Dickinson (2001); Kleffner, Lee and McGannon (2003); Ward (2003); Liebenberg and Hoyt (2003); Beasley Clune and Hermanson (2005); Drew and Kendrick (2005); Nocco and Stulz (2006); Rosenberg and Schuermann (2006); Beasley,Pagach and Warr (2008); Castro *et al*. (2008); Fraser, Schoening-Thiessen and Simkins (2008); Francis and Paladino (2008); Burnaby and Hass (2009); Mikes (2009); Power (2009); Gordon, Loeb and Tseng (2009); Arena, Arnaboldi and Azzone (2010); Arnold *et al*. (2011); Eckles, Hoyt and Liebenberg (2011); Pagach and War (2011); Lindberg and Seifert (2011); McShane, Nair and Rustambekov (2011); Paape and Spekle (2012); Lin, Wen and Yu (2012); Schiller and Prpich (2013); Baxter *et al*. (2013); Tekathen and Dechow (2013); Hoyt and Miller (2014); Farrel and Gallagher (2014); Hayne and Free (2014); Lundqvist (2014); Ching and Colombo (2014); Nair *et al.* (2014); Rubino and Vitolla (2014); Aven and Aven (2015); Beasley, Branson and Pagach (2015); Bromiley *et al*. (2015); Grace *et al.* (2015); Shad and Woon (2015); Lundqvist (2015); Lalitha (2015); Lyons (2015); Gatzer and Martin (2015); Zéghal and El Aoun (2016); Andrén and Lundqvist (2017); Bogodistov and Wohlgemuth (2017); Viscelli, Hermanson, and Beasley (2017); Aguilera, Judge, and Terjesen (2018); Farrel and Gallagher (2019); McShane (2018); Oliveira *et al.* (2018); McShane (2018).
Practitioners'	43 reports	COSO (1992); The Institute of Chartered Accountants in England and Wales (1999); Casualty Actuarial Society (2003); COSO (2004); AS/NZS (2004); Standard and Poor's (2008); Accenture (2009); British Standard (2009); Deloitte (2009); PwC (2009); OCEG (2009); Manigent (2009); McKinsey and Company (2010); Tower Watson (2010); BSI (2011b); BSI (2011c); RIMS (2011); Manigent (2011); Protivity (2012); COSO (2012); COSO (2013); McKinsey and Company (2013a); PwC (2013b); KPMG (2013b); Grant Thornton (2013); McKinsey and Company (2014); Tower Watson (2014); Deloitte (2015a); Deloitte (2015b); Deloitte (2015c); Deloitte (2015d); PwC (2015); COSO (2015a); Ernst and Young (2015); RIMS (2015); CGMA (2015); OCEG (2015); Thomson Reuters (2015); COSO (2016); McKinsey and Company (2016); American Institute of Certified Public Accountants (2017); KPMG (2017b); COSO (2017).
Regulators'	4 reports	SOX (2002); Dodd-Frank Act (2010); NYSE (2014); Financial Reporting Council (2016).
CsM		
Academics'	41 journals	Cicognani (1998); Strate (1999); Hong *et al*.(2003); Kotulic and Clark (2004); Peppard and Ward (2004); Posthumus and Von Solms (2004); Von Solms and Von Solms (2004); Gerber and Von Solms (2005); Chang and Ho (2006); Caralli *et al*. (2007); Da Veiga and Eloff (2007); Bojanc and Jerman-Blažič (2008); Humphreys (2008); Ma, Schmidt and Pearson (2009); Siponen and Willison (2009); Tashi and Ghernouti-Hélie (2009); Deibert and Rohozinski (2010); Von Solms and Van Niekerk (2013); Julich (2013); Atoum, Otoom and Abu Ali (2014); Fenz *et al*. (2014); Schiavone,Garg and Summers (2014); Singh,Gupta and Ojha (2014); Craigen,Diakun-Thibault and Purse (2014); Web *et al*. (2014a); Web *et al.* (2014b); Stoll (2014); Tyagy (2014); Robinson, Jones and Janicke (2015); Lehto and Neittaanmäki (2015); Min, Chai and Han (2015); Mohammed (2015); Nazareth and Choi (2015); Soomro, Shah and Ahmed (2016); Korovessis *et al*. (2017); Armenia *et al*. (2018); Raban and Hauptman (2018); Marotta and McShane (2018); Gordon *et al*. (2018); Von Solms and Von Solms (2018); Nasir *et al.* (2019).
Practitioners'	39 reports	ISSA (2004); British Standard Institution (2009); Lloyds (2010); Information Security Forum (2011); British Standard institution (2011a); British Standard Institution (2012); Deloitte (2012); KPMG (2013a); Ponemon Institute (2013); British Standard (2013a); British Standard Institution (2013b); British Standard Institution (2013c); PwC (2013a); McAfee (2013); CISCO (2014); Ernst and Young (2014); PwC (2014); Thomson Reuters Accelus (2014); McAfee (2014); KPMG (2014b); KPMG (2014c); KPMG (2014d); KPMG (2014e); CSIS (2015); KPMG (2015); Marsh (2015); Ponemon Institute (2015); IT Governance (2015); Verizon (2015); Websense Security Labs (2015); Deloitte (2014); World Economic Forum and Deloitte (2015); Deloitte (2015e); Deloitte (2015f); Accenture (2016); British Standard Institution (2016); Gartner (2016); Oliver Wyman (2018b); Deloitte (2018).

Regulators'	39 reports	OECD (2002); USA, Department of Homeland Security (2002); UK Cabinet Office (2009); UK Cabinet Office (2011); ISO (2011); NIST (2011); USA Department of Homeland Security (2011); ISACA (2012); ISO (2012); ENISA (2012); CESG, Cabinet Office, CPNI and Department for Business, Innovation and Skills (2012); CESG (2012); Bank of England (2013); ISACA (2013); NIST (2013a); NIST (2013b); ICAEW (2014); USA Department of Financial Services (2014); EUROPOL (2014); NIST (2014); UK London Chamber of Commerce and Industry (2014); CSBS (2014); Oxford Economics (2014); HM Government (2014); USA Department of Treasury (2015); Financial Industry Regulatory Authority (2015); NATO CCDCOE (2015); HM Government (2015a); HM Government (2015b); HM Government (2015c); CERT-UK (2015); CESG (2015 a, b); USA Office of Management and Budget (2015); BSI (2016a); ENISA (2017); Financial Stability Board (2017); Basel Committee on Banking Supervision (2018); Financial Conduct Authority (2018); Bank of England (2018).		
Alignment				
Academics'	52 journals	Henderson and Venkatraman (1989); Henderson and Venkatraman (1990); Baets (1992); Powell (1992); Broadbent and Weill (1993); Henderson and Venkatraman (1993); Venkatraman, Henderson and Oldach (1993); Baets (1996); Ciborra (1997); Luftman, Papp and Brier (1999); Papp (1999); Burn and Szeto (2000); Kearns and Lederer (2000); Reich and Benbasat (2000); Luftman (2000); Smaczny (2001); Chan (2002); Cragg, King and Hussin (2002); Bergeron, Raymond and Rivard (2004); Avison *et al*.(2004); Campbell, Kay and Avison (2005); Sledgianovsky and Luftman (2005); Chan, Sabherwal and Thatcher (2006); Chan and Reich (2007); Huang and Hu (2007); Luftman and Kempaiah (2007); De Haes and Van Grembergen (2009); Gutierrez, Orozco and Serrano (2009); Preston and Karahanna (2009); Taradfar and Qrunfleh (2009); Chen (2010); Johnson and Lederer (2010); Rahman and Donahue (2010); Corsaru and Snehota (2011); Saleh and Alfantookh (2011); Walter *et al*. (2013); Charoensuk, Wongsurawat and Khang (2014); Mekawy, AlSabbagh and Kowalsky (2014); Fakhri,Fahiman and Ibrahim (2015); Coltman *et al*. (2015); Gerow, Thatcher and Grover (2015); Reynolds and Yetton (2015); Wu,Straub and Liang (2015); Hinkelman *et al*. (2015); Karpovsky and Galliers (2015); Luftman, Lyytinen and Zvi (2015); Yarifard, Taheri and Zafarzadeh (2016); Salaheddine and Ilias (2017); Volk and Zerfass (2018); Jevtić *et al*. (2018); Joshi *et al*. (2018); Shao (2018).		
Practitioners'	3 reports	KPMG (2014a); Grant Thornton (2016); PwC (2018a).		
Regulators'	0 reports	none		
TOTAL	312	Documents		
		169 academics research papers	91 practitioner's documents	51 regulators documents

Source: The Researcher

Table 2-8 represents the key contributors who have written corresponding literature regarding some aspects of the research topic: RM field. While, the primary foundation of the topic is separated into three key related concepts: CsM, ERM and Alignment, it has been identified that in the case of CsM and ERM alignment there is scarce academic literature and for this reason other congruent research from IT and RM fields has been considered. The academic literature proposed consists of 169 documents, along with 91 practitioners' documents and 51 regulatory documents. Journals have been compared against the Academic Journal Guide 2015 (a consultative guide to measure journals rankings) of Association of Business Schools (2015) and thus might be subject to some limitation.

The systematic examination identified that apart from domain focus, the selected literature has been significantly extracted from the fields of finance and information management with predominant three stars' journals. Moreover, undertaking this approach validates that over recent years CsM and ERM have been hardly researched. ERM registers a similar situation, even though there are some journals related to traditional RM. Although 312 documents have been considered for this research, additional documents have also been used to extend prior work. The further additional contribution is falling outside the above literature review examination.

Paradigm	**Legend**: Author/s, (1) Main paradigm (adoption, implementation, measurement); (2) Key focus of research; (3) Methodology used (T=Theoretical evidence; E=Empirical evidence); (4) Contribution; (5) Future research recommended				
CsM	**Hong *et al*. (2003)** 1. Implementation challenges 2. Managerial effectiveness of IS 3. **T** (qualitative research methods) 4. IS management theory 5. Predict organisational behaviour	**Peppard and Ward (2004)** 1. Measurement challenges 2. IT/IS management performance 3. **T** (qualitative research methods) 4. IS/IT and delivering business value 5. Strategic management of IT/IS	**Posthumus and von Solms (2004)** 1. Implementation challenges 2. Effective information security strategy 3. **T** (qualitative research methods) 4. Propose a framework 5. Information security governance	**Kotulic and Clark (2004)** 1. Measurement challenges 2. Effectiveness of an IS programme 3. **E** (mixed: surveys, interviews) 4. IS domain being sensitive 5. Guidelines for managing IS	**Gerber and Von Solms (2005)** 1. Implementation challenges 2. Integrated approach to risks 3. **T** (qualitative research methods) 4. Guidance for integrated approach of IS 5. Alternative to holistic IS
	Chang and Ho (2006) 1. Implementation challenges 2. Influences in implementation IS 3. **E** (quantitative: surveys) 4. Real impact of organisational factors 5. IS management adoption and practice	**Da Veiga and Eloff (2007)** 1. Adoption challenges 2. Organisational culture towards IS 3. **T** (qualitative research methods) 4. IS framework 5. IS culture measurement	**Bojanc and Jerman-Blažič (2008)** 1. Implementation challenges 2. Problems associated with investments 3. **E** (quantitative research methods) 4. Standardised approach recommended 5. Standards determining the financial risk	**Siponen and Willison (2009)** 1. Implementation challenges 2. Complying with guidelines 3. **E** (qualitative research methods) 4. Generic practice of IS 5. Optimisation of practices	**Solms and Van Niekerk (2013)** 1. Adoption challenges 2. Cybersecurity defined 3. **T** (qualitative research: scenario) 4. Expanded the theoretical concept 5. International standards and practices
ERM	**Dickinson (2001)** 1. Implementation challenges 2. Top-down process of ERM 3. **E**: (quantitative: 123 surveys) 4. Part of organisation agenda 5. ERM and planning process	**Kleffner, Lee and McGannon (2003)** 1. Implementation challenges 2. Obstacles to implementation 3. **E** (mixed: survey and interview) 4. Guidelines are influencing RM 5. Common definition and standard	**Liebenberg and Hoyt (2003)** 1. Adoption challenges 2. Firm value and CRO 3. **E** (quantitative research methods) 4. CRO's contribution to ERM 5. Determinants of ERM	**Beasley, Clune and Hermanson (2005)** 1. Implementation of ERM 2. Embracing ERM 3. **E** (Quantitative: 123 surveys) 4. Factors of ERM implementation 5. ERM effectiveness	**Beasley, Pagach and Warr (2008)** 1. Implementation challenges 2. Appointment of a CRO 3. **T** (Qualitative:120 observations) 4. Various determinants factors 5. ERM adoption
	Gordon *et al.* (2009) 1. Measurement challenges 2. ERM and firm performance 3. **E (**quantitative research methods) 4. ERM and performance dependency 5. Contextual variables and ERM	**Arena *et al.* (2010)** 1. Measurement challenges 2. ERM performance management 3. **E** (Qualitative: interview/case study) 4. Explanations of RM practice. 5. Contamination with other disciplines	**Hoyt and Liebenberg (2011)** 1. Measurement challenges 2. Firm value /the appointment of a CRO 3. **E** (quantitative research methods) 4. Measurement of ERM 5. ERM contributes to organisational value	**McShane and Rustambekov (2011)** 1. Measurement challenges 2. ERM and firm performance 3. **E** (quantitative: statistics) 4. Pressure to implement ERM 5. ERM, culture and firm performance	Paape and Spekle (2011) 1. Implementation challenges 2. Factors associated with 3. **E** (quantitative: 825 surveys) 4. No evidence for COSO effectiveness 5. Gaps in practice and academia
Alignment	**Powell (1992)** 1. Adoption challenges 2. Alignment - competitive advantage 3. **E** (quantitative methods) 4. Confirmatory result on alignment 5. Organisational factors	**Henderson and Venkatraman (1993)** 1. Adoption of alignment 2. Dynamic model of alignment 3. **T** (qualitative research methods) 4. Strategic Alignment Model 5. Challenges in digital transformation	**Reich and Benbasat (2000)** 1. Implementation challenges 2. Social dimension of alignment 3. **E** (qualitative: interviews) 4. Shared domain knowledge 5. Creation of IT vision	**Luftman (2000)** 1. Strategic alignment maturity 2. Achieving and sustaining alignment 3. **E** (Qualitative: 6 case study) 4. Difficulties in achieving alignment 5. Further research on alignment	**Kearns and Lederer (2000)** 1. Measurement of alignment 2. Alignment competitive advantage 3. **E** (quantitative: survey) 4. Common plan (business and IS) 5. Shared understanding
	Burn and Szeto (2000) 1. Implementation challenges 2. Business strategy driver 3. **E (**quantitative: survey, case study) 4. Competitive potential 5. Industry-specific guidelines	**Smaczny (2001)** 1. Measurement challenges 2. IT strategy aligned 3. **T** (qualitative research methods) 4. Business and IT strategies aligned 5. Test practicality of alignment	**Bergeron *et al.* (2004)** 1. Measurement challenges 2. Alignment-business performance 3. **E** (quantitative: survey) 4. Ideal patterns of alignment 5. Longitudinal study of alignment	**Sledgianowsky and Luftman (2005)** 1. Measurement challenges 2. Achieve and sustain alignment 3. **E** (Qualitative: case study) 4. Methods of implementation 5. Improve IT-business alignment	**Preston and Karahanna (2009)** 1. Measurement challenges 2. Social dimension of alignment 3. **E** (quantitative: survey) 4. Shared understanding of social alignment 5. Explore shared understanding

Table 2-9 Key academics' contributors

Source: The Researcher

Table 2-9 outlines research limitations by emphasising the main ten contributors identified on each paradigm, respectively CsM, ERM, and Alignment. Points 1, 2 and 5 (gap, key focus and projected future research) are closely linked as they are the determinants of the research questions. Point 4 (contribution) represents the intellectual heritage based on the current research development. Additionally, point 4 defines and outlines the position of the research by demonstrating the foundation of knowledge and focus, and its limitations. Furthermore, the methodological inheritage of point 3 clarifies how the original problem has been investigated and defines its limitation. It represents the research methods that have been applied in order to identify key concepts and theories. It also represents the initial guidance underpinning the research design. Although the initial questions addressed by the key contributors have contributed to the research topic, unaddressed questions still remain (CsM aligned with ERM). The remainder of unsolved issues within the literature are synthesised in point 5 of Table 2-9.

The initial research gap identified in the literature is: (1) Scarce strategic alignment literature that focuses on CsM and ERM alignment, (2) low level of maturity in the implementation of the alignment, (3) lack of bottom-up consideration of the concept, (4) lack of common terminology, (5) lack of common guidance for implementation, (6) low level of cyber risk awareness inside organisations, and (7) lack of coherent theory. Thus, the expected contribution of research confirms that the problem subject to investigation deserves serious consideration and the aspect of research credibility is sustained.

2.9 Conclusion

The challenges encountered by organisations and the way they respond to cyber threats serve as a starting point to demonstrate that alignment of CsM with ERM encounters numerous challenges in theory and practice. Moreover, the relatively scarce literature focusing specifically on the topic demonstrates confusion and unclear direction at some points. How theory and practice link together has been considered for identifying, analysing and outlining the current state-of-art research problem. Thus, the exploration of the phenomenon considers key literature in order to recognise the literature legacy related to the research' topic and uses a three-fold approach analysis based on academics', practitioners' and regulators' viewpoints. Henceforth, the main objective of the research is to create a *Framework* that comprises of CsM with ERM alignment for the financial industry and identification of key literature is one of the steps that determines and outlines the gap. Over the years, the taxonomy of risk dimension in the business context has changed dramatically from a

traditional view (negative) to opportunistic. Moreover, along with organisations' shift to the cyber environment, the risk profile has upgraded accordingly. Likewise, literature that focused on ERM has expanded across multiple industries over the years. This is true even if some critics have argued that it has not reached a maturity level since failures of organisations have been registered. The review of the literature regarding CsM has revealed that although this discipline appears to be new, its roots confirm that it previously existed under different terminology. For instance, alignment literature transitioned from a strategic alignment in general, IT alignment with business strategy and alignment of CsM with RM. The evidence of the literature review outlines that the strategic alignment of CsM with ERM is scarce in academic literature and thus transformation is to some extent theoretically sustained, but more research is necessary. Without an appropriate strategy for enterprise risks and cyber risks, it appears to be a foregone failure for organisations. Identifying how to handle risk is imperative for the reason that it has broader long-term implications. Specifically, organisations need to move from a subjective perspective (i.e. based on return-on-investment) to incorporate and assure value creation for others (economy and society). While the findings demonstrate that alignment benefits are significant in the long-term, achieving alignment can be a milestone for many organisations unless they are well prepared beforehand. Alignment processes that focus on CsM and ERM alignment within the financial organisations register a low level of maturity, and a silo approach is often applied. In addition to immaturity, a misguidance of terminology, definitions and various frameworks lead to confusion and an unclear path for organisations. Alongside inconsistencies in practice, academics lack a coherent theory that specifically addresses the alignment of CsM and ERM. Thus, the legacy is constructed on partial approaches to this research' problem.

In conclusion, evidence has shown that more research is required in order to accomplish the alignment of CsM with ERM and that choosing a single view of academics would perhaps not have tapped into the same outcome. Therefore, the literature shows that despite various efforts to increase resiliency, the approaches prove to be partially (silo) addressed. This confirms that the organisational risk oversight is under-researched and the alignment of CsM with ERM is a joint effort that contributes to a holistic internal control of risks.

The following chapter (Chapter 3) further explores the literature through a systematic literature evaluation in order to identify a more specific literature gap. The results act as a second basis (derivate) for the proposed *Framework* that follows later in Chapter 4.

3. Chapter Three: Systematic Literature Evaluation

3.1 Introduction

Chapter Three moves beyond the exploration of the phenomenon to consider further possible answers to the research questions. It examines why alignment is necessary, how it is sustained, what the key debates regarding all three domains are, and how theory, practice and regulatory framework interrelate. It assesses the literature to identify the current situation, analyse practices and evaluate potential limitations, all of which validate the proposed *Framework*. It provides an overview of ERM, CsM and alignment literature through a systematic literature review to illustrate how published research has progressed in connection to the research problem.

This stage explores the key contributing factors related to the research topic and objectives and clarifies the role of academics, practitioners and regulators that influence the governance of risk. Identifying the gap in the literature and establishing its importance are the main driving forces of this chapter, forming the baseline for the conceptual framework that follows in Chapter Four.

Despite significant research over the past few years regarding risk resiliency, there are still unanswered questions as to why organisations are unsuccessful when implementing effective security at all levels. This chapter represents an additional understanding of the research problem and undertakes a more specific exploration. While Chapter Two adopted a traditional and more general approach, this chapter narrows the investigation specifically to the financial industry, addressing the relational analysis between concepts, themes and variables (Sekran and Bougie, 2013). Hence it more deeply explores the associations among the three domains through a qualitative literature systematic evaluation which is a more comprehensive and detailed analysis than the traditional approach (Robson, 2011), using coding and categorisation of data (Sekran and Bougie, 2013). This second phase of the literature review uses a Four-Quadrant Framework to synthesise and organise data into grouped classifications (Althonayan, 2003), with the purpose of understanding the relationships of contributors and their determinations. A thematic literature evaluation has been considered for alignment (see Section 3.4.1), providing an enhanced understanding of the paradigm.

By adopting the qualitative literature systematic evaluation, the researcher aims to demonstrate the rigour, transparency, clarity and validity of methods (Robson, 2011; Booth, Papaioannou and Sutton, 2011). A qualitative systematic literature evaluation represents a:

> '…method for integrating or comparing the findings from qualitative studies. It looks for "themes" or "constructs" that lie in or across individual qualitative studies' (Grant and Booth, 2009, p. 94).

The first section explores the ERM literature, the second the CsM literature, and the third explores the alignment contributor correlations, typology and evolution.

3.2 Research model to explore the typology of contributors

For the purpose of identifying literature maturity trends, the literature is analysed based on the initial model developed by Althonayan (2003), which suggests an evaluation based on quadrants, limited by four criteria. Therefore, the following Table (Table 3-1) defines the criteria that help to categorise the gradual literature focus, along with industry proportions and global settings. The research model adopted from Althonayan (2003) applies as a direction in investigating all three domains: CsM, ERM and alignment.

Table 3-1 Research model to explore the typology of contributors

Quadrant phases	Focus	Arguments
Quadrant 1 Adoption Proposes adoption. Theoretically oriented (benefits) without applicability based on strategic discussion with the implementation purpose.	Theoretical focus -descriptive (based on past theoretical evidence); -subject to factors.	• Identifies the purpose of alignment; • Analyses and evaluate the role of alignment; • Illustrates the outcomes of alignment.
Quadrant 2 Implementation Process building (validation) pre-operational, analyses the problem and test its applicability.	Strategic and Operational focus (infrastructure and processes) -descriptive; -subjective to plans.	• Identifies the risks and effects of Implementation; • Determines the theory's applicability; • Evaluates whether the intended action can function; • Forecasts the implementation results; • Identifies preconditions of alignment; • Explores the practice.
Quadrant 3 Maturity assessment Establishes guidelines and assess them. Strategic risk oversight and implementation (tactical because it proposes to overcome challenges).	Implementation maturity focus -prescriptive (considers other factors based on practice); - process focused.	• It is based on a strategic approach; • Defines, measures and determines the enablers and impediments; • Establishes, implements and maintains the alignment; • Determines optimisation.

Quadrant 4 Assesses compliance Dynamic evaluation (strategic practice).	Valuation (assessment) focus -prescriptive; -consolidation focused.	• Debates the value of implementation; • Challenges the options available; • Tests and assesses the implementation; • Compiles and compares the results for validation.

Source: Adapted from Althonayan (2003)

- **Quadrant 1** Adoption - includes studies that considered adoption and explored its benefits, determinants, and challenges. This section is characterised by its descriptive aspects (foundation) and incorporates strategic discussions regarding ERM implementation (design). Thus, this quadrant should respond to *what and why questions*;
- **Quadrant 2** Implementation – integrates some theoretical aspects of alignment, being initially a descriptive quadrant and later grounded on the applicability of theory in practice. In short, this quadrant represents the movement from guidance towards actions. As it is the second phase, its key features are low maturity and it is characterised by convincing arguments to incorporate the strategic alignment in organisational governance. The strength of this quadrant is that it set bounds to the theory and offers practical aspects of its support role, based on cost-benefit analysis and confirmatory purposes (i.e. factors, value, profitability, performance). Additionally, it circulates positive and negative aspects, putting the theory into practice. Therefore, it has prescriptive aspects and intends to assess the pre and post implementation operational variables. This section should offer answers to *how and when questions*;
- **Quadrant 3** Maturity Assessment - is related to Q1 and Q2 but with an additional purpose. The studies categorised in this quadrant evaluate the implementational design based on strategic risk oversight by testing its tactics and performance. Additionally, this quadrant provides a movement from guidance theory to applicability in practice (actions) and answers questions about *where* the organisation stands;
- **Quadrant 4** Compliance – is a hybrid, hence it includes the adoption theories (Q1), implementation state (Q2) and maturity (Q3) and regulatory compliance (Q4). It responds to questions regarding *how much compliance*.

As a result of this direction, further analysis begins on each domain.

3.3 Enterprise Risk Management

3.3.1 Overview of academics' literature contribution to ERM

As every organisation has a duty of care to safeguard itself against various threats, ERM has become the provision for protecting assets, people, processes and organisational architectures. Based on the quadrants mentioned above (see Table 3-1) the initial exploration of literature evaluation starts by focusing on RM evolution and its impact on various industries. This enables an understanding of past approaches, and it provides some explanations for current challenges.

Table 3-2 Overview of RM literature key contributors

Author/s	Study type	Setting/ s	Industry	Research contribution	Quadrant
Crockford (1982)	T	general	generic	A descriptive study that focused on the RM evolution and its impact on businesses.	Q1
Schmit and Roth (1990)	E	USA	combined	An early study that analysed RM through a quantitative evaluation by looking at cost-effectiveness with the aim to justify further investment and research.	Q1
Smith (1995)	E	USA	combined	Investigated the practice of RM and available supportive instruments (e.g. hedge and derivates) to govern organisations.	Q1
Stulz (1996)	E	general	combined	Questioned the discrepancies between theory and practice, hence considering literature and case studies for comparison.	Q1
Oldfield and Santomero (1997)	E	general	financial	Undertook an investigation to analyse the general risk governance within the financial industry.	Q1
Clarke and Varna (1999)	T	general	generic	Emphasises the strategic role of RM implementing in organisations.	Q1
Tilman (2001)	T	general	generic	Reflected on RM´s roots and its probabilistic evolution in organisation governance.	Q1
Hillson (2002)	T	general	generic	Extended the literature legacy with its recommendation to perceive risk as an opportunity opposite to negative risk.	Q1
Raz and Hillson (2005)	T	general	general	A comparative review that focused on the analysis of RM standard practices across the globe.	Q1
Nag, Hambrick and Chen (2007)	T	USA	education	It explores multiple perspectives of academics on strategic management by looking at the definition, discussions and implications.	Q1
Jorion (2009)	T	general	generic	The study concluded that past Global Financial Crisis (GFC) lessons (2007-2008) failed to be learned as industry register discordant risk controls.	Q1
Servaes, Tamayo and Tufano (2009)	E	general	combined	The study concerns the balance of theory-practice regarding RM and undertakes an empirical study to evaluate factors that determine such situation.	Q1
Borison and Hamm (2010)	T	general	generic	It highlights the fragility of RM practices implemented by organisations and encourages a mindset change that starts with executives (top-down approach).	Q1
Chang *et al.* (2011)	E	general	banking	Provides a useful approach to Basel II Accord application in pre and post GFC.	Q2
Pirson and Turnbull (2011)	T	general	financial	Review the organisation governance state before and after the GRC and based on findings recommends a unitary network governance to diminish the effects of unforeseen risks.	Q1
Yaraghi and Langhe (2011)	T	general	generic	Emphasised the importance of identifying the critical success factors for RM.	Q1
Verbano and Venturini (2011)	T	general	generic	Reanalysed the RM development path to portray its evolution in a compelling framework.	Q2
Aebi, Sabato and Schmid (2012)	E	general	banking	This ongoing discussion presumes that employing a CRO is highly related to an organisation's performance.	Q1

Dionne (2013)	T	general	generic	The study compiles of evidence of evolution from pure RM (except financial risks) to strategic RM.	Q1
Lenssen, Dentchov and Roger (2014)	T	general	generic	It discusses the post-GFC requirement for sustainable governance to consolidate the organisational risk capacity (tolerance) through five levels: individual, sectorial, national and supranational.	Q1
Falkner and Hiebl (2014)	T	general	generic	It is an explorative and systematic review of the RM literature that focuses on SME.	Q1
Calandro (2015)	T	general	generic	The author addresses a controversial belief among academics and practitioners that proper risk preparation can transform unpredictable risks to predictable and thus preventable risks.	Q1

Source: The Researcher

Key for table 3-2:
Combined – refers to studies that use more than two industries to gather empirical data.
General – refers to studies that omit to refer to a specific setting.
Generic – relates to the industry context of studies where this aspect is omitted or has broad applicability. The attribute is generated based on the content specification, not on author/s residence.

As seen above in Table 3-2, the risk at its origins has negative connotations in perspective of RM. However, it has evolved in modern ERM by contributing to organisations' risk; in other words, by understanding in a meaningful way the risk and opportunities as a performance enhancer to support informed decisions through the lens on enterprise-wide security. Although ERM is still immature (Agarwal and Ansell, 2016; AICPA, 2018; Slagmulder and Devoldere, 2018), it provides a new strategic way to tackle various challenges and serves as a provision in commencing opportunistic risks (i.e. upside risks versus downside risks). In contrast, RM paid attention mainly to downside risks, and thus, such approach faces challenges (Slagmulder and Devoldere, 2018). Accordingly, the following table further investigates RM evolution to ERM based on quadrants specifications. It follows a similar analysis used previously in RM literature.

Table 3-3 Overview of ERM key contributors

Author/s	**Study type**	**Setting**	**Industry**	**Research contribution**	**Quadrant**
Miller (1992)	E	general	generic	Developed a risk framework to categorise risks and acknowledge the further implications of strategic decisions.	Q1
Dickinson (2001)	T	general	generic	Outline the relevance of planning process in ERM implementation.	Q1
Lienberg and Hoyt (2003)	E	USA	combined	Conducted an analysis to establish if there are any connections between the appointment of a CRO and successful implementation of ERM.	Q1
Drew and Kendrick (2005)	E	general	generic	Developed a five-pillar framework based on culture, leadership, alignment, structure and systems as a baseline for further implementation of ERM.	Q1
Nocco and Stulz (2006)	E	general	generic	Clarified the purpose and role of ERM and gave options on how implementation should be managed.	Q1
Beasley, Pagach and Warr (2008)	E	USA	combined	Sought to illustrate the cost and benefits of ERM adoption.	Q1

Castro *et al*. (2008)	T	general	generic	Recommended the inclusion of a software system (ARMISTICE) to increase the capabilities and performance of RM.	Q1
Fraser, Schoening-Thiessen and Simkins (2008)	E	USA: Canada	combined	Provided a practical perspective of ERM theory applicability by exploring the perspectives of executives in regard to ERM baseline.	Q1
Francis and Paladino (2008)	E	USA	combined	The authors proposed to identify support practices for ERM.	Q1
Power (2009)	T	general	generic	Reiterated the failures of GFC and recommended a reformation of RM in order to avoid repetition of similar events.	Q1
Lin, Wen and Yu (2012)	E	USA	insurance	Tested the potential of ERM adoption and highlighted its benefits on performance.	Q1
Griffin and Boomgaard (2013)	T	general	financial	The main role of this study was to outline the risk and return when undertaking decisions and recommended organisation-specific optimisation measures.	Q1
Tekathen and Dechow (2013)	E	Germany	manufacturing	Analysed the way organisations seek to apply alignment compared with the initial COSO model.	Q1
Hayne and Free (2014)	E	USA: Canada	combined	Outlined the contribution of COSO framework, how it is perceived, and scrutinised the adoption scale.	Q1
Gatzer and Martin (2015)	T	general	generic	Evaluated the literature to identify what are the main determinants and impact of ERM implementation.	Q1
Rubino and Vitolla (2014)	T	general	generic	Reflected on IT and ERM common governance integration by referring to COSO, ERM and COBIT framework.	Q2
Kleffner, Lee and McGannon (2003)	E	Canada	insurance	Offered a descriptive account of ERM state-of-the-art in a single industry.	Q2
Ward (2003)	T	general	generic	Addressed the issue of integrated risk management through a multi-dimensional framework by looking at six components: risk, decisions, purpose, processes, responsibilities and resources.	Q2
Beasley, Clune and Hermanson (2005)	E	USA	audit	Focused its analysis on ERM implementation and the factors associated.	Q2
Burnabi and Hass (2009)	T	general	generic	Reanalysed the COSO model applicability and viability.	Q2
Gordon, Loebs and Tseng (2009)	E	USA	combined	Questioned the relationship between ERM and performance and provided confirmatory evidence.	Q2
Arena, Arnaboldi and Azzone (2010)	E	Italy	combined	Explored the evolution of RM into ERM and analysed its implementation in practice.	Q2
Wu and Olson (2010)	E	USA	banking	Demonstrated the use of scorecards validity to support organisation.	Q2
Paape and Speklé (2012)	E	Netherlands	combined	A European perspective on potential implementation factors.	Q2
Baxter *et al*. (2013)	E	USA	financial	Paid specific attention to ERM determinants and impediments and tested whether implementation leads to organisation's goals achievement.	Q2
Lundquist (2014)	E	Nordic countries	combined	Focused on identifying which frameworks are effectively applied and implications in deploying an organisation's internal framework.	Q2
Ching and Colombo (2014)	E	Brazil	combined	Based on multiple case studies, with an output of a conceptual framework developed to describe the RM cycle.	Q2
Grace *et al*. (2015)	E	USA	insurance	Analysed efficiency regarding financial performance post implementation.	Q2
Lyons (2015)	T	general	generic	Maintained the trend within the security research and based on an oversight model of three lines of defence recommended a strategy that involves a board of directors (executives, internal assurance, tactics (applied strategy) and line management).	Q2
Rosenberg and Shuermann (2006)	T	general	banking	Accentuated the integration of risk management approach within the banking sector.	Q2
Mikes (2009)	E	USA	banking	Compared and evaluated the risk-based controls that are considered by the banking sector.	Q3
Hoyt and Lienberg (2011)	E	USA	insurance	Examined the value and determinants of prosperous ERM through economic lenses.	Q3
McShane, Nair and Rustambekov (2011)	E	USA	financial	Evaluated whether ERM underpins value.	Q3
Pagach and War (2011)	T	USA	education	It explores prior research to examine if the appointment of a CRO is among the determinants of adoption and implementing an ERM.	Q3
Eckles, Hoyt and Miller (2014)	E	USA	insurance	Circulated the positive financial aspects of ERM implementation based on a quantitative analysis of operating profits.	
Farrel and Gallagher (2014; 2019)	E	general	combined	Attempted to offer guidance on how ERM maturity should be assessed, analysing the relationship between limitations and challenges between culture and executive engagement.	Q3

Hayne and Free (2014)	E	USA: Canada	combined	Assessed the COSO's ERM impact on practices across organisations and indicated a three-dimensional dimension of the framework: disruptor, creator, and maintainer.	Q3
Nair *et al.* (2014)	E	USA	insurance	Developed a model of dynamic capabilities that sought to outline the capacity and patterns applied in the implementation phase of ERM.	Q3
Schiller and Prpich (2014)	T	general	generic	Challenged the maturity of ERM and explored its weaknesses based on conceptual and empirical evidence of prior authors.	Q3
Aven and Aven (2015)	T	general	generic	Suggested that performance and risk balance are interrelated hence the return is the organisation's goal achievement.	Q3
Beasley, Branson and Pagach (2015)	E	USA	combined	Provided valuable insight regarding the board of directors and senior management internal processes that seem associated with more mature ERM programs and the usefulness of ERM as a strategic tool for competitive advantage.	Q3
Bromiley *et al.* (2015)	T	general	generic	Suggested that more research is needed hence theoretical review indicates that advances in this area could enhance proper risk governance.	Q3
Lalitha and Nandini (2015)	E	India	IT	Analysed and evaluated the effectiveness of the relationship between ERM and businesses; considering aspects such as culture, processes, structure, training, risk governance, and performance.	Q3
Shad and Woon (2015)	T	Malaysia	generic	Formed a conceptual framework for performance measurement by considering organisational structure, governance and processes.	Q3
Zéghal and El Aoun (2016)	E	USA	banking	A content analysis study that focused on analysing annual reports to assess the effects post GRC and to identify the reactive measures.	Q3
Arnold *et al.* (2011)	E	general	combined	Accentuated the purpose of compliance during and after ERM implementation.	Q4
Lindberg and Seifert (2011)		general	insurance	Describes the assisting role of ERM for insurance industry based on Dodd-Frank Act and Data Protection Act (DPA) pre-requisites to compliance.	Q4

Source: The Researcher

Key for Table 3-3: Nordic countries (Denmark, Norway, and Finland)

Based on the above-identified key contributing authors in Table 3-3, it can be observed that focus goes further, and the quadrant categorisation enhances other aspects. Consequently, many authors have undertaken their research by firstly addressing benefits; adaptation, effectiveness, and performance being the most significantly considered (Nocco and Stulz, 2006; Nair *et al.*, 2014; McShane, Nair and Rustambekov, 2011; Gordon, Loeb and Tseng, 2009; Grace *et al.*, 2015; Zéghal and El Aoun, 2016). Secondly, the determinants of ERM implementation (value delivery, culture, appointment of a CRO, organisational strategy) are considered by Smith, 1995; Lienberg and Hoyt, 2003; Beasley, 2008; Yaraghi and Langhe, 2011; Aebi *et al*., 2012; Gatzer and Martin, 2015; Lyons, 2015; Farrel and Gallagher, 2014). Thirdly, challenges were also considered. Therefore, their analysis may have overcome the reproduction of a suboptimal level of leadership, cost, culture, alignment or adequate structure (Drew and Kendrick, 2005; Schiller and Prpich, 2014; Eckles, Hoyt and Miller, 2014). Lastly, other authors have considered exploring the ERM design choices made by organisations beyond post-implementation results (Paape and Spekle, 2012; Hayne and Free, 2014) to extract the value of implementation on long-term.

3.3.2 Overview of practitioners' contribution to ERM

The results of failures in organisations have determined an increase in interest regarding the identification of a general practice that guarantees 'security'. In turn, the purpose of standards is defined as good practice that helps to protect the organisation's objectives and add value (FERMA, 2003). The consensus appears to be that the standards aim to define unique terminology, sequences of processes and organisational structure to enhance good practices against which an organisation can guide itself.

Table 3-4 An overview of ERM key practitioners' contribution

Domain focus	Year	Issuer/ Model/Framework	Setting	Purpose	Quadrant
RM	2003	Federation of European Risk Management Association (FERMA)	UK	Incorporated a sequence of recommended processes and structure to implement and maintain RM with the purpose to add value and protect organisation's objectives.	Q2
	2009 2018	British Standard ISO 31000:2009	UK: widely applied	Provides foundation guidance on how to develop, implement and revise ERM based on a systematic process.	Q2
ERM	2003	Casualty Actuarial Society ERM Framework	USA: widely applied	Created and defined a conceptual framework that considers four types of risks: hazards, financial, operational and strategic risks. The value of the framework resides in the fact that it prescribes an analogy of steps to be followed to gain ERM value and mitigate risks.	Q2
	1992 2004 2013 2017	COSO Internal Control-Integrated Framework	USA: widely applied	An internal strategic framework that developed a systematic approach to risk control to assure the achievement and maintenance of organisational objectives.	Q2
	2006 2015	RIMS Risk Maturity Model (RMM)	USA: widely applied	A standard that includes methods, processes and practices to evaluate the ERM maturity. The purpose of this framework was to support organisations to identify their maturity level and to upgrade to a future state of business resilience.	Q3

Source: The Researcher

As can be seen from the above Table 3-4, the main standards differentiate themselves into two categories: RM and ERM. In the RM category, the standards/frameworks place themselves in the same quadrant (Q2) hence the fact they offer support for the steps required for an implementation process, which considers the initial analysis, identification, analysis, evaluation, and treatment of challenging and demanding risk. FERMA RM framework follows a similar structure of AS/NZS 4360:2004 (AS/NZS, 2004) and therefore reflects on risk through the classification perspective. Moreover, both of them have a similar structure to Casualty Actuarial Framework, which considers ERM.

To limit the analysis and avoid redundant results, similar standards to ISO 31000 as AS/NZS ISO 31000: 2009 and 2018 and its initial form AS/NZS 4360: 2004 are excluded, and thus

their main content is similar. In the case of AS/NZS 4360:2004, the standard was replaced in 2009 with AS/NZS ISO 31000, which in turn was based on ISO 31000 (British Standard Institution (BSI), 2009).

The ERM category incorporates the Casualty Actuarial Society (2003) conceptual framework that designs processes, tools, and procedures required to undertake an ERM implementation and maintenance. The framework provided a basic structure and as previously mentioned, shows similarities to AS /NZS 4360:2004 structure. Accordingly, the first three steps of the framework are identical: establish the context, identify risks and analyse risk. The AS/NZS 4360:2004 used for the fourth, fifth and sixth steps employs a different terminology but with similar responsibilities. The framework differentiates from Casualty Actuarial Framework because it considers communication and consultation as an additional yet essential approach. Nonetheless, these similarities suggest that RM and ERM standards use similar principles.

Forming part of the same category (ERM) is the Risk Management Society (RIMS) Risk Maturity Model, which is an additional tool for measuring the organisational maturity of ERM by looking at its effectiveness and efficiency (RIMS, 2015). The view that ERM maturity needs assessment it is in line with the initial conceptual framework of Luftman (2000), who offers insights into ERM maturity processes. Similarly, it is also based on five steps. Apart from creating value, the RIMS model intends to yield an understanding of organisational development against a spectrum of criteria.

Additionally, the Open Compliance and Ethics Group (OCEG, 2015) developed a GRC (Governance, RM and Compliance) Capability Model known as the "Red Book to Guide Organisations". This model outlines basic principles concerning effective risk governance. As it strives to increase the performance and transparency based on best practices, it recommends the use of a unified vocabulary, standardised procedures, and ongoing communication.

3.3.3 Overview of regulators' contribution to ERM

The regulatory contribution is essential for understanding the origins of the discipline and its advancement in relation to regulatory assistance. For example, Turnbull Guidance (Financial Reporting Council, 2005) stipulates internal control basis and assists in facilitating guidance to monitor and maintain organisational effectiveness. Likewise, the Orange Book (HM Treasury, 2004) represents one of many examples of RM regulatory

guidelines (for the public sector) with the purpose of being supportive in improving the organisation's resilient capacity. Moreover, the emphasis of management responsibility fostered by Sarbanes-Oxley Act of 2002 clarifies that decision-making executives must directly involve assuring protection of investors possessions. The Sarbanes-Oxley Act reassures deployment of calculated decisions with regard to internal controls and encourages accountability for decision-making that preserves financial investments of shareholders by its continual emphasis on performance (Bloem, van Doorn and Mittal, 2005).

More recently, the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 mandate prudential practices driven by past incidents failing to sustain economic stability and as such it requires mandatory disclosure of practices. The Dodd-Frank Wall Street Act (2010) represents an acknowledgement of scarce prudential practices, and it, therefore, requires increased measures to supervise organisations' resiliency risk practices in order to assure the financial stability of the economic system.

While most countries have industry-specific regulation, usually the Acts mentioned above influence and foster ethical behaviour, ethical organisational practices, and appropriate internal controls (processes) to safeguard loss limitations.

3.4 Cybersecurity Management

3.4.1 Overview of academics' literature contribution to CsM

The concept of cybersecurity fails to be clearly defined, and for this reason, its meanings fluctuate from covering the control of unauthorised access (Bayuk *et al*., 2012) to management function designed to protect an organisation (Kaplan, Bailey, and Rezek, 2015). Failure to identify a common definition leads to a discussion regarding the real role of cybersecurity: strategic function, operational function or technological function. Accordingly, some authors consider cybersecurity a continuing prevention, detection, and recovery (Humphreys, 2008). Although others (Gerber and Von Solms, 2001; Posthumus and Von Solms, 2004) define cybersecurity through the perspective of confidentiality, integrity and/or availability of information assets. The researcher of this paper believes the latter definition incomplete and only partially true (foundation). Even though the previous description refers to information, Bayuk *et al*. (2012) and Von Solms and Niekerk (2013) are among few authors who have identified and outlined that CsM is more than information and data security. The information represents an asset, and correspondingly cybersecurity is more than the protection of information, as it involves other assets, technology, processes

and people (Da Veiga and Eloff, 2007; Von Solms and Niekerk, 2013). On account of these three determinants (assets such as information, processes, and people), cybersecurity prompts one to re-think the traditional view of IT and incorporate tools, policies, procedures, safeguards, guidelines, certifications or technology software (Da Veiga and Eloff, 2007; Solm and Niekerk, 2013), and many other safeguards designed to mitigate risks in an integrative manner.

As a consequence, a variety of terminology and definitions in literature continue to generate confusion. The most significant confusion lies between CsM and information security (IS). Although appearing similar, they are distinct and IS refers to protection in a silo of information. This confusion leads to fragmented literature, with common definitions including confidentiality, integrity, and availability (e.g. Saleh and Alfantookh, 2011). Frequently, the terms are employed interchangeably, with identical meanings, a phenomenon described by Thompson *et al.* (2018) as being 'conflating'. As a result, clarification on what IS represents are scarce, and among the little clarification there is, the BS ISO/IEC 27000: 2016 states that IS embodies "preservation of confidentiality, integrity and availability of information" (BSI, 2016, p. 6). There may be a continuous sustenance of the traditional approach which believes that "Information Security encompasses technology, processes, and people" (Da Veiga and Eloff, 2007, p. 361). However, this approach is misguided, subjective and uninformative (Craigen, Diakun-Thibault, and Purse, 2014), with a fluctuation in its focus (e.g. information, IT or systems). Likewise, Von Solms' and Von Niekerk's (2013) study explains that literature often misguidingly uses the meanings of CsM. IS is based on data-driven security strategy while CsM incorporates IS, thereby presenting the compelling argument is that it is distinctive because it considers the management security of assets, processes and people (Von Solms and Von Niekerk, 2013).

Therefore, the cybersecurity subdivisions were initially well-known due to their technical focus (IT-centric) as frontline solutions for security. As nowadays cybersecurity has become more complex, for the purpose of this study, IT security, information security, and cybersecurity literature are reviewed based on academic resources and adopt the following definition of cybersecurity:

> "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and users' assets" (Von Solms and Van Niekerk, 2013, p. 97).

The Researcher concludes that *cybersecurity management (CsM) is a multi-faceted strategic mechanism that proactively makes use of risk controls and risk oversight functions (technical, cultural, and operational components) ingrained at all levels in order to ensure both value protection and value enhancement across an organisation; it is driven by organisational strategy and is dependent on variables such as cyberspace, people, practices, processes, assets, technology, and information.*

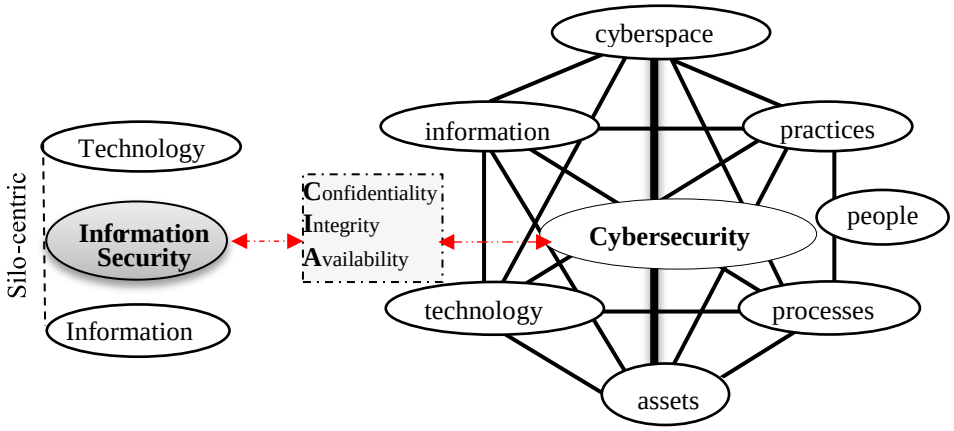


Figure 3-1 Contrast of IS Principles with Cybersecurity Principles and its Components Adapted from Althonayan and Andronache (2018)

Overall, Figure 3-1 highlights the contrast between IS and CsM, emphasising the commonality of the CIA triad and differences amongst each other's components. Despite debates regarding information security being the same as cybersecurity, there has been little agreement on what constitutes cybersecurity. Perhaps of more concern is that many organisations use a variety of terminologies, each directly effecting cybersecurity scope, derivations, meanings, and implementation. As can be seen in Figure 3-1, cybersecurity incorporates many more components for protecting an organisation. In contrast to the information security perspective, cybersecurity moves beyond internal control to incorporate the protection of IS components plus additional components such as cyberspace, people, practices, processes, and assets. Nonetheless, CsM and IS are different in scope despite being complementary and equally important.

Accordingly, the following phases have been identified as main categories based on the direction taken by literature: type 1: neutral, type 2: information security and type 3: cybersecurity inclusive. A synthesis of the cybersecurity fluctuation is highlighted below in Table 3-5.

Table 3-5 An overview of CsM literature key contributors

Domain Path	Author/s	Study type	Settings	Industry	Research contribution	Quadrant
Type 1: Neutral IT	Deibert and Rohozinski (2010)	T	general	generic	Reiterated the need for security in the realm of cyberspace along with risk dimension perception.	Q1
	Craigen, Diakun-Thibault and Purse (2014)	T	general	generic	Attempted to provide a new definition of cybersecurity by capturing an updated view of practitioners.	Q1
Type 2: ISM	Hong *et al*. (2003)	T	general	generic	The study advocated the unified theory of ISM with extended focus on several theories such as security theory, RM theory, control and auditing theory and contingency theory.	Q1
	Kotulic and Clark (2004)	T	USA	generic	Outlined the Information Security Management (ISM) effectiveness and drew attention to aspects of undertaking an empirical investigation that attempted to tackle sensitive aspects of organisation governance.	Q3
	Peppard and Ward (2004)	T	general	generic	It restates the role of IS within the business sector and discusses its main drivers.	Q1
	Posthumus and Von Solms (2004)	T	general	generic	The authors suggested the need for a model that integrates IS with organisational governance.	Q2
	Von Solms and Von Solms (2004)	T	general	generic	The authors identified ten main rules regarding IS governance plan, ideal for a successful implementation.	Q2
	Gerber and Von Solms (2005)	T	general	generic	Studied the spectrum risk evolution from RM perspectives.	Q1
	Chang and Ho (2006)	E	Taiwan	generic	Proposed to examine BS7799 (UK standard) effectiveness and determining factors that influence the completeness of implementation.	Q3
	Da Veiga and Eloff (2007)	T	general	generic	An updated ISM framework based on the analysis of previous frameworks that focus on IS culture.	Q1
	Bojanc and Jerman-Blažič (2008)	E	general	generic	Exemplified a practical and quantitative analysis to justify further investments to incorporate RM and IS.	Q3
	Humphreys (2008)	T	general	generic	Presents arguments for IS standards contribution in maintaining organisational security.	Q3
	Ma *et al*. (2009)	T	general	generic	Justifies the value of internal and external acknowledgement in control development.	Q1,2
	Siponen and Willison (2009)	T	general	generic	Highlighted that most guidelines and standards are generic and universal and in turn do not address specific organisational and security requirements.	Q1
	Tashi and Ghernouti-Hélie (2009)	T	general	generic	An overview of ISM theory that considered RM and security management as components.	Q1
	Fenz *et al*. (2013)	E	general	generic	Summarised challenges with the field of ISM.	Q1
	Singh, Gupta and Oija (2013)	E	general	combined	An exploratory study that proposed to identify the main internal factors that may impede the ISM.	Q1
	Schiavone, Garg and Summers (2014)	T	general	generic	Highlighted the adoption of organisational security based on an ontology that pertains prevention as a predictive tool.	Q1
	Web *et al*.(2014a)	T	USA	generic	Assessed the deficiencies and practice of IS using a model based on situation awareness.	Q3
	Web *et al*.(2014b)	T	USA	generic	Re-analysed the deficiencies and practices of IS based on the previous models and identifies inappropriate assessment, overestimation, and routine practices.	Q3
	Nazareth and Choi (2015)	T	general	combined	Analysed the potential of using detection tools to aid managers in undertaking security decisions.	Q1
	Soomro, Shah and Ahmed (2016)	T	general	generic	The authors believe that ISM should embed the holistic approach. The study, therefore, analysed possible factors (management participation, awareness, training, policy development) that can determine realisation.	Q1
	Julich (2012)	T	general	generic	Focused on four anti-patterns (intuition, lack of foundational security, knowledge and weak security governance) that the author claims to be the impediments of an effective CsM.	Q3
T y	Von Solms and Van Niekerk (2013)	T	general	generic	A comparison study between IS and cybersecurity terminology and evolution. The study intended to	Q1

				demonstrate that the interchangeable use of terminology is incorrectly used.	
Atoum, Otoom and Abu Ali (2014)	T	general	generic	Proposed a conceptual framework that recommends a cybersecurity implementation based on a holistic cyber security implementation framework (HCS-IF).	Q2
Mohamed (2015)	T	USA	financial	Tackled the regulatory aspects of CsM and analysed repercussions on the financial industry.	Q3
Min, Chai and Han (2015)	T	USA, EU and Japan	generic	Covered comparative aspects of public-private collaboration regarding CsM strategies.	Q1

Source: The Researcher

Apart from focusing on a specific domain (silo) or aligning with another domain, some authors have considered an analysis of internal and external factors (Ma *et al*., 2009; Singh, Gupta and Oija, 2013; Chang and Ho, 2006; Fenz *et al*., 2013). They have addressed the importance of internal factors (e.g. training, awareness, culture, audit, use of best practices, knowledge sharing or value assignment) and external factors (e.g. regulations, competitors, customers' expectations, suppliers' requirements) as necessities for developing risk control function (Ma *et al*., 2009).

Based on the literature evaluation, trends are as follows:

- phase one – neutral - refers to papers with a generic content;
- phase two – refers to an IS based perspective (an elementary view based on a silo approach to secure information);
- phase three – refers to papers that considered cybersecurity as an inclusive domain

In phase two, Gerber and Von Solms (2005) are among the first academics to analyse the shifting complexity of the risk realm. The authors suggest that risk exposure achieves another level of development, and thus consider risk exposure of intangible assets (information). As a result, the section incorporates studies that have explored the impact of cyber risks by analysing information, information systems and safeguards with strict reference. However, it must be noted that this viewpoint fails to define cybersecurity on its own since the study mainly makes direct references to information and information systems. While their research attempts to address the issue of cyber-attacks, the definition provided by the authors misleads the reader as it refers to a silo approach. The content directly refers to cybersecurity, yet it is indirectly related because it discusses a subdivision of cybersecurity (IS) and omits certain aspects such as people, assets, and processes security.

The related literature shows a variety of approaches and Da Vega's and Eloff's (2007) research is an example of a different approach (showing the value of culture) through the interaction of information, technology, processes and people.

Finally, the third phase virtually represents the complete picture of what cybersecurity underpins and indicates a pronounced significance and holistic applicability. Taking into account Julisch's (2012) research, which recognises the critical role played by cybersecurity failures, this section echoes the protection of organisations based on holistic strategy, not intuition. Overall, foundational security controls are considered and perceived as integrated.

3.4.2 Overview of practitioners' contribution to CsM

The practitioners' viewpoint is open to debate and controversial but represents the true applicability of cybersecurity, paying attention to guidelines, policies and standards yielded from past lessons. It also portrays the state of cybersecurity based on a general practitioner's perspective (Ponemon Institute, 2013).

Standards are present predominantly in order to provide assurance and protection, as well as an organisational structure, resilience, and a continuity and recovery plan in case of an incident (BS ISO 27003:2010). Guidance is not mandatory but usually represents the expected practices in regard to risk oversight.

Cybersecurity's *insecurity* for organisations is challenging, and a report from the Ponemon Institute (2013) confirms that cybersecurity needs serious consideration as its occurrence and sophistication have increased. Another contribution of this report is that it cites a low adoption of cybersecurity management (31%) in 2013. This suggests that the remaining percentage can be divided into two possible categories: 1) some of the organisations created in-house capabilities (perhaps due to premium fees if such service was contracted) and 2) some organisations denied the cybersecurity threats.

Likewise, Ernst and Young's (2014a) report recognised the critical role of cybersecurity and updated the initial hypothesis that some organisations deny its challenges. By adding up-to-date information that showed an increased level of awareness (79%) of respondents acknowledged an increased level of threats), the survey confirmed a general knowledge of the threat. However, clear rates of adopted preventative measures were not addressed. Recognising that a cybersecurity incident has an unforeseen aspect because it is based on an opportunistic criminal mindset, the Ernst and Young survey's contribution lies in the fact that it emphasises aspects as the importance of executive awareness in dealing with cybersecurity attacks, organisational preparation as well as adequate investments to sustain achievement of cybersecurity maturity.

Furthermore, the data generated by literature evaluation regarding industry practice is reported in Table 3-6.

Table 3-6 An overview of practitioners' key frameworks and guidelines

Domain focus	Year	Framework		Setting and industry	Purpose	Quadrant
IT	2012	COBIT 5 for IS		Widely used	Emphasised a strategic integration of IT and organisation security by focusing on the governance and management of risks.	Q2
IS	2004	ISSA Generally Accepted Information Security Principles and (GAISP) and IT Security RM Framework		USA	This initiative had the purpose of developing a common practice for IS and ingrain awareness of security in organisations.	Q1
	Octave	1999	Octave	USA	Facilitated a continuous measurement, assessment and mitigation of risks related to information security.	Q3
		2003	Octave -S	USA	Developed a methodology addressed to small organisations to help them to address risks.	
		2007	Octave Allegro	USA	It focused mainly of information assets and developed a method to assess operational risks.	
	2013	IASME		UK	The standard is in line with ISO 27001 and aims to support certification for information assurance in SME.	Q3
	BS ISO series	2010 2014 2016 2017	ISO/IEC 27000	Widely used	Informative guidance in regard to vocabulary and baseline information used on ISO series implementations.	Q2
		2005 2013 2017	ISO 27001	Widely used	It illustrates the requirement for a security framework establishment and maintainers.	Q2
		2013 2017	ISO 27002	Widely used	An operational standard that refers to the selection process of security controls.	Q2
		2010 2017	ISO 27003	Widely used	It sustains the initial actions of the previous series (27000, 27001 and 27002) and provides guidance on establishing the planning processes for implementation.	Q2
		2009 2016	ISO 27004	Widely used	It introduces the concept of measuring the effectiveness of ISO standard implementation.	Q3
		2011 2018	ISO/IEC 27005 (BSI, 2011a)	Widely used	It concentrates on the control by using IS management techniques and introduce the RM techniques.	Q2
		2012	ISO/IEC 27015	Widely used	A supplement that is meant to guide financial services and insurance organisation to implement and adapt to ISO/IEC 27001 and 27002.	Q2
		2012	ISO/IEC 27032	Widely used	The standard represents a technical guidance for information sharing, coordination and incident handling.	Q2
	2011	ISF Standard of Good Practice		Widely used	A security model that recommends good practice in IS to enhance alignment between security and organisation strategies.	Q2
	NIST series	2011	SP800-39 (manage)	USA based: widely use	It ensures integration of IS in RM practices to manage organisational risks.	Q2
		2013	SP800-53 (select)	USA based: widely use	Assisted IS to support selection and implementation of security controls to protect operations.	Q2
		2010	SP 800-53a (assess)	USA based: widely use	It verifies the implementation of RMF and is a guide to identify if the organisation achieved the goals and objectives.	Q3

	2011	ICAS Information Security Framework	UK	Assessment of security controls for data protection. It also ensures organisation security control and policies compliance.	Q3
	2014 2015	KPMG's Global Cyber Maturity framework	Widely used	Promotes a proactive approach of executives' involvement. Mainly focused on maturity assessment in the context of information security and RM.	Q3
	2014	EY' Cyber program management (CPM) framework	UK	Assessed the information programs structures.	Q3
	2016	Grant Thornton's Cyber Risk Management Program	Widely used	It proposes a cyber risk strategy alignment with business strategy in the context of performance achievement.	Q1
CsM	2013	PAS 555	UK	It incorporates governance, and management principles to recommend baseline security by using the strategic and operational approach.	Q2
	2014	NIST Risk Management Framework (RMF)	USA based: widely used	Proposed to guide organisations in related cyberspace activities, emphasising cybersecurity governance. Its objective is to align CsM with RM (operational and strategic).	Q2

Source: The Researcher

Based on the above structure, the following section outlines and formulates an overview of the standards. However, benefits of applicability are discussed further in Subsection 4.3.3, Chapter Four.

3.4.2.1 Stage trends in the practice of CsM

- Phase 1: Information security and business focus

The structure of Operationally Critical Threat, Assets, and Vulnerability Evaluation Framework (OCTAVE) is based on technical aspects of IS risks and was released by the Software Engineering Institute (Caralli *et al*., 2007). The framework was initially published in 1999, but it has subsequently undergone five more updates. The basics of the framework are structured in three steps: profile assessment, measurement, and mitigation. It encompasses asset identification (their critical value) and vulnerabilities measurement to determine potential losses.

The downside of the framework is that it addressed and underpinned operational and technical control perspectives to generate resilience and assess information security risk through a silo perspective (information) even though it considered the security implication of people, facilities, and technology. The approach of this framework predominantly depends on the CIA triad (confidentiality, integrity, and availability) principles.

Standard of Good Practices for Information Security (ISF, 2011) is another security model that considers the alignment of security with organisational strategy. It accentuates an enhancement of controls and a means of developing alignment to evaluate the effectiveness of the process. Moreover, it focuses on coordinating activities, supporting their achievement

and finally measuring output. Drafted in 2011 by Information Security Forum, the content of the framework defines good practices and foundation of information security. This international standard is aligned with many practitioners and regulatory practices as ISO series, Cobit, Basel and Sarbanes-Oxley Act (2002, USA), among many others.

Generally Accepted Information Security Principles (GAISP) represents an initiative of Information Systems Security Association (2004) that proposed to compile a unifying principle to motivate an increased control of risk. In addition to its initial recommendation, the GAISP gave rise to an IT Security RM Framework that highlights basic practices as asset identification, threat identification, vulnerability identification, impact assessment, and safeguarding and risk mitigation principles. Accordingly, the guideline disseminates these processes as a means of defining boundaries of analysis and the rationale for transparency of processes.

- Phase 2: Information Security and RM focus

A key limitation of this approach is that it considers the security of information assets and omits to consider all parts involved holistically. It also discusses the alignment from the perspective of RM and does not address the problem of the silo approach to risk oversight. One of the main standards that are part of this category is Cobit 5, which was released by ISACA (Information Systems Audit and Control Association). It was initially developed as an IT and business-centric framework and saw updates in 2003 regarding cybersecurity and RM uniform governance. Besides being viewed as a strategy that enhances the movement from micro governance to the macro governance of risks, the merit of the framework lies in the fact that it supports compliance and facilitates a holistic management.

However, it must be argued that a downside of this framework is the IT-centric approach under RM. In particular, an enterprise-wide strategic approach is not forthcoming since its focus is technical, operational, and managerial control instead of strategic.

Given these points, another component is the ISO series, which was initially published as BS7799 in 1999, subsequently transformed into ISO series in 2002, and incorporates many other versions. ISO/IEC 27000:2016, 2017 (BSI, 2016a; BSI, 2017b) defines its strategy as an information security management system (ISMS) and assesses risk, applies risk treatment, and aims to leave small residual risk (the difference between risk threats, minus counteraction).

ISO/IEC 27000 standard contains an approach for risk treatment. The recommended action to risk exposure is its identification and treatment through modification, retention, avoidance and/or sharing techniques (BSI, 2016a; BSI, 2017b).

BS ISO/IEC 27001 define the requirement for establishment and maintenance being a starting action point. As such, further steps are addressed by BS ISO/IEC 27002, providing details on how security control tools as policies (management directions), processes, procedures, organisational structure, and software and hardware functions can all contribute to successful implementation.

ISO/IEC 27005:2011, 2018 (BSI, 2011a; BSI, 2018c) is another framework with a strategic approach under the RM umbrella, and its main function is to identify, analyse and evaluate risk. Likewise, ISO/IEC27032:2012 (BSI, 2012) is a technical guidance on how to react to cyber risks and considers other standards. Although this standard has a low rate of implementation in comparison to ISO/IEC 27000, its merit is that it guides the organisation on how to technically prepare itself (BSI, 2012).

ISO framework series is complex and in general starts by defining terminologies in order to avoid misinterpretations. Although its series has registered fluctuation from technical to strategic approaches, it is one of the most recognised standards in the UK. In contrast, its disadvantage is that its main function is to secure information and systems, but it fails to address other aspects of cybersecurity such as protection of cyberspace, people, practices, processes, assets, technology and information. It can, therefore, be considered a traditional approach to information security.

Further research on CsM and RM is continued by the ICAS Information Security framework published by The International Association of Accountants and Technology Consultants (IAAITC) and encompasses the recommendations of Data Protection Act, UK (DPA). Generally, this risk framework appears to be voluntary. However, in reality, it represents a legal responsibility addressed to all businesses and such omissions constitute a lack of due care (IAAITC, 2012). The framework ICAS Information Security provides a useful approach for small organisations (less than 500 employees) to assess IS risks. It covers just one of DPA's requirements, respectively the assessment. Hence, the framework is specific, and its purpose is to verify and ensure that organisations comply with DPA requirements. The framework represents an initial step to deploy a risk control mechanism. Thus, one of the most significant contributions of this framework is that it emphasises risk profiling and asset

identification before moving on to security controls and policies. The downturn is that it has a silo perspective and despite acknowledging the security implication of assets, it only considers information security risks. The framework claims to be compatible with other industry frameworks, and its theory is based on OCTAVE2 principles. Although essential, the assessment step is insufficient and incomplete as a comprehensive strategy hence it only addresses the assessment. Therefore, many other aspects need to be considered in order to deploy better security. As a result, the framework omits the adoption of a holistic approach to risk, and this method requires additional framework mixture.

Additionally, IASME Standard for Information Assurance intends to provide support for organisations, which due to their size and financial constraints are unable to implement standards that are more appropriate for large organisations (e.g. ISO, NIST, Cobit). Apart from focusing on ensuring the confidentiality, availability and authenticity of information, a differentiated point of this framework is that it considers physical security. Apart from supporting an organisation in becoming compliant, it also suggests methods that can be used to measure the security maturity of an organisation.

- Phase 3: CsM and RM

The previous sections have shown that some standards addressability is incomplete. Although this section adopts a similar approach, its merits lie in the fact that it addresses a partial solution (CsM). Even if it refers to RM domain, it omits to discuss alignment and thus responds only partially to the aims of this research.

Risk Management Framework (NIST, 2014) has been developed based on an official stance to cyber risk (USA Government) and incorporates industry and governmental collaboration. Therefore, it has been constructed on the premises of global research, standards, guidelines and practices (NIST, 2014). Its main purpose is to offer guidance for the protection of critical infrastructures. The solution proposed by this standard is based on documented terminology and on five functions: identify, protect, detect, respond, and recover. The advantage of this framework is that even though it appears to be voluntary, it sets the tone for organisations and prevails as the basic principle of cyber hygiene in the USA (maintain a safe environment) also continued in other NIST 800 series. The negative feature of this framework is firstly, the omission to evaluate the current state of an organisation as it moves straight to risk, threats, and vulnerabilities identification. Secondly, it focuses on predictable risks and fails to consider hazards or ‘black swans’ (unpredictable events). Lastly, despite underpinning the RM perspective, it appears to be more concerned with operational aspects. Formulating the

benefits of CsM and RM applicability provides the overview of security governance and management specifications and thus PAS 555: 2013 (BIS, 2013); it proposes to provide a framework with these considerations. Although the initiative was sponsored by industry organisations, the standard is under the license of the British Standard Institution (BSI). The holistic approach takes into consideration internal and external factors (i.e. third-party strategy regarding security). Moreover, it incorporates the strategic, operational and technical approach. The drawback, however, is that although it should clearly define the implementation of the standards, the structure of the standard leaves decisions up to organisations, hence offering a multitude of options to respond to risks might mislead organisations.

- Phase 4: CsM and ERM (scarce evidence)

The analysis of documents regarding CsM and ERM indicates a scarcity of documents that consider both domains in an in-depth way. Consequently, similar approaches are considered (phase 1, 2 and 3) in order to address this issue and to identify insights and recommendations for completing the objectives of this research. Further research is desirable to develop existing knowledge and as thus Grant Thornton's (2016) Cyber Risk Management Framework is designated to organising the various factors and considers business enabler as strategy, leadership, regulations, resources, and ERM as a whole. Nonetheless, it fails to grasp separation on internal and external variables. It also offers a descriptive account of elements involved in governance (assets, processes and technology). Despite the fact that it claims to refer to cybersecurity, it promotes good practices for alignment in IT security. Another gap identified is that while it proposes to be a strategic framework with some technical reference (IT-centric), it omits stipulating how it should be leveraged. In bridging the framework's gap, this particular framework is used to outline that the industry partially understands the research problem. It proposes a better preparation and alignment of IT (even if it claims to be cybersecurity) and ERM practices. This framework prompts a re-think about alignment and suggests effects of a holistic approach yet does not provide ample support for the assertion of cybersecurity alignment to ERM. The researcher argues that it represents a good starting point to address the benefits and value creation while value protection requests additional research.

3.4.3 Overview of regulators' contribution to CsM

Legal and regulatory requirements require diligent compliance with legislation. As mentioned previously, the financial industry has additional requirements with regards risk

oversight. Although fulfilling legal requirements is sometimes less supervised in other industries (often supervised on a voluntary basis), in the case of financial industry compliance it is double-sighted, and consequently, both ERM and CsM are mandatory even though they often overlap (i.e. mandatory ERM requirements, Whitman, 2015). In the case of CsM, the recent new regulation of New York State Department of Financial Services (2017) demands financial organisations implement a cybersecurity program and to report findings annually. This reporting is thought to contribute towards an understanding of organisation risk oversight maturity within the financial industry.

Given the fact that the cornerstone of risk oversight is based on the CIA triad (FISMA, 2002) and shaped by expected characteristics (ISSA, 2004), it is generally accepted that regulatory constraints are based on the accountability of compliance and litigations. Accountability is based upon an accepted responsibility among all parties and in turn an actively preventative action regarding insecurity (e.g. responsibility for access and usage of organisational premises and systems), as opposed to a reactive action that takes place after an event has happened (ISSA, 2004). This is a basic ethical principle that, along with the duty of care, should form part of an organisation's strategy. Organisations tend to exploit the potential of technological opportunities thus a more pragmatic approach to effectively mitigating risks has become more necessary. To reach their goal, regulators are empowered with increased capabilities and intend to equip organisations with minimum preparation, although accountable in actions (voluntary or imposed).

Awareness principle (standards, conventions, mechanisms) - assists achievement and education. It is the expected acknowledgement of baselines, procedures, guidelines, policies and responsibilities among all relevant parties. Awareness might include, for instance, the skills for understanding the techniques, tactics and tools necessary to comprehend threats; for example, employees qualification might include mandatory competencies and recommended training to enhance better preparation (ISSA, 2004).

Improved security strategies such as '10 Steps to Cyber Security' from CESG, Cabinet Office, CPNI and Department for Business, Innovation and Skills (UK 2012) are required to provide basic support to organisations so they can protect themselves in cyberspace interaction. Since its publication, the guidance has reinforced the effects of cybersecurity accountability (organisation duty of care). Hence, it encourages vigilance and awareness.

To emphasise CsM accountability and compliance requirements, it should be noted that the safeguard measures and awareness (due diligence) of an organisation are a legal

responsibility and any misalignment could result in liability disputes (fines, penalties, cyber costs) should negligence be proven. Most experts believe that the problem of cybersecurity has not been addressed appropriately due to the velocity of technology development whereas others believe that before analysing the options available, serious consideration should evaluate regulators' recommendations and duty of care assessment results. Accordingly, innovation in security practices in collaboration with the industry is encouraged (e.g. UK cybersecurity strategy).

A lack of common regulation for the financial industry underpins multiple challenges such as USA regulation tends to transform from voluntary self-regulation to enforced self-regulation (Min, Chai, and Han, 2015), a fact that contradicts an organisation's policies; for instance, a financial institution from the USA that follows a policy under the strict perspective recommended by the government (i.e. NIST recommended by the USA Government). Whereas, a financial institution from the EU uses regulatory guidance more as a consultative paper. The trend in cybersecurity regulation from different countries requires an additional effort for organisations. Thus, liability and responsibility may have various levels if dispersed geographically in jurisdictions (Mohammed, 2015); a fact that leads to poor enforcement, confusion, and overlaps in the efforts made by organisations with global operations. As a result, risk-taking deficiencies have different layers according to each country, and this affects residual risk (the risk that remains after implementing safeguards); while inherent risk, it mainly refers to a situation where organisations take no action towards risk (Antonucci, 2017). Cybercrime does not recognise countries' borders and frontiers, and accordingly Acts, guidance and any preventative measure should not. Denoting such perspective, an initiative such as those provided by Table 3-7 synthesis, brings insights of mandatory and voluntary aspects.

Table 3-7 An overview of regulators contributors to CsM

Document type	Year	Document	Settings	Purpose	Quadrant	Domain type
Frameworks	2015	CESG Cyber Security Model	UK	It provides a common framework to enable and assess Information Assurance (IA) maturity.	Q4	IA
	2014	HMG Security Policy Framework	UK	Represents an official statement of general security policies and procedures undertaken by HM Government that can be used as a point of reference for organisations to develop their policies.	Q2	IS

Source: The Researcher

Table 3-7 illustrates the scarcity of regulatory frameworks. HMG Security Policy Framework represents an example of security policies related to IS and its implementation. A more satisfying approach seems to be in CESG Cyber Security Model that incorporates Information Assurance Maturity Model (IAMM) and Information Assurance Framework (IAAF) and addresses the expected measures required to assure the security of information and assess the level of measures undertaken. The CESG Cyber Security Model has almost identical criteria for measuring the organisational maturity to that provided in the initial model developed by Luftman (2000). To ensure its validity, the model is aligned with RM practices of BS ISO/IEC 27001:2005. Additionally, CESG makes an indirect recognition by aligning to BS ISO/IEC 27001, which in turn refers to IS and respectively information assurance. Firstly, it employs two models, which each focus on information assurance. Secondly, it uses cybersecurity terminology for its frameworks. Both these features demonstrate that the industry is using terminology without clear correlation and in an inappropriate way, and thus confusing IS/IA (data assurance/security) with cybersecurity (security of people, processes, and assets). Overall, the findings suggest that these two frameworks demonstrate that the regulatory literature of CsM is dominated by informative (rather than practical) guidance.

3.5 Strategic alignment

Studies focusing on alignment are prominent in literature and have been researched from many different perspectives (IT, RM, CsM), focusing on a variety of dimensions (e.g. social, strategic, structural or cultural dimension). For the purpose of this research, the main dimension considered is strategic. However, some aspects of the remaining dimensions are discussed because they represent a contribution to the alignment theory and in turn interrelate with strategic alignment dimension.

Alignment concerns the establishment of a common structure for processes that involves all resources for the common objective of achieving the organisation's mission, strategy, objectives, and plans. In short, Pitt and Koufopoulos describe alignment as a "…pattern or plan that integrates an organisation's major goals, policies and actions sequences into a cohesive whole" (Pitt and Koufopoulos, 2012, pp. 6). Nonetheless, alignment literature abounds with examples that significantly focus on IT and Information Security (IS). This suggests that cybersecurity (for example, IS) is still seen as a part of IT. For example, Saleh and Alfantookh (2011) are among some authors that demonstrate the benefits of IT/IS alignment with RM but fail to acknowledge that is alignment.

Regarding the focus of prior research, it can be observed that abundant studies were investigating how to achieve alignment in general terms, by looking at advantages and unique factors regarding specific cases (e.g. communication, competence, governance, partnership, capabilities, planning, industry, size, culture, skills) (Huang and Hu, 2007; Avison *et al.*, 2004; Chan *et al.*, 2006; Reich and Benbasat, 2000; Wu *et al.*, 2015). While the advantages and factors represent the theoretical argument (descriptive) for achieving the alignment, other authors undertook a deep analysis and scrutinised the cost-benefit (Womer *et al.*, 2006), consequence of performance of alignment, its impact on organisational governance, and possible means to maintain and develop alignment maturity (practical).
The next section comprises of a synthesis of alignment literature separated in four domains: neutral, IT and business, IS and RM, and IS and ERM, and the categorisation have the purpose of exemplifying the domains consideration of academics along the years.

Table 3-8 An overview of literature key contributors to alignment

Domain Path	Author/s	Study type	Settings	Industry	Research contribution	Quadrant
Neutral	Powell (1992)	T	USA	generic	Outlined that alignment is enhanced by the organisational factors that lead to competitive advantages.	Q1
	Walter *et al. (*2013)	E	USA	education	Examined and validated the performance based on alignment	Q1
IT: business	Baets (1992)	E	Europe	banking	Analysed the practical perspective of successful alignment and developed a Strategic Alignment Process Model.	Q1
	Broadbent and Weill (1993)	E	Australia	generic	Explored practices regarding alignment.	Q1
	Henderson and Venkatraman (1993)	T	USA	generic	Delimited the benefits of alignment through the SAM model.	Q1
	Venkatraman, Henderson and Oldach (1993)	T	USA	Insurance and manufacturing	Evaluated the management implications of alignment and developed the Continuous Strategic Model.	Q2
	Baets (1996)	E	USA: Europe	banking	Identified a discrepancy between theory and practice and developed a Strategic Alignment Model.	Q1
	Ciborra (1997)	E	USA	manufacturing	It investigates the alignment evolution.	Q1
	Luftman, Papp and Brier (1999)	E	USA	combined	Examined the enablers and inhibitors in aligning the IT plans and business plans.	Q2
	Papp (1999)	E	USA	combined	Analysed whether alignment could improve productivity.	Q4
	Burn and Szeto (2000)	E	Hong Kong	chemical and manufacturing	Quantitatively analyse on IT and business alignment perspective.	Q3
	Kearns and Lederer (2000)	E	USA	combined	Addressed the issue of reciprocal plan alignment.	Q2
	Reich and Benbasat (2000)	E	Canada	insurance	Examined the social dimension of alignment and developed: Social Dimension Model.	Q2
	Luftman (2000)	E	USA	combined	Discussed how alignment could be achieved and measured its maturity through SAMM.	Q3
	Smaczny (2001)	T	Australia	combined	Validated the applicability of SAM model.	Q1
	Chan (2002)	E	USA	combined	Assessed the alignment preconditions.	Q2
	Cragg, King and Hussin (2002)	E	UK	manufacturing	Explored how alignment can be measured.	Q3

	Bergeron, Raymond and Rivard (2004)	E	Canada	manufacturing	Evaluated the co-alignment patterns to identify the performance rate. The strategic alignment is limited to strategy and structure, without security considerations.	Q2
	Avison *et al*. (2004**)**	E	Australia	finance	Developed an alignment assessment tool.	Q2
	Campbell, Kay and Avison (2005)	E	Australia	generic	Considered the social and strategic (intellectual) dimension of alignment and developed the alignment diagram.	Q1
	Sledgianovsky and Luftman (2005)	E	USA	chemical	Validated the SAM model in the chemical industry.	Q2
	Chan, Sabherwal and Thatcher (2006)	E	USA: Canada	combined	Examined strategic impediments in alignment.	Q2
	Chan and Reich (2007)	T	Canada	hospitality	Examined antecedents of alignment.	Q1
	Huang and Hu (2007)	E	USA	biopharmaceutical	Explored alignment through balanced scorecards tool.	Q3
	De Haes and Van Grembergen (2009)	T	Belgium	combined	Developed a basic model to implement the alignment.	Q2
	Luftman and Kempaiah (2007)	E	general	combined	Updated and validated the initial SAMM.	Q3
	Gutierrez, Orozco and Serrano (2009)	E	general	combined	Validated SAM alignment model can be applied to SME.	Q3
	Preston and Karahanna (2009)	E	USA	healthcare	Illustrated the role of shared understanding in strategic alignment through a shared understanding model.	Q1
	Taradfar and Qrunfleh (2009)	E	USA	combined	Explored the tactical aspects of alignment.	Q1
	Chen (2010)	E	China	combined	Developed a tool to measure the alignment maturity in China.	Q3
	Johnson and Lederer (2010)	E	USA	combined	Demonstrated that mutual understanding plays a significant role in alignment.	Q2
	Corsaru and Snehota (2011)	E	Switzerland	ICT	Evaluated alignment evolution and implementation.	Q2
	Charoensuk, Wongsurawat and Khang (2014)	E	Thailand	hospitality	Extended Henderson's and Venkatraman's model by analysing the strategic and operational alignment. It developed Business Information Technology Alignment model.	Q3
	Mekawy, AlSabbagh and Kowalsky (2014)	E	Middle East: USA	insurance	Analysed the potential of business-IT alignment with a strategic, tactical and operational focus.	Q3
	Coltman *et al*. (2015)	T	general	generic	Outlined antecedents and consequences of alignment between business and IT - empirical evidence that reveals positive effects of alignment on business performance.	Q1
	Gerow, Thatcher and Grover (2015)	E	USA	generic	Developed an analysis based on prior work and identified six dimensions of alignment.	Q3
	Hinkelman *et al. (*2015)	T	general	generic	Increasing demands for optimisation for sustainability purposes.	Q3
	Reynolds and Yetton (2015)	E	USA	banking	Carried out analysis based on functional, structural and dynamic alignment.	Q3
	Wu, Straub and Liang (2015)	E	Taiwan	generic	Examined the effectiveness of alignment on IT governance.	Q2
	Lutman, Lyytinen and ben Zvi (2015)	E	general	generic	Updated and validated the SAM model.	Q3
	Karpovsky and Galliers (2015)	T	general	generic	Explored the historical evolution of alignment literature.	Q1
IS: RM	Saleh and Alfantookh (2011)	T	general	generic	It considers a structural and operational dimension to support the IS management functions, together with RM guidelines to improve an organisational security capability.	Q1 Q2
IS: ERM	Rahman and Donahue (2010)	T	general	generic	This study makes a recommendation on applying the convergent strategy.	Q1
	Fakhri, Fahiman and Ibrahim (2015)	T	general	generic	Explored the strategic governance role.	Q1

Source: The Researcher

Table 3-8 provides an overview of the research interest in the paradigm of alignment which is prevalently considered by academics at the detriment of practitioners or regulators. Beyond this aspect, the literature ought to consider the alignment of CsM with ERM hence it is often seen only as a partial side of the issue through silo perspective of IT, RM or ERM in the detriment of compiling an enterprise-wide approach.

Moreover, the literature identified is scarce within the context of the financial industry, a fact the reiterates once more the value of this research.

3.5.1 Trends in the literature of alignment

The identified literature is thematically categorised by its focus on neutral alignment, IT business alignment, IS and RM alignment and IS and ERM alignment (similar to ERM and CsM literature analysis).

- Neutral alignment

Powel (1992) undertakes his investigation based on business standpoints and refers to the alignment of departments for scope, competencies and governance. As an isolated approach, it evaluates competitive advantages and performance.

- IT: Business alignment

The work of Henderson and Venkatraman (1993) indicates the role of aligning the strategy, organisation infrastructure and processes to increase capabilities through the SAM model (Strategic Alignment Model). Many other researchers later applied this model's contribution and further developed it to analyse the alignment implementation.

Some researchers like Burn and Szeto (2000) and Johnson and Lederer (2010) analysed the alignment based on primary data, investigating whether the mutual consideration of CEO and CIO (organisational executives) could underpin an adequate alignment between IT and enterprise. Their results suggest that mutual understanding can contribute towards some dimensions of alignment. Although their results represent a conceptual and initial validation of alignment importance, some studies have further advanced this investigation and shown the benefits of applying the alignment to SME (small, medium enterprises). Additionally, the research of Campbell, Kay, and Avison (2005) emphasises the IT practitioner's perspective, which provides a useful appraisal of alignment challenges through a social and intellectual dimension. Likewise, Chan (2002), advances the hypothesis that in practice the alignment implementation is preconditioned by the social interaction of staff due to the informal structure of some organisations. Accordingly, the author sustains that despite the

theoretical framework, a significant role in implementation is how the human side perform due to flexibility and informal procedures.

Additionally, the values, attitudes and beliefs delimitate the cultural dimension. Chan and Reich (2007) carried out their investigation and reported that alignment could have many levels of implementation; for example, organisational, project level or individual level. The IT business alignment seems to be the most considered strategy hence this research has identified most journals dedicated to this section whereas other sections were scarce.

- IS and RM alignment

Subsequent studies of Saleh and Alfantookh (2011) constructed a framework through STOPE perspective (strategy, technology, organisation, people, and environment) based on IS and RM theory. A key aspect of this framework is that although it does not make use of alignment terminology, it takes into consideration an integration of both theories (IS and RM) in order to establish a favourable and safe environment for business. The framework provides a useful account regarding how RM perspective together with IS can enhance better governance. The main disadvantage of the framework is that the framework focuses more on IT infrastructure and physical threat. However, despite its initial focus on IS, the framework fails to respond to cyber risks as its falls short of being directed to another aspect of the structural and procedural dimension of physical security. Along with RM perspective contribution, the framework indicates that a combination/integration of two-silo governance can have a significant impact on risk reduction.

On these grounds, Fakhri, Fahimah and Ibrahim (2015) indicate that alignment continues to be a challenge. One of the most distinguished aspects of this research is that it highlights the benefits of the alignment. While the study proposed achieving an alignment between IS and business strategy, the content omits the cyber aspects and similarly with Saleh and Alfantookh (2011) redirects its focus on physical security incidents, physical security, or employee's security. The study's findings demonstrate that the proposed study aims were not met. However, the authors do succeed in identifying some possible advantages associated with alignment. Saleh and Alfantookh (2011) tackle the safeness of organisations and propose a unified process based on common processes and tools.

- IS and ERM alignment

Furthermore, Rahman and Donahue (2010) are among few authors who debate that information security represents the security of data, information or metadata (a large amount

of data) and the information systems involved. Moreover, the authors evaluate the challenges and benefits of alignment and understand their wide applicability among organisations.

The basic premises of this level are also evidenced by Campbell, Kay and Avison (2005) who analyse the practitioners' approach in regard to alignment, and their findings outline that the organisation's culture plays a major role in the process.

3.5.2 Typology trends of alignment

Moving from literature levels evolution, the literature shows another categorisation based on typology. Based on the initial quadrant categorisation (Althonayan, 2003) as discussed at the beginning of this chapter, the section that follows explain in detail the typology categorisation of alignment:

- Quadrant 1 (Adoption) refers to studies that champion alignment adoption. For example, the theoretical contribution of Powel's (1992) study lies in the fact that it supports alignment definitions, offers insight into how this can be achieved and prompts a reconsideration of achieving and maintaining an initial maturity level. The studies that are classified in this quadrant thrive in motivating the adoption of alignment and question why this step should be taken. It also raises the argument that an organisation can gain benefits (Powel, 1992) as a competitive advantage (performance or cost), which reflect in strategy change.
- Quadrant 2 (Implementation) refers to studies that discuss alignment implementation. As an example of Quadrant 2, Reich and Benbasat (2000) analysed the determinants of alignment based on certain factors (enablers and inhibitors). Other authors have focused explicitly on individual determinants such as communication, value (Venkatraman, Henderson, and Oldach,1993) governance, partnerships architecture, skills, and/or performance (Baets, 1999; Chan, 2002; Bergeron, Raymond, and Rivard, 2004).
- Quadrant 3 (Maturity Assessment) incorporates studies that explored the implementation dimension of alignment. One clear example is the study of Hinkelman *et al*. (2015), which demonstrates how past approaches can be optimised (tailored) and applied to the current challenges in order to increase capabilities and reaction (agility).
- Quadrant 4 (Compliance) comprises of an in-depth focus on alignment assessment and analyses its role, impact, and discrepancies. This category even took into

consideration some aspects of quantitative methods to measure alignment while the main studies are based on qualitative analysis and thus address the theoretical legacy and develop new models that assess the maturity based on criteria.

Baets (1996) argues the impact of alignment can also be measured by a quantitative method. Findings indicate that there are many discrepancies in practice for applying the theory. Consequently, the human factor and lack of awareness play a significant role in the alignment process (Kerstin, Simone and Nicole, 2014). The study of Luftman (2000) illustrates how alignment can be achieved and assessed using level maturity criteria. Smaczny (2001) used the SAM model of Henderson and Venkatraman (1991) to test its veracity and validity and found that its model is applicable even though alignment proved to be at a conceptual stage.

3.6 Limitations overview and research problem (gap)

Based on the literature assessment, the first section illustrates an overview of findings, materialised in a quadrant categorisation of the literature review. Thus, the preliminary results indicate that there are four domains which register fluctuations. The findings from quadrants categorisation have a number of possible limitations. Namely, for analysis only, 169 from a total of 312 documents are considered (see Table 2-9, Chapter 2) because only academics' papers were considered. This method was carried out due to the relevance of papers. For a visual representation, the following (Figure 3-2) shows the evolution of focus in the academic literature.

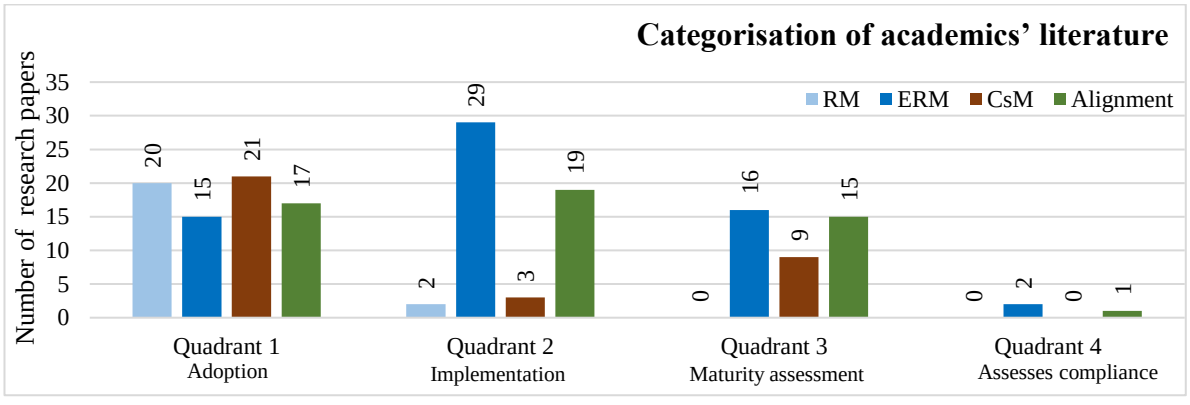


Figure 3-2 Quadrant categorisation of academics' literature

Source: The Researcher

As Figure 3-2 shows, there is a significant difference among research evolution of academics. The most predominant domain is RM with an extended focus on Q1 (adoption) as 20 academic journals cover this. If combined with ERM (hence emerged from), these two

domains are the most significant of the three quadrants (Q1, Q2 and Q3). This denotes that literature on RM/ERM is predominant in view of adoption and is almost equal regarding the focus on implementation and measurement. Though, it is almost non-existent regarding research on compliance.

Based on the results, it can be determined that RM literature pays particular attention to adoption (determinants, enablers and inhibitor) (Q1), whereas a small proportion focuses on exploring the aspects of implementation (Q2) or maturity measurement or compliance. This gap is expected to be completed by ERM. Thus, this evidence helps to confirm that literature on ERM adoption, implementation, measurement, and compliance is expanding.

In the case of CsM, the implementation quadrant suggests that literature focusing on implementation is sub-optimal, yet prior literature on cybersecurity has registered considerable focus on adoption and measurement. Lastly, the alignment registers significant considerations in academic papers. Regarding the alignment, Table 3-2 shows that academics significantly question the strategic alignment. The initial analysis of alignment displays that considerable research is carried out on IT and business alignment strategies. This evidence matters for current research even if the focus differs slightly from the purpose of this research. Consequently, alignment research remains invalidated in practice and non-existent regarding CsM alignment with ERM.

The following section focuses on identifying the proportion of industries considered across all four domains. For instance, Luftman, Papp and Brier (1999) consider that strategic alignment was examined, focusing on specific sectors, and the results might be inappropriate. Luftman, Lyytinen and Ben Zvi (2015) agree that the analysis and its outcome are inappropriate for general applicability since many models are developed across different industries and a model developed primarily for a particular industry cannot be applied to another without taking into consideration the internal and external context or organisations' characteristics. Authors such as Baets (1992, 1996), Broadbent and Weill (1993), Avison *et al*. (2004) and De Haes and Van Grembergen (2009) are among few who have focused their research exclusively on banking and financial services.

Further findings are synthesised in Figure 3-3, which outlines the prominence and variability of industries across for three domains.

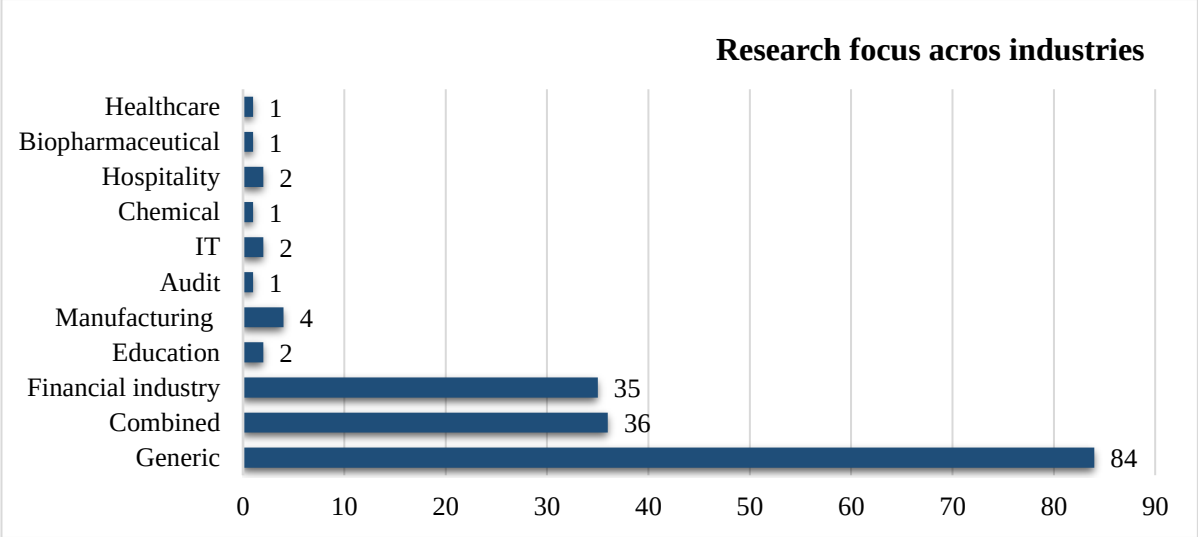


Figure 3-3 Research focus across industries

Source: The Researcher

Similar to the previous table, only 169 papers from 312 are considered appropriate in terms of performing the analysis of industry proportion. It was found that the financial industry registers only 35 from selected papers.

Continuing with analysis, the next section illustrates the demographical propensity of each domains.

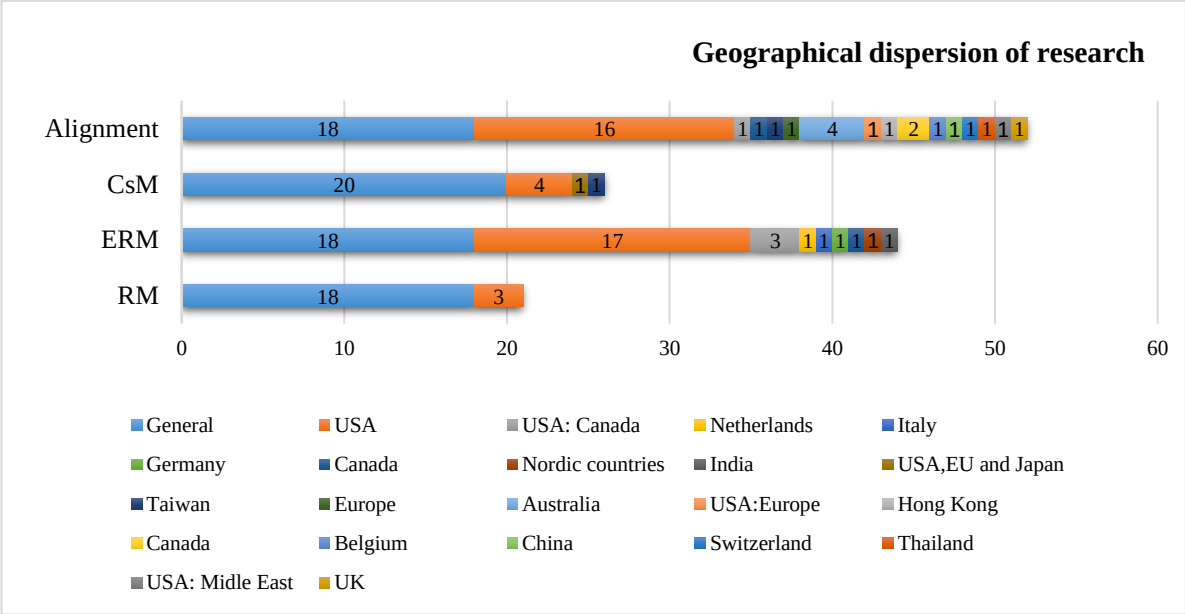


Figure 3-4 Geographical dispersion of research

Source: The Researcher

As shown, a significant percentage of papers reference unspecified focus on a country practice, being generally applicable. The option to classify the paper based on the author's location is rejected by the researcher hence analysis is focused in identifying papers scope (e.g. country-specific practice). It is evident from data gathered that prior studies have considered a global and general perspective, followed by studies considering USA settings. Most likely, a generically geographical dispersion can omit region-specific requirements and thus affect the applicability. It has been emphasised that geographical dispersion has become a current challenge for organisations (Oliver Wyman, 2018b).

Finally, warranting particular emphasis is the coincidental evolution of all four domains over time. As can be viewed in the below table, the years 2008-2009 saw an expanded interest. This might be related to the period post-global financial crisis. The trend continued until 2010 which, one can assume, was when the effects of the crisis were absorbed /accepted by organisations.

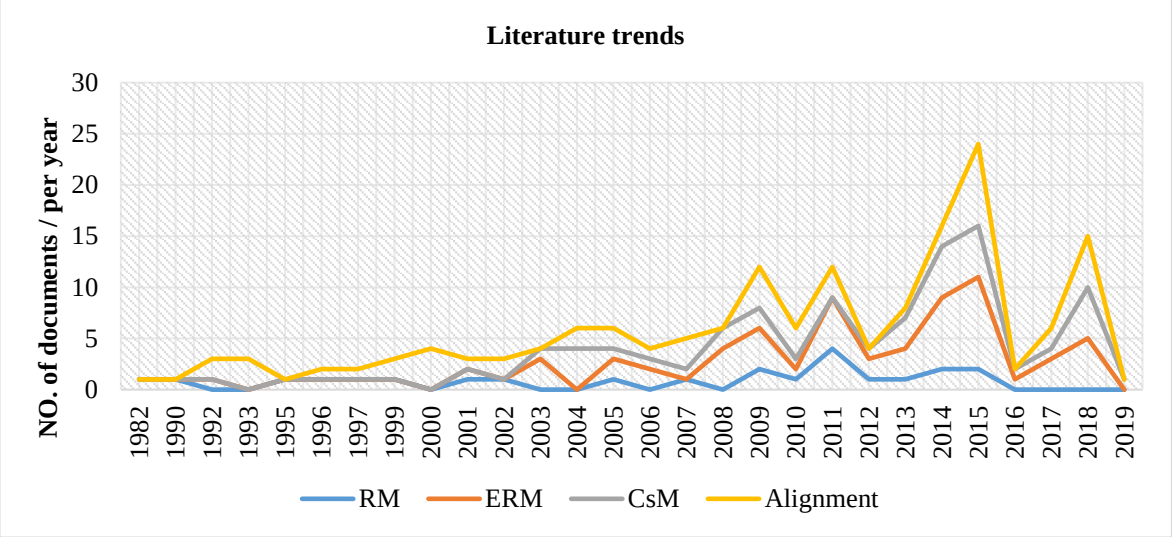


Figure 3-5 Focus of selected literature across the years (1982-2018)

Source: The Researcher

The data obtained shows a consistent fluctuation regarding alignment, which in turn demonstrates that between 2010 and 2015 its applicability in organisational context yielded benefits. Likewise, years 2017-2018 show consideration for alignment and CsM. Earlier research explored alignment generically, and thus current research proposes to reanalyse certain contexts in order to apprehend its applicability to the financial industry (aspects discussed in Section 3.1, Chapter 3). Previous research deployed detailed analysis on alignment layers, namely IT alignment with business, IS with RM, and CsM alignment with

RM. This research aims to consider prior research and to expand CsM alignment with ERM. The evidence compiled in this synthesis points towards the idea that there is scarce alignment literature that considers the integration of CsM and ERM. It also confirms that alignment is at an undeveloped phase (i.e. scarce consideration of regulatory bodies demonstrates that the problem was formally ignored).

Table 3-9 Summary of literature gap (1982-2018)

Literature dimensions Strategic Structural Social Cultural				
Domain	**Theoretical derivations**	**Author/s (year)**		
		academics	**practitioners**	**regulators**
CsM	**UNCLEAR THEORY** Lack of coherent terminology and theory	Craigen, Diakun-Thibault and Purse (2014); Hong *et al*. (2003); Von Solms and Van Niekerk (2013).	none	NATO CCDCOE (2015); HM Government (2015b); HM Government (2015c).
	GRANULAR STRATEGY Deficient silo approach of security strategy and business strategy. Ineffective identification for internal challenges. Scarce practices of enterprise-wide risk culture. Role culpability transparency (silo departments). Lack of shared risk spectrum oversight (unified capabilities of reporting, analysis and mitigation).	Da Veiga and Eloff (2007); Singh, Gupta and Oija (2013); KPMG (2014d); PwC (2014); Schiavone, Garg and Summers (2014); Web *et al*.(2014b); Nazareth and Choi (2015); Mohamed (2015); Von Solms and Von Solms (2018).	McAfee (2013); EY (2014); KPMG (2014e); Thomson Reuters Accelus (2014); McAfee (2014); Ponemon Institute (2015); Verizon (2015); (Deloitte, 2015f); Gartner (2016).	UK Cabinet Office (2009); UK Cabinet Office (2011); USA Department of Homeland Security (2011); ENISA (2012); Europol (2014); UK London Chamber of Commerce and Industry (2014).
	DRAWBACKS IN IMPLEMENTATION Embedded silo practices. Fragmented practices for implementation. Optimisation required to organisational needs. Granular holistic implementation. Fragmented practices of implementation. Lack of organisational risk awareness. Lack of effective organisational risk governance: boardroom involvement.	Von Solms and Von Solms (2004); Peppard and Ward (2004); Kotulic and Clark (2004); Gerber and Von Solms (2005); Chang and Ho (2006); Bojanc and Jerman-Blažič (2008); Humphreys (2008); Tashi and Ghernouti-Hélie (2009); Siponen and Willison (2009); Deibert and Rohozinski (2010); Julich (2012); Fenz *et al*.(2013); Min, Chai and Han (2015); Soomro, Shah and Ahmed (2016); Korovessis (2017); Armenia et al. (2018); Gordon *et al*. (2018); Rubino (2018); Nasir *et al*. (2019).	ISSA (2004); Lloyds (2010); KPMG (2013a); CISCO (2014); KPMG (2014c); KPMG (2014a); Websense Security Labs (2015); KPMG (2015); Accenture (2016); Deloitte (2018).	CSBS (2014); HM Government (2015a); Financial Industry Regulatory Authority (2015); Financial Stability Board (2017).
	RESILIENCY CHALLENGES Difficulties in measuring maturity compliance with regulators and industry demands (submission failures). Reactive versus proactive-difficulty in achieving resiliency-increased cost.	Web *et al.*(2014b); Raban and Hauptman (2018); Marotta and McShane (2018).	Deloitte (2012): Ponemon Institute (2013); PwC (2013a); CSIS (2015); (Marsh, 2015); Oliver Wyman (2018b).	OECD (2002); Bank of England (2013); USA Department of Financial Services (2014); ENISA (2017); Bank of England (2018); Financial Conduct Authority (2018); Basel Committee on Banking Supervision (2018).
RM and ERM	**ADOPTION BENEFITS** Effectiveness and performance. Determinants and impact of ERM implementation. Maturity-performance relationship. Internal framework benefits. Return on investment (ROI).	McShane, Nair and Rustambekov (2011); Griffin and Boomgaard (2013); Eckles, Hoyt and Miller (2014); Lundquist (2014); Gatzer and Martin (2015); Dabari, Kwaji and Ghazali (2017); Cohen, Krishnamoorthy and Wright (2017); Bogodistov and Wohlgemuth (2017).	KPMG (2017b).	none

	IMMATURE APPLICATION Incomplete understanding of implementation benefits. Granular literature on implementation. Unclarified determinants of successful ERM. Partial understanding of organisational factors. Research focus path variations Scarce proofs of lessons learnt.	Dickinson (2001); Nocco and Stulz (2006); Rosenberg and Shuermann (2006); Schoening-Thiessen and Simkins (2008); Beasley, Pagach and Warr (2008); Francis and Paladino (2008); Power (2009); Pagach and War (2011); Hoyt and Lienberg (2011); Paape and Speklé (2012); Baxter *et al*. (2013); Ching and Colombo (2014); Rubino and Vitolla (2014); Beasley, Branson and Pagach (2015); Lyons (2015); Bromiley *et al.* (2015); Andrén and Lundqvist (2017); Majdalawieh and Gammack (2017);Viscelli, Hermanson, and Beasley (2017); McShane (2018); Rubino (2018).	The Institute of Chartered Accountants in England and Wales (1999); (PwC, 2009); McKinsey (2010); PwC (2015); Ernst and Young (2016); Deloitte (2015c); American Institute of Certified Public Accountants (2017); PwC (2018); AICPA (2018).	none
	IMPLEMENTATION DRAWBACKS External and internal variables. Shortcomings to embed implementation. Granular governance: lack of proactive practices (reactive). Organisational culture interaction with risk oversight. Scarce applicability of the holistic approach. Misaligned risk strategy with business strategy. Misalignment of risk appetite with objectives and risk exposure. Unclear implication of silo risk oversight. Un-continuous lifecycle of risk oversight. Fragmented integrative approach. Unclear accountability of risk. Highly embedded in IT practices. Top-down internal control (leadership led).	Miller (1992); Ward (2003); Kleffner, Lee and McGannon (2003); Lienberg and Hoyt (2003); Drew and Kendrick (2005); Beasley, Clune and Hermanson (2005); Castro *et al*. (2008); Burnabi and Hass (2009); Mikes (2009); Gordon, Loebs and Tseng (2009); Wu and Olson (2010); Arena, Arnaboldi and Azzone (2010); Lin, Wen and Yu (2012); Tekathen and Dechow (2013); Farrel and Gallagher (2014); Hayne and Free (2014); Hayne and Free (2014) Grace *et al*. (2015); Aven and Aven (2015); Lalitha and Nandini (2015); Shad and Woon (2015); Zéghal and El Aoun (2016); Farrel and Gallagher (2019); Oliveira *et al*. (2018); Aguilera, Judge, and Terjesen (2018).	Deloitte (2009); Manigent (2009); Manigent (2011); Protivity (2012); Grant Thornton (2013); Tower Watson (2014); Thomson Reuters (2015); COSO (2017).	none
	DUE CARE FOR COMPLIANCE Difficulties in measuring maturity-compliance reporting. Lack of transparent decisions. Compliance pressure to ensure risk baseline under necessity not desire.	Arnold *et al. (*2011); Lindberg and Seifert (2011); Nair *et al*. (2014); Schiller and Prpich (2014).	Standard and Poor's (2008); Accenture (2009); McKinsey and Company (2016).	SOX (2002); Dodd-Frank Act (2010); NYSE (2014); Financial Reporting Council (2016).
Alignment	**STRATEGIC ALIGNMENT** Immature alignment (objectives and strategies). A lack of practical alignment literature guidance. Lack of operational flow within organisational departments.	Henderson and Venkatraman (1993); Smaczny (2001); Baets (1996); Chan (2002); Bergeron and Rivard (2004); Campbell, Kay and Avison (2005); Sledgianovsky and Luftman (2005); Luftman and Kempaiah (2007); De Haes and Grembergen (2009); Gutierrez, Orozco and Serrano (2009); Preston and Karahanna (2009); Johnson and Lederer (2010); Chen (2010); Charoensuk, Wongsurawat and Khang (2014); Mekawy, AlSabbagh and Kowalsky (2014); Reynolds and Yetton (2015); Lutman, Lyytinen and ben Zvi (2015); Gerow, Thatcher and Grover (2015); Fakhri, Fahiman and Ibrahim (2015); Joshi *et al*. (2018).	none	none
			none	none
	SOCIAL ALIGNMENT Scarce of leveraged communications amongst departments. Holistic immersion of employees.	Powel (1992); Luftman, Papp and Brier (1999); Papp (1999); Kearns and Lederer (2000); Luftman (2000); Cragg, King and Hussin (2002); Chan (2002); Avison *et al*. (2004**);** Chan, Sabherwal and Thatcher (2006); Huang and Hu (2007); Taradfar and Qrunfleh (2009); Rahman and Donahue (2010); Wu, Straub and Liang (2015); Volk and Zerfass (2018).	none	none

	STRUCTURAL ALIGNMENT Inadequate structural collaboration. Restrained organisational change behaviour.	Burn and Szeto (2000); Chan and Reich (2007); Corsaru and Snehota (2011).	none	none
	CULTURAL ALIGNMENT Immature organizational culture	Reich and Benbasat (2000); Shao (2018).	none	none
	IMPLEMENTATION CHALLENGES Antecedents pointers and consequences of misalignment Inadequate attention for internal and external variables. Partial understanding of factors, challenges and inhibitors. Immature strategic and structural operational alignment. A lack of practical alignment literature guidance.	Powel (1992); Broadbent and Weill (1993);Venkatraman,Henderson and Oldach (1993); Ciborra (1997); Luftman, Papp and Brier (1999); Papp (1999); Kearns and Lederer (2000); Luftman (2000); Smacny (2001); Chan (2002); Cragg, King and Hussin (2002); Avison *et al*.(2004**);** Chan, Sabherwal and Thatcher (2006); Huang and Hu (2007); Taradfar and Qrunfleh (2009); Rahman and Donahue (2010); Walter *et al.*(2013); Hinkelman *et al*.(2015); Karpovsky and Galliers (2015); Wu, Straub and Liang (2015).	PwC (2018a)	none
	MATURITY ASSESSMENT Flaws in alignment effectiveness	Yarifard, Taheri and Zafarzadeh (2016); Joshi *et al.* (2018); Jevtić *et al.* (2018).	KPMG (2014a)	none

Source: The Researcher

Based on the systematic review of the secondary data, the following gaps have been identified:

(1) A lack of clear terminology and definitions in all three domains - initially identified in Chapter 2 and validated subsequently by the findings of this chapter.

There is considerable ambiguity with regards terminology across all three domains, maintain a lack of consensus among academics, practitioners, and regulators (i.e. terminology and semantic applicability) alike. Confusion regarding terminology and definitions raises many ambiguities such as security responsibilities having come initially from Loss Prevention plans before evolving to become the responsibility of a Chief Security Officer and finally that of a Chief Information Security Officer. Such evolution proves the need to redefine CsM as it is still seen as a fragmented function of securing information.

Such discrepancies are also present in various terminologies used by standards, guidelines and governmental reports (i.e. NIST used terminology CsM where ISO UK refers to it as Information Security). The question of variation in terminology needs to be addressed urgently as it affects industry practices as well as professional qualification developments.

(2) A lack of practical alignment literature guidance (academics, practitioners and regulators) -a significant amount of literature is focused on the adoption aspects (Q1).

In the case of alignment, research tends to have been carried by academics rather than practitioners or regulators. Although in the case of CsM and ERM some contributors have addressed this problem and over recent years' alignment has received attention, it has unfortunately been applied in isolation (e.g. IT-centric, RM-business centric).

A growing body of literature demonstrates that there is a lack of correlation between the practices of academics' and practitioners. Hence, the first category has considered the value (benefits) of implementation while practitioners have considered the operational aspects regarding how it can be implemented and how value can be created.

(3) A lack of common governance practices across all three domains (various guidance).

(4) Scarce alignment literature that considers the integration of CsM.

(5) Scarce industry-specific focus – namely the financial industry (ERM has a more significant consideration, while CsM and alignment address generically).

(6) Scarce consideration of regulatory bodies regarding the alignment processes.

(7) A lack of clear practices towards ERM, CsM, and alignment implementation.

(8) The literature of CsM is fragmented among different domains (e.g. Information Security, Information Assurance).

(9) Granularity of CsM terminology encouraged by various professional accreditations.

(10) Geographical dispersion of industry practices and procedure significantly influenced by two main players: the UK and the USA (for example ISO series for ERM and CsM are reproduced by other countries). Not only is there a lack of uniformity among all the anti-cybercrime measures (some are preventative, and some are curative), but there is a lack of uniformity regarding which country adopts which measures and the vocabulary used in the measures.

(11) A discontinuous temporal attention in the literature (e.g. main focus is between 2008-2009 and 2015-2016) – although a possible explanation of this could be the effects post-financial crisis.

(12) Criteria considered by the literature of ERM varies between value, performance, appetite, culture, and governance, and each of them is addressed in isolation.

(13) CsM is still seen as an IT problem, problems treated in isolation.

(14) ERM and CsM practices are seen as minimum compliance (reactive measure rather than proactive controls).

The evidence compiled in this synthesis points towards the idea that there is scarce literature on alignment and the integration of CsM and ERM. It also confirms that alignment is in an undeveloped phase because scarce consideration from regulatory bodies demonstrates that the problem had been previously ignored.

3.7 Conclusion

In the development of the findings stated in the previous chapter, this chapter has more thoroughly explored how imperative alignment is. This has been achieved by exploring and comprehending the current state of literature related to the research problem. Although the alignment of CsM and ERM within the financial industry is identified as having been only partially addressed in prior studies, it has nonetheless concentrated on diverse topics, diverse types of approaches, and varied viewpoints.

The findings of this chapter articulated gaps in theory, practice and regulatory terminology, definitions, approach or strategy. As the construction of this chapter has been developed on the research question and its derivations, the relevant sources of literature. The effects of implementing the new framework shall be discussed later in this research. Prior efforts have been made to understand the research problem and undertake literature examination (the first research aim of this research – 'to investigate the alignment of CsM with ERM within the financial industry') to support justification of the research basis.

The contribution of relevant references that have contributed to CsM alignment with ERM legacy in terms of long-term sustainability has been discussed. The findings demonstrate that recent developments of risk practices are fragmented and focus significantly on silo approaches. However, a significant number of proposed strategies have been applied, albeit in a fragmented manner (e.g. IT aligned to business strategy, IS aligned to RM, CsM aligned to RM). The analyses of literature reveal that alignment of CsM with ERM can enhance a superior risk assessment, mitigation, and resilience in organization, and thus a reduced risk profile. Transferring the whole organisation into an enhanced state of cybersecurity has been demonstrated through the interconnectivity of CsM and ERM. On the contrary, a lack of integrated approaches amplifies work required and the cost.

Based on the identified results, it has been determined that literature trends have varied between domains. Due to limited literature on alignment, this chapter has examined an exploration of prior literature based on separate domains and through the inclusion perspective (alignment). In the case of exploration as a separate domain, it is particularly

important that it provides an understanding of how it has been perceived independently (e.g. RM, ERM, CsM or alignment). To evaluate literature maturity, the literature has been categorised into four types of quadrant: adoption, implementation, maturity assessment, and compliance. The literature has been categorised to understand its transitions and how it is concentrated.

It has been identified that RM literature pays particular attention to adoption (determinants, enablers and inhibitor) (Q1), whereas a small proportion focuses on exploring the aspects of implementation (Q2) or maturity measurement or compliance. This gap is expected to be completed by ERM, which contributes equally in all four quadrants. Thus, this evidence helps to confirm that literature on ERM adoption, implementation, measurement and compliance denotes the innovative and integrative aspects of it. Although the implementation quadrant has suggested that the application is sub-optimal and researched in academic papers, in contrast, the practitioners' cybersecurity legacy has registered considerable evidence for adoption and measurement. On the other hand, alignment literature has indicated only significant considerations in academic papers and non-existent consideration of practitioners or regulators. Consequently, the researcher is of the opinion that the evidence demonstrates that alignment research remains invalidated in practice and scarce regarding CsM alignment with ERM. Consequently, the ambiguous evidence identified (e.g. terminology, definitions) along with immature adoption within the financial industry demonstrate that often a holistic strategic approach is scattered in silo approaches, most often as a tick box approach for compliance purposes rather than enterprise-wide embedded.

In conclusion, the different types of evidence prove that further work needs to be done to manage risk and effectively sustain organisations in the long-term. Moreover, the findings of this chapter highlight main contributors, attitudes towards risk mitigation, and literature's current limitation. It has also demonstrated that capabilities of ERM, CsM and Alignment work in an integrative manner to sustain an organisation strategically.

To further the research, Chapter Four considers a derivation of literature along with a further summary of prior frameworks for gap identification purposes, which along with theoretical supporting theories serve as a platform for the *CsM-ERM Strategic Alignment Framework.*

4. Chapter Four: Development of CsM-ERM Strategic Alignment Framework

4.1 Introduction

Chapter Four draws on the initial findings of the literature reviews in Chapters Two (first derivate) and Chapter Three (second derivate), which allowed identification of the research gap (third derivate). It examines supporting theories (fourth derivate) and supporting frameworks and gaps (fifth derivate), and combines them with the previous information to identify the *CsM-ERM Strategic Alignment Framework.*

The first section considers theoretical premises of modern management theories (contingency and institutional), along with some components of organisational theory to inform the basic premises on which this research is constructed. The second shows a more practical perspective from all three domains (CsM, ERM and alignment) to explore current practices and study how the identified gaps correlate with the *Framework* purposes. The key concepts and key practices are incorporated in the third section, which provisionally informs the proposed solution.

4.2 Supporting theories

A theory represents an 'explanation' of a specific phenomenon (Nilsen, 2015), and the correlation between supporting theories and the research problem is grounded on the premises of concepts and principles (e.g. management, governance, alignment and coordination of interdepartmental control function) so as to understand the phenomenon (Olum, 2004; Hatch and Cunliffe, 2013) within its systematic construction and its specific boundaries (Bhattacherjee, 2012). Thus, in supporting the Framework, Contingency Theory and Institutional Theory have been selected to offer an explanation to the research problem because they reflect on contingencies and dependent factors within an internal and external environment along with their causal relationship (Sutton and Staw, 1995) and with institutional norms.

As the considered theoretical premises respond to the research problem in isolation, accordingly each philosophical perspective partially reflects an answer to the research problem. Nonetheless, each one is beneficial in its own right because this approach

highlights inclusivity and legacy support for a coordination mechanism that is reflected in alignment (Pupke, 2008).

4.2.1 Contingency theory

It is recognised that Contingency Theory is a modern organisational theory that sustains organisations' effectiveness, conformance and performance (Donaldson, 2001; Ghofar and Islam, 2015) by matching capabilities between organisational characteristics (structure) with environment pressure (Donaldson, 2001).

With its roots in Organisational Theory (Chenhall, 2003), the Contingency Theory was initially presented by Adam Smith in 1776 (Hatch and Cunliffe, 2013). Hence it cultivated a baseline for organisational sustainability. Over time, it has been considered in many circumstances and disciplines. It has been evolved into various types of approaches, each broken down into prehistory, modern, symbolic and postmodern (Hatch and Cunliffe, 2013).

The current modern Contingency Theory observes behaviour patterns in order to identify and solve organisation issues in an optimised manner, ensuring organisational efficiency (i.e. objectives achievement with limited resources) rather than general efficiency (merely objectives achievement), and with the intention of yielding profitability, competitive advantage (Hatch and Cunliffe, 2013), and sustainability. To achieve this, it is necessary to be able to handle internal and external pressure. Henceforth, Hatch and Cunliffe argued that: "…effective organisations are those in which multiple subsystems are aligned to maximise performance in a particular situation" (Hatch and Cunliffe, 2013, p. 32). Referring to Contingency Theory in relation to the research problem, it is centric for an organisation to fit its organisational characteristics with external pressure. This case is firstly about marrying CsM and ERM with organisation strategy and objectives. Secondly, it is to respond to any external pressure.

To simplify, Fry and Smith (1987) define Contingency Theory as an intact system, along with congruency relationships between variables such as organisational components. Contingency terms such as *fit*, *congruency*, *match* or *alignment* are used to refer to the relationship/link between two or more variables (i.e. environment pressure and strategy) in order to identify an additional variable (e.g. performance or effectiveness) (Schoonhoven, 1981). This is often defined as 'laws of relationship', as stated by Fry and Smith (1987). Consequently, a vast variety of terminology is used for the same thing, sometimes leading to confusion (Fry and Smith, 1978). As an example, Fisher (1998) describes the same process

as a *match* to enable performance. Thus, the environment is the one upon which the organisation's design and control functions are adapted.

Particular to the contingency theory is that it implies the identification of contingencies for each situation with the intention of deriving the ideal fit amongst them (Hatch and Cunliffe, 2013). Fit perspective or contingency refers to "*variables fit"* (Weill and Olson, 1989). In turn, it has been demonstrated that Contingency Theory is a situational theory that refers to management decisions in a given situation and in accordance to internal and external variables (e.g. resources, management, environmental) (Luthans and Stewart, 1977; Otum, 2004; Weill and Olson, 1989).

As a result, a misfit between environment and organisational variables (contingencies, dependencies, factors, conditions) leads to low performance and inefficiency (Gresov, 1989). An important implication of previous contributions is that contingency factors have been considered in a granulated manner by academics. Some academics have considered the following contingency variables individually: technology, strategy, governance, leadership, organisational age, size, organisational characteristics, structure, processes, competitive conditions, environment complexity, task, and individual person and/or culture (Mintzber, 1979; Zeithaml, Veeradarajan and Zeithaml, 1988; Weill and Olson, 1989; Donaldson, 2001; Hopkins, 2005; Bets, 2011).

So far, it has been identified that contingency represents a successful relationship between two or more variables (Blau, 1970) with the purpose of increasing organisational performance or effectiveness. In the case of the environment, Mintzberg (1979) articulates that it challenges the match between organisational design and environment. Accordingly, based on the above facts, organisations' design is formed and dependent on its contingencies (Donaldson, 2001). Additionally, variables such as uncertainty and the organisational capacity to cope with are detrimental (Hickson and Hining, 1971). In this context, it is worth considering that "a strategy is a plan for interacting with the competitive environment to achieve organisational goals" (Daft, 2012, p. 62). More specifically, Contingency Theory strategically provides consensus to align CsM with ERM management functions such as strategy alignment, objectives alignment, planning alignment, structural and operational organisation with social systems, and leading and control—all intended to better cope with external pressure.

Over time, subsequent studies that have focused on Contingency Theory have been interested in a variety of components: between internal (e.g. organisational integration/fit (Lawrence and Lorch, 1967), organisational structure, subunits/departments power (Hickson *et al.*, 1971) as well as a variable external environment and specific situations/conditions (Dzimbire, 2009). Thus, the theory has rejected a prescribed universal approach and in turn, recommended an optimised and unique response corresponding to the situation as determined by events and circumstance. This tends to suggest that literature prompts further attention to be paid to organisational alignment implications and dependency of internal and external variables (Hanson, 1979; Jaffe, 2001) for organisational sustainability and efficiency.

Thus, these arguments support key arguments that organisations are unique, with their own personalised practices that trigger multiple results. So, the solution varies, and the organisation, in turn, needs to adapt itself (Hanson, 1979; Tosi and Slocum, 1984; Rubino (2018). For example, Gupta, Dirsmith and Fogarty (1994) define contingency from a perspective of control and coordination because it involves a structural organisation of tasks.

There are various definitions of Contingency Theory. In addition to the aforementioned perspective, other authors define it as a contingency shift to a security perspective, where prevention and detection help organisations to react and respond (Hong *et al*., 2003). Others consider it from the viewpoint of interrelationship and the sequence of the elements acting together (Beckford, 2009). The differentiation is that every action implies a unique situation (Lorsh, 2013) and thus yields different and unique results. This school of thought is followed by Vorbeda *et al*. (2012), who discuss various means to achieve performance (more than one option) triggered by organisational setting but also by context setting.

Therefore, one can conclude that generally, contingency refers to the performance of fit of organisational design regardless of whether it is about structure, people, technology, strategy, culture, organisational structure, security, or management. This suggests the need for a dynamic management within the environment (Bets, 2011) to align its characteristics in a given situation, triggering organisation contingencies fit, performance and structural interrelationship (Weill and Olson, 1989; Ghofar and Islam, 2015).

Environment variables refer to internal and external criteria and represent the boundaries of a theory (Fry and Smith, 1987). The environment is a constraint upon which the organisation

structures its direction (Child, 1972). Hence, ‘variability’, ‘complexity’ and ‘iliberality’ (velocity of threats) affect the performance of an organisation (Child, 1972).

Consequently, environmental variables are one of the pillars of Contingency Theory. Supporting this statement, the following section discusses variables and relationships, as considered by academics.

- **Internal variables** - can include but are not limited to organisational size, task, architectural level, environment, technology, people, management, structure, culture, performance, processes, communication, effectiveness, fit, strategy, business units/departments, and support functions;
- **External environmental variables -** when undertaking an analysis of contingencies, external environmental variables are related to the external environment. It is common practice to consider PESTLE (political, economic, social, technological, environmental and legal) analysis. Furthermore, other studies refer to external environmental variables through VUCA concept (volatility, uncertainty, complexity and ambiguity) such analysis might illustrate variables’ dependencies and interdependencies on which organisational performance lies (Luthans and Stewart, 1977; Olum, 2004; Kerstin, Simone and Nicole, 2014). So, the effectiveness of an organisation depends on a range of abilities to adapt to a situation or change in connection with variables (COSO, 2017). In turn, Contingency Theory rejects the use of a approach (Zeithaml, Veeradarajan and Zeithaml, 1988; Cole, 2004). For example, the national culture involves efforts for an organisation because different countries have many cultural characteristics to which they need to adapt and comply (Chenhall, 2003). Within the internal context, beliefs, attitudes, experiences, communication or informal norms, a specific response and behaviour towards risks can be determined.

Although having witnessed some key variables such as effectiveness, environment, and congruency, contributors’ focus has varied within multiple variables over time (Tosi and Slocum, 1984). It is assumed that the Structural Contingency Theory supports organisations selecting the structures that aid the selection of further structures with a common goal of improved overall company performance (Evans, 2007). For example, in practice, Contingency Theory can represent the stance of managers in undertaking decisions based on organisational characteristics and internal variables in the interaction with the external environment. Based on this, decisions can be made (Vorbeda *et al.*, 2011) for further

enterprise-wide deployment of risk oversight practices. This can be illustrated by internal variables such as:

- **Strategy and management** – these variables are dependent on three main structural contingencies: environment, organisation, and strategy (impacts unit structure) (Donaldson, 2001). Burns and Stalker in Hatch and Cunliffe, 2013 (managing individuals and organisation) support evaluation of the impact of management style and how it affects organisational effectiveness and performance through a stable (mechanistic) and unstable (organic) internal structure (Jaffe, 2001). Along with strategy and management style, Fiedler proposes a psychological subsystem that looks at organisational behaviour to pose as an internal variable that takes place when leadership style is contingent with various situations (Kast and Rosenzweig, 1973). Therefore, on this basis, Contingency Theory suggests that before a decision is taken, all aspects, variables, and interdependencies of an organisation must be acknowledged. Moreover, Fredrickson (1984) outlines that a strategic capability balance internal capability with the external environments pressure. Hambrick and Lei (1985) also outline the importance of strategy regarding business performance and reiterate the fact that all depend on the variables (e.g. technological, environmental, product lifecycle). Ginsberg and Venkatraman (1985) analyse the effect of strategy by considering same variable (environment), and additionally the organisation and its performance.
- **Structure –** a contingency variable that refers to organisational structure concerning the organisation of processes and employment roles. An administrative mechanism of how systems are structured (Chenhall, 2003) depends on situational variables (Child, 1972) of internal and external pressures (Lawrence and Lorch, 1969 (structure and environment). Some authors believe that structural contingencies are more successful by interacting with technology (Woodward, 1967; Perrow, 1979).

Contingency examined through the perspective of structural sub-systems (structure) is also known as *Structural Contingency Theory* (Van de Ven and Drazin, 1984). This is because it explores the fit between the organisational context and its structure in order to understand how performance can be fostered. Van de Ven and Drazin (1984) indicate that Contingency Theory can be defined through the perspective of fit, interaction, and system approach because an organisation's ability to identify and adapt to fit in the context of its dependencies represents its ability to fit within a system through interaction and respond to internal and

external variables (Van de Ven and Drazin, 1984). It is therefore considered an Organisation Change Theory (Donaldson, 2001), which relies on fit-performance rapport.

Moreover, in a more simplistic manner, Perrow describes the structure of the organisation as a complete interaction defined through the system, where the interconnection of systems is essential in order to achieve the task.

In 1969, Lawrence and Lorch considered the internal structure and external demands on an organisation's management (Jaffe, 2001). Jaffe (2001) has reiterated the findings of Lawrence and Lorch and outlined that a rigid and formalised internal structure assures stability while an unstructured internal structure requires complementary efforts in cases of increased external pressure and demands (Jaffe, 2001). Additionally, the structure (form) of an organisation is interrelated and dependent and thus has impact on its construction (Lawrence and Lorch; Burns and Stalker in Hatch and Cunliffe, 2013).

While some contributors reflect only on environment and structure, Penning (1975) emphasises that effectiveness depends on the organisation's ability to adapt to environmental uncertainty variables such as technology and competition. A fit between environment and structure might assure organisational effectiveness in the long-term.

- The **Size** of an organisation is considered closely connected to the need for specialisation and expansion through the development of additional divisions and administrative actions (Chenhall, 2003). Although organisational size can trigger opportunities (Child, 1972), it also implies a need for increased administration dimensions (Blau, 1970).
- **Technology** is seen as a significant variable in designing organisational structure (Child, 1972).
- **Cultural variables** can interfere with the organisational design or structure due to their interrelationship with other variables (Tosi and Slocum, 1984). For example, cultural differences are variables which can affect managerial control as well as individual evolution and input. Additionally, they put pressure on strategic decisions as all of these variables are interrelated to some degree (Tosi and Slocum, 1984).

In conclusion, contingency theory avoids recommending a specific manner to organise contingencies, as it is believed that what is appropriate in one situation might fail in another. Due to the Contingency Theory's recognition of every organisation and every organisation's situation being unique, it can be adapted and tailored (Schoonhoen, 1981). Thus, Contingency Theory can be effective or ineffective depending upon how it is tailored to meet

ever-changing and ever unique variables. If it is not tailored correctly, it will be ineffective. For example, an organisation's internal norms, traditions or philosophy might prompt the way risks are perceived, communicated, and understood (RIMS, 2014).

4.2.2 Institutional theory of organisation

The essence of Institutional Theory originates in how institutions are perceived in a social realm (Hodgson, 2006). An abstract view of institutions is a format of systems or structures taken for granted that constrain behaviour in the form of rules, norms (e.g. communication, sovereignty), values, or beliefs pertaining to social interaction (Barley and Tolbert, 1997; Hodgson, 2006). Such a view of institutions defines the appropriate relationship of social actors based on shared rules (Barley and Tolbert, 1997).

In the same way, this theory applies to organisational context to establish command and assign responsibilities. Thus, Institutional Theory refers to an organisation structure's ability to reflect institutional pressure/requirements towards a maximisation of institutional conformity (also referred as legitimacy) and effectiveness (Donadson, 2008; Hsu, Lee and Straub, 2012).

In short, it represents the organisational behaviour as a reaction of how it adapts, based on well-known informal and formal norms, to an action (Hu, Hart and Cooke, 2007; Hsu, Lee and Straub, 2012). It also represents the organisational homogeneity (expectation vs. organisational response) towards mimetic, normative, and coercive pressure (Daft, Murphy and Willmott, 2014). Institutional Theory is an organisation theory which was initially researched in the 1957's by Selznick, who was interested in exploring and understanding how processes shape organisations (Vorberda *et al*., 2011; Greenwood, Hining and Wheten, 2014) and vice versa (Greenwood, Hining and Wheten, 2014).

Although the Institutional Theory of the 1950s does not closely relate to cybersecurity management and ERM, it is the predecessor of the modern Institutional Theory, which does indeed bare great significance on the topic of this research.

The Modern Institutional theory

Known also as Neo-Institutional Theory, the Modern Institutional Theory supersedes the old "definitional*"* approach of Selznick and moves towards interaction with social phenomena within organisations for "explanatory purposes" (Hu, Hart and Cooke, 2007). The theory addresses what sets the condition of an action (e.g. rules, norms, practices, structures,

processes, obligations) (Lawrence and Shadnam, 2008; Suddabi, 2010). The theory has come to be used as a way to understand how and why institutions interact under internal and external environmental pressures (Zucker, 1987; Hu, Hart and Cooke, 2007), and how they adapt, evolve, or dissolve (Lawrence and Shadnam, 2008).

Some authors believe that organisational environment seems to shape an institution's goals, ways of functioning (Scott, 1987), structure, management, and coordination (Meyer and Höllerer, 2014). In short, the Institutional Theory appears to portray the issue in terms of boundaries, grounded on the assumption that the relationship between structures, resources, processes, or governance of an organisation depends on environmental pressure (Casson and Rose, 2014).

Meyer and Rowan (1977) introduce the value of formal organisations, paying considerable attention to coordination and control of activities through a formal structure. DiMaggio and Powell (1983) articulate that institutionalisation refers to 'structuration', 'bureaucratisation', and 'rationalisation' for the purpose of efficiency.

Lawrence and Shadnam (2008) highlight that institutional context is a major constituent towards isomorphism (i.e. institutions identity is alike ─ form, structure, processes). Henceforth, organisations defined through isomorphism refer to a single legitimate form, the tendency to deviate from the expected pattern and expose the organisation to be illegitimate.

Consequently, external rules, also known as 'rationalised myths' (traditional conformity) can influence an institution, and isomorphism has been associated with three forms: coercive, mimetic, and normative (Jaffe, 2001; Lawrence and Shadnam, 2008).

- Coercive isomorphism refers to the informal and formal pressures on organisations from various sources and their effect on organisational behaviour (Daft, Murphy and Willmott, 2014). For example, regulatory compliance represents a significant factor in undertaking decisions (Lawrence and Shadnam, 2008). Essentially, coercive pressure refers to external pressure exerted on an organisation in order to render the adoption of specific behaviour (similar to other organisations) recognised as a professional expectation in the form of a norm, obligation, moral, standard or duty (Daft, Murphy and Willmott, 2014). This can include, for example, the effect of peer organisations, competitors, regulatory bodies (Teo, Wei and Benbasat, 2003), political influence or influence from supervisory authorities, economic factors (Hsu, Lee and Straub, 2012), among many others. Undeniably, regulatory pressure

(Sarbanes-Oxley Act, Data Protection Act, as previously discussed in Subsection 3.3.3) for security practices is validated in a practical way through studies (Hsu, Lee and Straub, 2012). This 'rationalised myth' of coercive isomorphism is highly related to the research problem because it aims to understand the exercise of control and dependence of regulatory tools along with practitioners' and academics' views**.**

- Normative isomorphism addresses the collective influence of professionalisation (Hsu, Lee and Straub, 2012) and focuses on normative social expectations to control specialist positions categorisations (Lawrence and Shadnam, 2008) that delegates responsibilities. Some examples of normative influences are professional interactions at events (e.g. conferences, professional associations meetings) within specialists (Hu, Hart and Cooke, 2007). It can also refer to the managers' capability to champion risk awareness campaigns to sustain the value of CsM alignment with ERM.
- Mimetic isomorphism questions the cognitive influence to imitate successful organisations as taken for granted a solution to thrive and be recognised as legitimate (Jaffe, 2001; Hsu, Lee and Straub, 2012). It analyses what leads to specific organisational decisions taken in specific practices (Lawrence and Shadnam, 2008) mechanism or structures (Daft, Murphy and Willmott, 2014).

This approach (institutional) is similar to Contingency theory except it refers to homogeneity while contingency relates to the influence of variation. There are various interpretations regarding institutional views, hence the response of academics focusing on various aspects. Institutional Theory posits to explain how mimetic, coercive, and normative pressures affect the interdepartmental linkage compliance on daily work practices (Teo, Wei and Benbasat, 2003).

4.2.3 Mixing the Contingency Theory and Institutional Theory

While Institutional Theory regards how institutional constraints (i.e. known as isomorphism) shape organisations' behaviour (Vorberda *et al.*, 2011; Greenwood, Hining and Wheten, 2014), the Contingency Theory focuses on how organisations can be managed and coordinated as a whole, marrying organisational structures, systems, and external environments (Greenwood, Hining and Wheten, 2014).

Referring to the association of theories, literature has considered conflicting aspects that might appear between the theories. Even though these issues have been suggested, many

authors (Donaldson, 2008; Vorbeda *et al*., 2011) have succeeded to empirically test the validity of mixing the two theories as complementary and co-dependent. Furthermore, associating the theories may be appropriate (Evans, 2007; Greenwoood, Hining and Wheten, 2014) as both of them have roots in Organisational Theory and are related to organisation design/structure (Donadson, 2008).

However, the difference lies in the fact that each of them focuses on a different perspective or 'fit' and offers a different outcome. For example, Contingency Theory concentrates on achieving an internal fit with an external environment, whereas Institutional Theory concentrates on achieving an external fit (e.g. recognition of conformity, external support) by adapting its internal environment; this leads to a 'meta-fit' (Donaldson, 2008) as well as performance and effectiveness (Chorn, 1991; Vorberda *et al*., 2011). It has been found that both theories are influenced by factors and variables. In the case of Contingency Theory, it strives to adjust to variables, while Institutional Theory is under the authority of institutional 'norms' pressure/conformance (Vorberda *et al*., 2011), in other words, an 'institutional template' (Greenwood and Hining, 1996).

Although the terminology of *alignment* registers various terminologies in strategic management (i.e. both the Contingency Theory and Institutional Theory use the term 'fit') it is clear that it refers to the aspects of alignment (previously discussed in Section 2.7, Chapter Two). Along with the important implications stemming from the findings presented in Section 2.7 from Chapter Two, reviewing the literature has also demonstrated that scholars have used the concept of alignment by using 'fit' terminology. Some examples of varying terminology can be found in the studies carried out by Donaldson (1987), Tosi and Slocum, 1984), Prescot (1990), Roth and Morrison (1992), Zajac *et al*. (2000), Hitt *et al*. (2001), Birknshaw *et al.* (2002); all of which referred to the contingency *fit* instead of *alignment*. Not adopting a uniform terminology, renders confusion regarding what alignment is. As previously discussed, in both theories the term 'fit' refers to alignment. However, it must be acknowledged that some authors such as Vorberda *et al*. stipulate that 'fit' originates from Contingency Theory (Vorberda *et al*., 2011).

Researching deeper, one can read contingency and institutional fit approaches are both co-alignment approaches that focus on different types of synergy between the organisation and its environment" (Vorberda *et al*., 2011, p. 1044). This is relevant when proving the theories' commonality and appropriateness. Although this theoretical framework of the dimension of

alignment depends on the Contingency Theory and Institutional Theory, it strives towards the same purpose; i.e. attaining organisational goals (Semler, 1997) along with achieving legitimacy and sustainability. By referring to the dependable, Figure 4-1 illustrates the various internal dependable (contingencies) of each theory in terms of its interaction with the external environment.

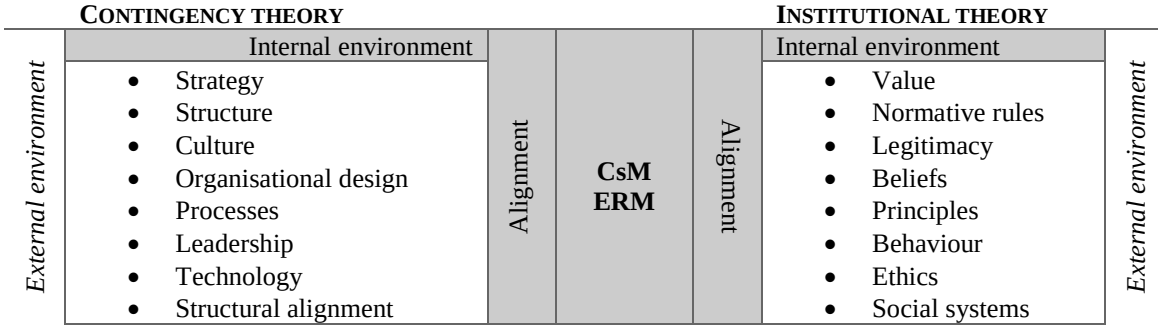


Figure 4-1 Theoretical derivations of research *Framework*

Source: The Researcher

Figure 4-1 compares any intercorrelations among the theories in order to determine its suitability within a CsM and ERM context. As an example of industry applicability of mixing theories, the COSO 2016 framework for ERM acknowledges both internal and external variables, even if its main focus is internal governance. Although it does not specifically mention using theories, the spectrum of variables to which it refers relates to Contingency Theory (i.e. it uses the PESTLE model a macro-environmental analysis towards examining the Political, Economic, Sociocultural, Technological, Environmental and Legal factors) along with internal variables. Moreover, the Institutional Theory is embedded in the COSO framework as it forms its core values based on: "the entity's beliefs and ideas about what is good or bad, acceptable or unacceptable, which influence the behaviour of the organisation" (COSO, 2016, p. 104). As organisations are unique, a combination of Contingency and Institutional Theories is advocated by the Researcher with the purpose to explore and explain how a correlation of them can ensure performance, sustainability and effective strategic alignment between CsM with ERM.

4.3 Preceding related frameworks

With reference to the previously identified *Framework* derivates— (1) literature review Chapter Two, (2) literature evaluation Chapter Three, (3) research gap Sections 2.8 and 3.5, (4) supporting theories - Section 4.2—this section encompasses a critical synthesis of frameworks (5^{th} derivate) that aim to demonstrate the validity and necessity of the *CsM* -

ERM Strategic Alignment Framework for organisations. Moreover, this section is driven by Research Objective 3: *To review and evaluate the effectiveness of current CsM and ERM frameworks.*

More specifically, the first subsection gives a comprehensive account of specific frameworks for ERM, CsM and Alignment. However, because the frameworks have often been individualistically investigated by previous research, the appraisal and comparisons have been made in isolation for each domain and in some cases, even the terminology for 'framework' (model, standard) varies. Lastly, based on the initial evaluation of the preceding supportive frameworks made in Chapter Three, the *Framework* derivations are emphasised, along with a synthesis of framework research gaps.

4.3.1 Enterprise Risk Management frameworks

This subsection will discuss the ERM frameworks' value with reference to their contribution and limitations, in context of the proposed research Framework, evaluated through the use of maturity quadrants tool, (Quadrant 1 Adoption, Quadrant 2 Implementation, Quadrant 3 Maturity assessment and Quadrant 4 Assesses compliance) and as discussed previously in Chapter Three, Section 3.2.

4.3.1.1 ERM academics' frameworks

The nature of this subsection is conceptual, hence the theoretical dimension being a characteristic of academic frameworks. Numerous authors have shown interest in developing ERM frameworks. However, only five are specifically considered and explored, despite others being considered for substantiation. Table 4-1 exemplifies them accordingly.

Table 4-1 ERM frameworks conceptual-specific

Issuer/year	Framework	Industry focus	Domain	Key function
Miller (1992)	Integrated RM framework in international business	generic	RM	Q1
Ward (2003)	Integrated RM: a multi-dimensional framework	generic	RM	Q2
Drew and Kendrick (2005)	CLASS framework	generic	ERM	Q1
Ching and Colombo (2014)	Conceptual ERM framework	combined	ERM	Q2
Shad and Woon (2015)	ERM implementation framework	generic	ERM	Q3

Source: The Researcher

Table 4-1 brings to attention various insights regarding ERM and they are further explored in below paragraphs.

Integrated RM framework in international business

One of the early ERM frameworks is that of Miller (1992), who proposed to integrate RM in accordance to managerial decisions. One implication of this framework is that it incorporates procedures needed to classify risks in the industry and firm up specific variable uncertainties. Accordingly, it considers internal and external risks that might derail an organisation from achieving its objectives. This derivation of the framework is integrated into the assessment phase of the research Framework. Whilst valuable in terms of theoretical contribution, the Miller's framework represents an initiation towards an integrated and mature ERM framework. Being conceptual in its nature, it is characterised by pre-implementation aspects (e.g. benefits, barriers, uncertainties) addressed within international context. Thus, it represents a partial perspective (Q2) that has an industry-generic addressability through the lens of strategic management—a siloed approach of strategy is therefore lacking in cybersecurity considerations.

Integrated RM: A Multi-dimensional Framework

Another contributor is Ward (2003), whose framework has a multi-dimensional approach (six dimensions) to transform merely hypothetical strategy into one that is actually applied. Based on a sequence of steps, the framework emphasises an understanding of risks illustrated in the form of classification to help the achievement of informed treatment measures and investment. Acknowledgement of classification aspect deploys further decisions based on clear purpose, processes, and responsibilities. While this framework contributes to the literature, its lack of detail and practical validity seems to suggest that more complex procedures are required to establish an ERM framework. Even though the framework endorses the implication of achieving organisational governance, this Researcher argues that its structure seems to be that of a general overview without providing a practical approach. For instance, in the first pillar, culture is acknowledged as a meaningful way to establish norms, values, attitudes, and a framework of ethical behaviour. In addition, the remaining pillars are generically described. In short, they are considered but their role in establishing the vision, strategies, collaboration, leadership, alignment, or organisational structure is briefly discussed.

CLASS Framework

Similar to the previous framework of Ward, the framework of Drew and Kendrick (2005) questions organisational governance from the viewpoint of five pillars: culture, leadership, alignment, structure, and systems (CLASS framework). The importance of RM is explored

in the context of organisational strategy and context. Therefore, most considerations are focused on highlighting the value of an internal and external environment fit. Moreover, a clear understanding of risk profile in the interaction with organisational risk exposure leads to appropriate control and more specifically towards an RM aligned with organisational governance. However, the CLASS framework lacks clarity regarding how alignment should be achieved in practice. In short, it stretches the objectives but omits to indicate the plan of implementation as it only focuses on adoption (Q1).

Conceptual ERM Framework

Ching and Colombo (2014) provide a framework with a more practical structure of internal control. Based on an ERM cycle, the conceptual ERM framework recommends consideration for internal factors to enhance assessment, followed by implementation, analysis, monitoring, review and lastly, a continuous improvement. Mainly, restricted to findings extracted from the practices of organisations, Ching and Colombo's frameworks are descriptive in nature, limited to implementation aspects, and show scarce consideration for all potential factors (external).

ERM implementation framework

Given the orientation of previous frameworks, the following framework of Shad and Woon (2015) is grounded in a practical approach and covers ERM implementation, looking at structure, governance, processes, and a method to measure the approach through an economic value added (EVA). Within governance, the impact of objectives, use of standards, and use of tools to measure performance (KPI) and risk indicator (KRI) are examined. This framework address ERM implementation based on identification, analysis, assessment, mitigation, and the monitoring of risks; a process that aims to prevent a deviation from objectives.

In response to the aforementioned framework, this research argues that when synthesising the frameworks' focus, their contribution represents a descriptive approach (lack of empirical evidence). Therefore, the applicable procedures for establishing an ERM framework are incomplete/immature and suggest the need for a more realistic and practical approach.

4.3.1.2 ERM practitioners' frameworks

Practical industry insights are introduced through ERM mandatory-specific frameworks (known as standards) and ERM advisory-specific frameworks, the former being more voluntary specific due to their commercial nature.

4.3.1.2.1 ERM mandatory-specific frameworks

This subsection summarises the main ERM mandatory-specific frameworks.

Table 4-2 ERM frameworks of mandatory-specific organisations

Issuer/year	Framework	Industry focus	Domain	Key function
FERMA (2003)	FERMA's Risk Management standard	financial	RM	Q2
Casualty Actuarial Society (2003)	Casualty Actuarial Society ERM framework	generic	ERM	Q2
BSI (2009a; 2018a)	British Standard ISO 31000:2009, 2018	generic	ERM	Q2
COSO (1992, 2004, 2013, 2017)	COSO Internal Control-Integrated framework	generic	ERM	Q2
RIMS (2006, 2015)	RIMS Risk Maturity model	generic	ERM	Q3

Source: The Researcher

Figure 4-2 depict some of standards that have considered ERM applicability. The academic literature indicates that the most used are FERMA, ISO, COSO, RIMS and Casualty Actuarial Society standards. This subsection it represents an evaluation in terms of relational aspects with the proposed framework, where an initial evaluation has been made previously in Subsection 3.3.2, Chapter Two.

FERMA's Risk Management Standard

The Federation of European Risk Management Association (FERMA) standard uses basic principles of RM processes (e.g. internal and internal factors) in order to establish an implementation. Along with a monitoring process of any given modification, it extends its structure in contrast to other standards and emphasises the value of formal audit. Nonetheless, its dependency on ISO terminology (ISO Guide 73) demonstrates the dependency on an additional source and thus is improbable to implement exclusively. Whilst incomplete due to its dependency and partial focus (Q2), FERMA's Risk Management Standard is valuable in terms of a simplified process guided by strategic direction and internal control. However, it yet seems too focused on the operational dimension of processes and risk reporting.

Casualty Actuarial Society ERM Framework

Casualty Actuarial Society ERM Framework is conceptual in its nature and incorporates processes, tools, and procedures for the purpose of creating value (CAS, 2003). The

framework is characterised by a preventative attitude towards risks and recommends prior investigation and identification of risks types. Conversely, the downside of the framework is that it only addresses the alignment of RM with organisational strategy and is therefore a partial framework focusing on implementation (Q2).

BS ISO series family

Seeking to extract new derivates for the research *Framework*, two versions of BS ISO Standard 31000 are considered as derivates. Initially, ISO 31000: 2009 builds its structure focusing on processual aspects of implementation (purpose: strategic and operational). Although withdrawn/superseded in 2018, it incorporated basic principles of RM and served as the basis for the updated version: ISO 31000:2018 (Institute of Risk Management, 2018). As do other standards, ISO 31000: 2009 makes reference to context, assessment, treatment, and monitoring. The superseded version of ISO 31000:2018 highlights importance of risk oversight and emphasises accountability, continuous communication, and monitoring. Thus, the version of 2009 adds merit. Additionally, ISO 31000: 2009's consideration in an early phase for appraisal of internal and external context represents another valid point of this standard.

Furthermore, the standard's effectiveness was supported by additional guidance such as BS ISO Guide 73:2009 vocabulary (BSI, 2009b), BS ISO 31010 assessment (BSI, 2011b), and BS 31100 implementation (BSI, 2011c); a fact that provides convincing evidence that its application fosters performance. For example, BS ISO 31100:2011 incorporates additional guidance in the form of principles and recommendations for the ISO 31000. Apart from its focus on RM processes and correlation with ISO 31000, it pays careful attention to details in the monitoring and reviewing processes, so capabilities, effectiveness, and optimised processes can be developed to counteract deficiencies in practice.

The updated version of BS ISO 31000:2018 keeps the initial principles and also expands upon the strategic approach to risks as it proposes to serve organisations' objectives achievement and performance (BSI, 2018a). For simplicity purposes, the 2018 version focuses on the importance of leadership and commitment and the value of implementing effective RM principles (adds a new perspective on value protection). It also reframes internal controls in processes (communication, scope, risk assessment, risk treatment, monitoring and recording, and reporting).

Figure 4-2 illustrate in more detail the above discussed.

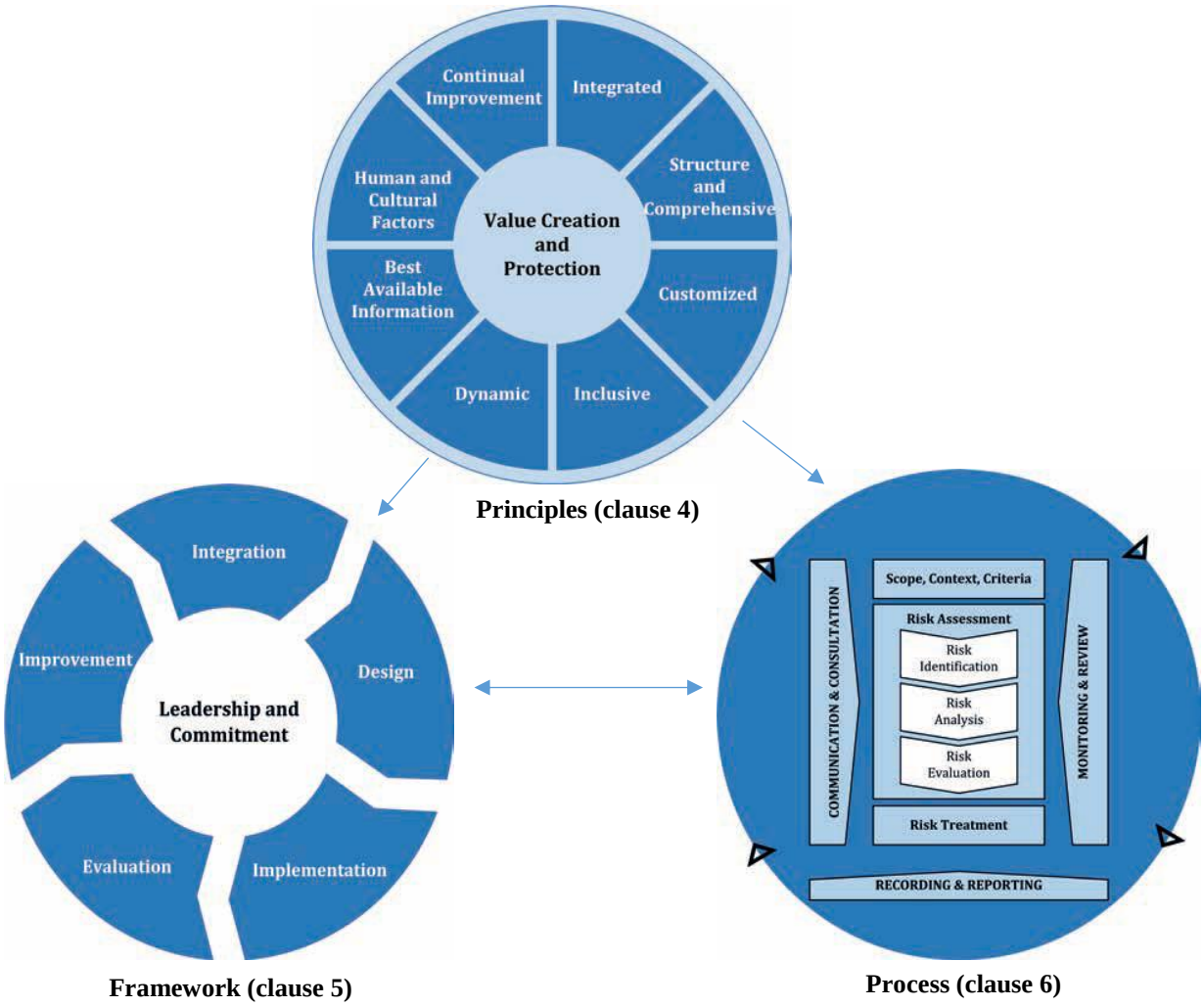


Figure 4-2 ISO Standard 31000:2018

Source: BSI (2018a)

Figure 4-2 presents the updated version of ISO Standard 31000:2018. For instance, RM principles are changed in the 2018 version. It also diverts focus from internal controls to value creation and protection (Institute of Risk Management, 2018). Moreover, the updated version shows consideration for RM integration with governance and emphasises the role of leadership in achieving RM maturity, both of which are valuable for current research *Framework* as a basic principle for achieving alignment of risk control, oversight and governance.

COSO Internal Control-Integrated Framework

In an effort to sustain organisations dealing with risk, the initial COSO (2004) Internal Control-Integrated Framework has been gaining importance over recent years as it strives to achieve an organisation's objectives based on strategy (direction) and the establishment of processes (instruction, assessment, control, communicate, monitor). Figure 4-3 below illustrates the COSO framework, which has evolved from basic control functions (in 1992) to a complex flow of risk control activities.

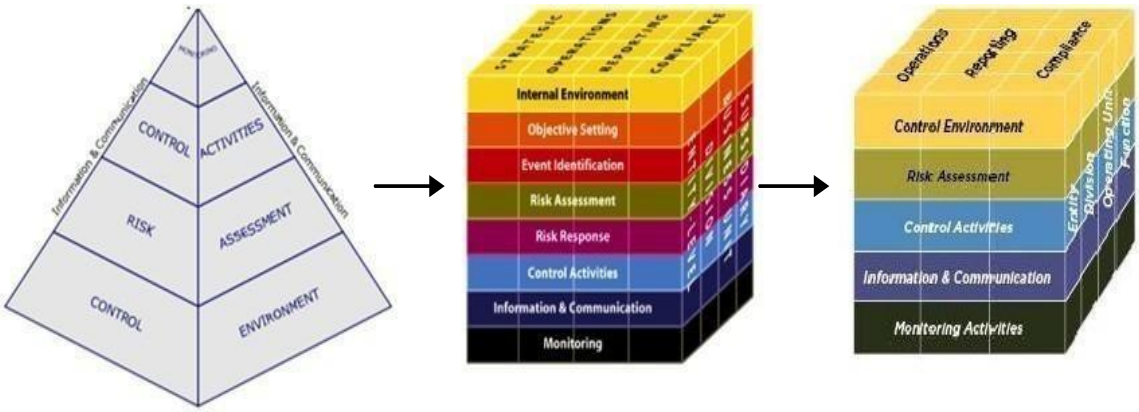


Figure 4-3 COSO framework evolution

Source: Keith (2015) cited in COSO (1992; 2004; 2013)

To compare the COSO framework evolution, Figure 4-3 illustrates its progress from 1992. Compared to ISO 31000, there are similarities regarding process deployment. In terms of complexity, the COSO framework represents a distinctive document; hence, all recommendation in its implementation is incorporated into one single document. In contrast, ISO series triggers the use of multiple supporting guidance and standards. Another distinction is that it only considerers the internal environment as a basis for implementation (e.g. risk appetite, organisational culture and philosophy) and considers external events only in light of internal events (incident). As well as ISO 31000, communication and monitoring are considered sustainable mechanisms.

There is most definitely a connection between standards. Therefore, the similarities that exist between them validate the applicability of processes; for example, regarding the Casualty Actuarial Society ERM Framework, a processual step is directly related to AS/NZS 4360. Based on a sequence of steps, the Casualty Actuarial Society Framework understands the value of creating a baseline before action is taken (e.g. assessment of context).

Relating to the evolution of COSO frameworks (as discussed in Section 2.4 and Subsection 3.3.2), the recent framework of 2017 raises an idealistic assumption of performance through the alignment of strategy mission, vision, and values.

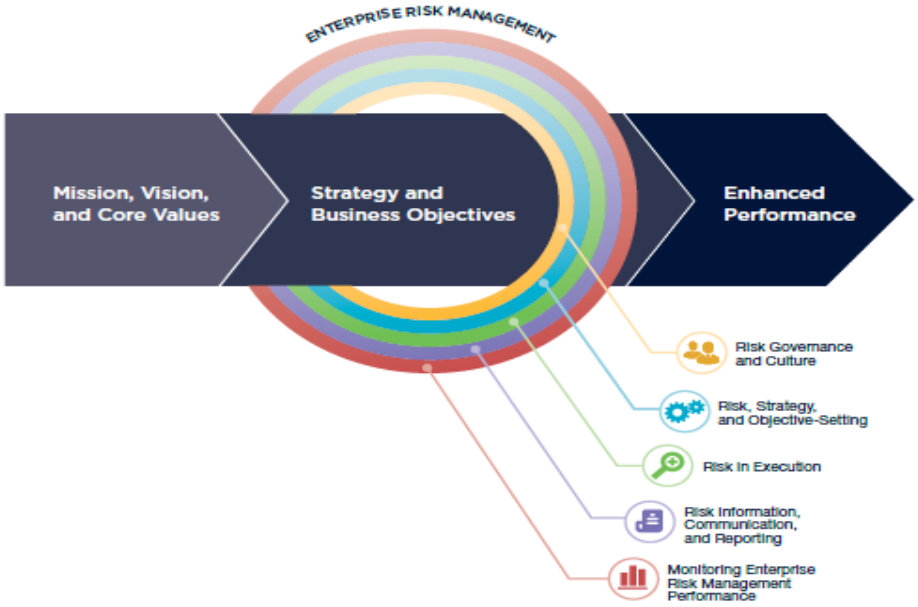


Figure 4-4 COSO's Enterprise Risk Management Framework 2017
Source: COSO (2016)

Figure 4-4 provides an overview of core framework functions in terms of risk oversight. The COSO 2017 reduces its components from eight initial components to five. Risk governance proposes a top-bottom approach, strategically managed to pertain the desired outcome. With a key focus on performance, the Enterprise Risk Management framework incorporates human aspects that can hinder in aligning strategy through a cultural component. Thus, it proposes an alignment of culture, ethics, and individual behaviour along with strategy alignment (COSO, 2016). Thus, it has been acknowledged that culture influences organisational alignment and performance. Compared to the 2013 framework, it has maintained the same components despite having slightly changed regarding terminology and having developed a focus in governance and performance.

However, the downside of the COSO framework is that while it considers technology for administrative purposes, it broadly omits to aggregate. Despite considerable contribution, COSO's Enterprise Risk Management Framework it is incomplete if contextualised in setting of research problem.

RIMS Risk Maturity Model

RIMS Risk Maturity Model (RMM) is a tool that helps to understand expectations (requirements) and to determine the status of an organisation's ERM maturity with the purpose of further forming developments and actions. Based on a five-level sequence, the model compares the results of ERM assessment against criteria for measuring the maturity. While RMM provides a perspective on organisational maturity, it also proposes continuous improvement plans for risk and control processes. Nevertheless, the purpose of the standard is mainly limited to the implementation phase (Q2) and measurement of the risk control processes.

4.3.1.2.2 ERM Advisory-specific frameworks (voluntarily)

In addition to the ERM standards mentioned above, advisory-specific organisations are additional players in developing strategic behaviour to sustain organisational performance. Table 4-3 illustrates the main ERM advisory-specific frameworks.

Table 4-3 ERM frameworks of advisory-specific organisations

Issuer/year	Framework	Industry focus	Domain	Key function
KPMG (2009, 2017a)	KPMG's ERM framework	Financial	ERM	Q1
Grant Thornton (2013, 2016)	Holistic Enterprise Risk management	Financial	RM	Q2
EY (2015, 2016)	EY's ERM framework	Financial	ERM	Q2
PwC (2009, 2015)	PwC's Comprehensive Framework for Assessing ERM	Financial	ERM	Q1, Q2, Q3
McKinsey (2013a, 2013b, 2016)	McKinsey's Enterprise Risk Management framework	Financial	ERM	Q2

Source: The Researcher

As summarised in Table 4-3 the ERM advisory-specific frameworks are identified as key contributors that happens to be tailored specifically to financial industry.

KPMG's ERM Framework

KPMG's ERM Framework 2009 proposes an approach based on risk governance, assessment, risk quantification, and control basis for performance enrichment. KPMG provides a useful approach to risk control function, emphasising the ERM benefits. Like many other frameworks, it recommends using a cyclical approach of a five-step sequence that concentrates on the management of organisational risks. A holistic approach that acknowledges the dependence on culture, communication, infrastructure, risk aggregation, and/or risk reporting (KPMG, 2017a). The way in which the framework develop refers to a strategic, operational, and social alignment in one single framework. Granting the value of a diverse perspective, this framework may serve as a descriptive guideline for ERM categorised as an adoption advocate (Q1). Overall, it provides a generic description that

discusses the value of ERM and not necessarily how enterprise-wide features can be achieved through strategic means. It specifically aggregates the financial industry's risk, while in comparison with the proposed research Framework it addresses only a partial perspective on enterprise risks instead of full addressability.

Grant Thornton's Holistic Enterprise Risk Management Framework

Grant Thornton (2013, 2016) provides a framework based on a top-down approach, formulated cyclically (similar to KPMG framework) and relying on governance, strategy, and risk culture to support the risk response processes. Grant Thornton's framework is grounded on RM approach and driven by two main industry frameworks: ISO 31000 and COSO. On this basis, it recommends achievement of business strategy through the incorporation of governance, risk culture and compliance. Apart from its initial strategic focus, it considers the integration of operational and social dimension to be variants in RM deployment. Therefore, the Grant Thornton's Holistic Enterprise Risk Management Framework has an operational focus (Q2) rather than theoretical. Thus, the theoretical premises of this framework are scarce but abundant in details of applicability and execution. The issue whether this framework is comparable with the research Framework is impractical, as it mainly addresses a partial perspective under a siloed approach of RM.

EY's ERM Framework

Ernst and Young's (2015, 2016) ERM Framework is an integrative framework of RM within the financial industry, guided by the integration of culture within processes, operations and strategy. A noticeable characteristic of this framework is that it examines the relationship between human side and risk culture aggregated in risk governance (EY, 2016). Overall, it promotes an integrative mechanism to support avoidance of decentralised risk control. Apart from this highly valuable contributing derivation, it validates the view that internal and external factors are desirable elements and are thus should be considered. However, it tackles a partial perspective of implementation (Q2) and omits ERM maturity assessment and compliance maturity.

PwC's Comprehensive Framework for Assessing ERM

PwC (2009, 2015) forecast that leadership is essential if embedded in risk oversight. Based on leadership, the RM aggregates with organisation governance and strategy across all business functions. Similar to KPMG's framework, PwC follows the same format of the five-step sequence. They include strategic and operational aspects of execution and define

its expectations beforehand through a risk appetite framework. In addition, it shows benefits of executives' involvement by highlighting dependency on risk culture, role responsibilities, and organisation structure. Despite its main focus on assessment (Q3), PwC's Comprehensive Framework for Assessing ERM is by far the most complete advisory framework; hence it addresses three components of maturity: Quadrant 1 Adoption (Q1), Quadrant 2 Implementation (Q2), and Quadrant 3 Maturity assessment (Q3). It omits to consider Quadrant 4, assessment of compliance.

McKinsey's Enterprise-Risk-Management Framework

McKinsey's Enterprise Risk Management Framework is strategic driven and is structured similarly to other frameworks in five-cyclical steps (e.g. Grant Thornton, KPMG and PwC frameworks). The framework incorporates a combination of top-down and bottom-up approaches, hence it combines strategic (e.g. strategy, appetite, governance) and operational dimensions (e.g. processes, transparency) of implementation. It incorporates culture, communication, compliance, and governance in deploying integrated risk decisions to ensure performance, with specific consideration paid to the insurance sector. It engages operational aspects of implementation, scrutiny, and maintenance and is thus prescriptive in its form. Regardless of its derivation and its specific guidelines for implementation (Q2), by influencing practices for an organisation, this framework only partially addresses the research problem and is thus limited in applicability. While it is valuable in influencing sound practices for an organisation, regrettably it addresses only one limited perspective (adoption and ERM) relating to the research problem.

4.3.1.3 ERM regulators' frameworks

In the case of regulators, the requirements for a proper governance of ERM imposed by laws and regulations include risk oversight, assurance, transparency and disclosure among many other factors; a fact that has triggered the development of norms. Overall, the norms are intended to avoid suboptimal practices concerning risk and in turn ensure basic resiliency. Along with its authority, the regulators' recommendations (mandatory or voluntary) derive from further developments in the industry (e.g. standards, guidelines, frameworks, models). As an illustration, the case of the Combined Code of the Committee on Corporate Governance (2003) (also known as Turnbull guidance or the Guidance for directors on the Combined Code, 2005) reinforces the value of internal control in organisations in order to assure quality, compliance, and efficient operation. Its content emphasises the accountability and monitoring responsibility of management in communicating the risk to boards of

directors. Nonetheless, although these Acts praise themselves as frameworks, they in fact embody mandatory rules that omit the operative aspects of implementation. Therefore, apart from legal aspects and guidance, two main frameworks are identified—see below table (Table 4-4).

Table 4-4 ERM regulatory framework, guidance-specific

No.	Issuer/year	Framework	Industry focus	Domain/s	Key function
1.	HM Treasury (2009)	RM Assessment Framework (RMAF)	Government and generic	RM	Q3
2.	HM Treasury (2004)	The Orange Book - The Risk Management Model	Government and generic	IA: RM	Q3

Source: The Researcher

Although the above are applicable to the public sector, due to the scarcity of specific regulatory framework for the financial industry, the Researcher makes reference to them as good ERM practices. Table 4-4 is similar in terms of industry focus (Q3) yet has some reminisces of Quadrant 1 which promotes good practices beforehand adoption.

RM Assessment Framework (RMAF)

RMAF (HM Treasury, 2009) is a generic framework that proposes to be a standard tool for organisations that want to assess their internal RM standard It focuses on leadership, partnership, processes, and risk handling to achieve the expected performance and progress after implementation. Mainly focused on assessment of RM, it makes use of its ability to handle risk (HM Treasury, 2009). Moreover, it aims to foster good practices of internal risk control and resources. It highlights the importance of a top-down approach and human aspects that contribute to the development of a RM framework. Despite its valuable insights, RM Assessment Framework remains an assessment tool (Q2) and adopts a siloed perspective, and as such it only considers enterprise risks through the perspective of traditional RM.

The Orange Book - The Risk Management Model

Perceived as a model, the Orange Book - The Risk Management Model promotes itself more as a guidance of internal control. What stands out in both regulatory frameworks is the general pattern of indicating what is expected along with the importance of the ongoing review of practices. Its directive aspects aim to influence improvements of risk control. By understanding the capabilities of internal controls, risk exposure, and more importantly risk appetite, public sector organisations will be expected to be more efficient regarding their

approach to risk (HM Treasury, 2004). Unfortunately, it mainly considers the RM and its measurement and neglects to consider enterprise-wide and cybersecurity aspects.

4.3.2 Cybersecurity Management frameworks

This subsection incorporates different sub-domains of CsM and shows the variations across academia, industry and regulators.

4.3.2.1 CsM academics' frameworks

To assess the contribution of CsM frameworks, this section particularly evaluates academic framework contribution. This isolated perspective is later compared with the qualities and limitations of practitioners' and regulators' frameworks in order to understand the position and value of the proposed *CsM - ERM Strategic Alignment Framework.*

Table 4-5 below summaries the identified CsM frameworks that are related or specifically referred to as CsM frameworks. Due to limited literature and semantic confusion of the CsM domain, the terminology varies. However, these aspects were clarified previously in Chapter Two, Sections 2.5 and 2.6.

Table 4-5 CsM conceptual frameworks

No.	Issuer/year	Framework	Industry focus	Domain/s	Key function
1.	Posthumus and Von Solms (2004)	Information Security Governance (ISG) framework	generic	IS: RM	Q2
2.	Da Veiga and Eloff (2007, 2010)	Information security governance framework	generic	IT, IS: business	Q2
3.	Ma *et al*. (2009)	Integral framework for IS Management	generic	IS: business	Q1 and Q2
4.	Saleh and Alfantookh (2011)	Information Security Risk Management (ISRM) framework	generic	IT/IS: RM	Q1 and Q2
5.	Atoom, Otoom and Abu Ali (2014, 2017)	Holistic Cyber Security Implementation Framework (HCS-IF)	generic	CsM: RM	Q2
6.	Web *et al*. (2014)	Situation Awareness Information Security Risk Management (SA-ISRM)	generic	IS: RM	Q1

Source: The Researcher

The evidence illustrated in Table 4-5 provides a summative insight on how CsM is defined, categorised, and pertained. A more detailed assessment of derivations and limitations is discussed below for research framework justification and validity purposes.

Information Security Governance (ISG) Framework

The exemplification of Information Security Governance (ISG) framework of Posthumus and Von Solms (2004) points out that integration requires a combined governance in order to direct and control the management of IS. Besides its integration recommendations, the *ISG framework* associates technical CIA triad criteria with practice, referring to internal and external risks as prerequisites that complement informed decisions. The framework

contributes by providing positive supportive evidence of integrating IS with RM. However, it omits details in how functions control (governance and management) shall align. Consequently, the framework validates the value of integrating IS to organisational governance and suggests practical implications of understanding the internal and external factors before implementation in order to avoid negligence and uninformed decisions (Posthumus and Von Solms, 2004). Perhaps, a valuable insight can be obtained if a preliminary analysis of governance maturity is identified and correspondingly a further target state (anticipated) proposed. The security is limited to information assets (no valuation of other assets is recommended). Thus, the practicality of the framework is limited regarding applicability (even if its main focus is on implementation (Q2)) due to its conceptual aspects. Overall, the lack of details in regard to its applicability and restriction to a silo approach (information assets) of traditional RM that is driven by two determinants (leadership and competitive advantage) delimits the framework to a core function of implementation (Q2) with some consideration to support adoption (Q1). In short, the Information Security Governance (ISG) framework represents a governance baseline, adopted by many studies but incomplete in terms of accommodating today's evolving context.

Information Security Governance Framework

Da Veiga and Eloff's framework is constructed on the premise that the protection of information resources can only be initiated through the provision of cultural awareness. Thus, the authors claim that a proper cultivation of culture should protect an organisation against loss (Da Veiga and Eloff, 2007). On these premises, awareness, education, training, ethics and ethical conduct shall compound a code of conduct as a guidance of managerial expectations that influence attitudes and behaviours to risks. Although this represents only a side of a holistic plan to increase risk oversight, it delimitates the fact that governance encompasses multiple elements. Henceforth, the human behaviour towards cyber risk can influence/impede an organisation's achievements (Da Veiga and Eloff, 2010). It represents partial applicability (social) of a holistic approach in the context of IS and business. Broadly, the Information security governance framework tends to focus mainly on cultural aspects yet somehow it over-emphasises its impact and neglects the enterprise-wide strategic directions and implications.

Integral Framework for IS Management

Furthermore, in the Integral Framework for IS Management, Ma *et al*. (2009) suggest a structure in a five-step process (assess, establish, analyse, develop and implement), with the

purpose to align security goals with business strategy. Whilst valuable for strategic reflections and its consideration for internal and external requirements, the drawback of this framework is that it considers only IS and does not accept integrating RM or ERM. It combines strategic aspects, and operational dimension in the context of IT/IS, but remains traditionally embedded in the protection of information and information systems (i.e. refers to computer security) and recommends alignment with business strategy. A more comprehensive approach would include alignment with other control functions (RM, ERM) that would sustain the organisational goal achievement. Nerveless, it neglects to incorporate the new dimension of cybersecurity that moved from computerisation and informatisation phase, towards a cyberisation paradigm. Additionally, the non-empirical evidence categorises the framework as a conceptual framework. Synthesising the Integral Framework for IS Management, this conceptual framework builds its structure on a simple construct (IS) to validate the theoretical value of aligning security goals with business strategy for integrated objectives. Another drawback is that the order of steps recommended duplicate themselves (e.g. assess and analyse) due to assessment meaning identification, analysis, and evaluation. Overall, the framework of Ma *et al*. presents a contribution to IS domain but is limited to an IS silo approach and unclear path of direction, hence the framework initially being described as strategic but in reality, it refers to operational and technical aspects.

Information Security Risk Management (ISRM) Framework

The Information Security Risk Management (ISRM) framework of Saleh and Alfantookh (2011) is based on the STOPE view, which considers strategy, technology, organisation, people, and environment as a scope to construct the cyclic DMAIC (define, measure, analyse, improve and control) processes. Formulating this approach to implementation and control, the framework identifies itself as conceptual. Like many other frameworks, it validates the value of risk profile identification and additionally highlights the importance of responsibility for identification and classification of assets in a descriptive manner. Concerning the framework structure, is identified as a preparatory descriptive that fosters adoption yet is inclusive with a procedural dimension and thus focused on implementation guidance (Q2). Nonetheless, the framework's drawback is that it mainly has an operational focus and is valid in its applicability only with additional support. Therefore, an implementation requires prior preparation (planning), planned investments, and an implementation strategy that relies on initial organisational objectives - for all of which it represents a strategic approach; an aspect neglected by the Information Security Risk

Management (ISRM) framework. Much work on the potential of IT/IS management implementation in RM context affects organisational strategy (measurement), and consideration for the alignment paradigm might be carried out if a wider assets reflection were to be considered.

Holistic Cyber Security Implementation Framework (HCS-IF)

The Holistic Cyber Security Implementation Framework (HCS-IF) of Atoom, Otoom and Abu Ali (2014) intends to control risk and to recommend strategies that evaluate its implementation's maturity. Even if the framework is to be employed by governmental bodies, the basic principle of goal identification triggers prioritisation based on valuation. As a result, implementation occurs post-evaluation of existing control state, as an effect of valuation that stimulates the appropriate formation of strategic controls. Demonstrably, this represents a superficial approach due to the lack of details provided by the framework but nonetheless accounts for a positive initiative to signpost the value of a holistic approach to control and audit risk.

However, in comparison to other frameworks, it at least uses appropriate terminology (i.e. even if in a different form 'cyber security', opposed to the form used by the present research 'cybersecurity'). Recommendation to assess an organisation's existing state sets the context for future maturity levels. Posthumus and Von Solms, 2004, considered a similar approach in their framework. Another point worthy of consideration is that it identifies basic principle, despite its incomplete sequence (e.g. monitoring, improvement). Therefore, it argues that implementation is sufficient and runs automatically.

Covering only one phase (respectively implementation (Q2)), this framework represents a partial solution for the research problem as is omits to explain how it relates to RM and more specifically how it integrates with business objectives. RM is a traditional approach to risks (Lundqvist and Vilhelmsson, 2016), and thus, an incomplete strategy. Additionally, CsM is addressed as operational and technical, and the framework lacks risk governance alignment correlation with business strategy. Perhaps less focus on software engineering, operational aspects, and IT-related concentration would redirect attention to a more transparent and strategic directions and implications.

Situation Awareness Information Security Risk Management (SA-ISRM)

From the above findings, it is clear that directing, executing, and controlling a framework is a complex process. As emphasised in the previous framework of Atoom, Otoom and Abu

Ali, the processes are often formulated superficially. In support of this view, Web *et al*. (2014) focus mainly on assessment and the development of a framework even if it were to represent a partial solution. The Situation Awareness Information Security Risk Management (SA-ISRM) provides confirmatory evidence that before any action is to be taken, an assessment is imposed to identify and collect details about the environment, looking at the past and current organisational profile, governance results, and the way it prioritises its actions. So, it considers all sources of risk (Web *et al.*,2014a) pertaining to internal and external pressure. However, despite being valuable for a pre-implementation phase (Q1), it is incomplete because it only addresses the protection of information resources in a single phase; a fact that indicates it is incomplete on its own.

4.3.2.2 CsM practitioner's frameworks

This subsection portrays the practitioners' influence on practices and extract derivations. In some cases, the baseline practices are described as frameworks or standards. Table 4-5 illustrates this fact.

4.3.2.2.1 CsM frameworks of mandatory-specific organisations

This subsection is particularly focused on mandatory-specific frameworks, respectively standards. Below, the identified main standards are illustrated.

Table 4-6 CsM frameworks of mandatory-specific organisations

Issuer/Year	Framework	Industry focus	Domain/s	Key function
BSI (2011a, 2013b, 2017a)	ISO family standard series	generic	IS	Q2, Q3
NIST (2013, 2014)	NIST family standard series	generic	CsM	Q2, Q3
OCTAVE (1999, 2003, 2007)	OCTAVE series	generic	IS	Q3
ICAS (2011)	ICAS Information Security standard	generic	IS	Q3
PAS 555 (2013)	PAS 555 standard	generic	CsM	Q2
IASME Standard (2013)	IASME framework	generic	IS	Q3
ISF (2011)	Information Security Forum Standard of Good Practices for Information Security	generic	IS	Q2

Source: The Researcher

From Table 4-6 shown above, it can be seen that CsM frameworks are scarce and most often are grounded on traditional views of IS. Based on these finding, the following section examines the practical and theoretical relevance of the frameworks in more detail.

ISO family standard series

Among practitioners' frameworks, the ISO family standard series provides guidance about planning, implementing, controlling, and assessing risk by supporting and supplementing different aspects of their interrelationship based on the basic principle used across ISO standards: plan, do, check, and act (initially cultivated by Deming's PDCA cycle method) (Salaheddine and Ilias, 2017). Based on this principle, the standard family is constructed and has different purposes that result in, for example, all ISO standards being aligned towards a baseline standard to support the applicability over various dimensions.

The initial BS ISO/IEC 27000 establishes vocabulary and a sound baseline for the whole series related to IS. Furthermore, ISO/IEC 27001:2013/2017 (BSI, 2013b; 2017a) establishes requirements for preparing implementation and maintenance. The characteristic of this standard and its contribution lies in the fact that behind the main goal of implementation, internal and external issues that can interfere with the action are considered. Additionally, it is driven by the assessment of organisational needs and establishes resilience. In this research, the assessment process of organisational needs (scope, boundaries, and applicability) and risk assessment structure is extracted as a derivation from this standard.

Although not designed for the financial industry, BS ISO/IEC 27001 is one of the most heavily used (CSIS, 2015) and its employment demonstrates compliance and risk preparedness. One drawback of this standard is that it perceives security through information systems/information security yet combines both strategic and operational perspectives. Besides, it is grounded on the old approach of information security which focuses on the security of information and system within which they operate. Whereas cybersecurity sees outside its systems or information assets hence, it intends to protect more than just information (discussed previously in Section 2.6, Chapter Two).

BS ISO/IEC 27003:2017 (BSI, 2017d) consolidates the implementation guidance initiated by BS ISO/IEC 27000, 27001 and 27002 as indispensable due to its value for documentation and direction for planning the implementation. The planning process is based on a five-step process: approval, scope identification, analysis of the organisation, assessment, and final design of implementation. The standard developed a logical structure, which is to be followed before implementation. This evidence supports the framework with its legacy regarding scope clarification, organisational planning, analysis, and design.

BS ISO/IEC 27004 advances an understanding of implementation maturity by evaluating and verifying the performance by subjective (human judgement) or objective (numerical) value (BSI, 2016b).

The purpose of BS ISO/IEC 27005 is to align IS with RM and develop a procedure based on a four-step process of plan, do, check, and act (BSI, 2011a; 2018c), which has its roots in a quality control approach. The simple procedure starts by establishing the plan that builds its structure on identifying the context. The 'do' refers to the implementation based on the previous phase of assessment that leverages implementation of a treatment plan. It then incorporates 'check', which relates to the process of monitoring and reviewing of the process. Finally, 'act' is a continual process based on previous processes which were developed to improve existing practices and recommend good, new practices. For the purpose of this research, all processes stem from this standard.

Although several standards and frameworks have proposed different approaches to strategically align IS and RM in an effort to explain the dynamic of implementation, the BS ISO/IEC 27005 differentiates itself because it proposes first to identify the organisation's boundaries and scope before undertaking any actions. It considers the organisation's objectives, function and structure, legal regulatory and contractual requirements, policy, approach to RM, assets, locations, constraints, cultural environment, and, finally, expectations. The drawback is that it considers assets from an information perspective, while RM considers assets as well as people, technology, and processes. Regrettably, IS on its own has a silo approach (risk considered in isolation) and its emphasis is on the security of assets that are stored electronically (information systems) as opposed to CsM, which considers all types of assets. While the standard has proposed to act holistically, in fact, it uses a two-silo approach to risk: IS and RM that considers tangible and intangible (digital) assets.

While all ISO standards refer to security from an information system point of view, the BS ISO/IEC 27032 standard differentiates itself by using the terminology 'cybersecurity'. The standard provides confirmatory evidence for inconsistency among practitioner's terminology and articulates that IS mainly concerns the protection of information (e.g. personal information, trade secrets, employee data, financial data) and therefore the standard represents another fact that proves CsM to be different from IS. However, apart from this terminology evidence and other definitions of concepts, the standard represents a technical guidance, and in this research mainly theoretical aspects are considered.

NIST family standard series

Clarification of terminology plays a significant role, and NIST family standard series demonstrates the feasibility of cybersecurity terminology. For instance, the Risk Management Framework (RMF) version 1.0 developed by NIST is widely used and differentiates itself by the fact that it addresses industries that are part of a critical infrastructure. With the purpose of managing risks, the framework applies the practices of RM and suggests an alignment with business objectives. Based on this recommended approach, business, and technology are aligning together towards the same goal (NIST, 2014). By these means, it addresses the strategic and operational approach.

For this research, considerations about profile identification (organisational risk profile) and target profile function (anticipated state) are extracted from this framework. Furthermore, detection and response incorporate technical and operational aspects and fr this reason were dismissed. The last function of recovery might incorporate all three dimensions: strategic, operational, and technical.

OCTAVE series

Incidentally, OCTAVE series are considered for their contribution to qualitative risk assessment of information assets. There are three Octaves (Octave, Octave-S, and Allegro) that form the Octave assessment family. Firstly, the frameworks propose to optimise the procedure of an assessment process for risks. They focus on qualitative evaluation and thus consider an evaluation based on the qualitative identification of assets, vulnerabilities, and threats (Octave Allegro, 2007). Even if the framework uses a qualitative method and is exposed to subjectivity due to a lack of numerical rules (objective), it measures its success against how many times it is adopted by organisations.

Secondly, it mainly considers operational risk regarding assets. The profile of the framework derives from asset protection. Its focus is on the assets profile and threats, and the means to mitigate assets' risks through an operational perspective. Thus, the framework omits the holistic view of CsM approach by primarily considering the information assets risk profile. Despite questions regarding the holistic approach, the Octave series' contribution lies in the fact that it establishes basic principles of risk assessment. This is an essential step that, in combination with other measures, leads to a more consistent way to strategically respond to risks. These partial answers outline the methodology of identifying the organisational approach to risks; followed by a second step of assessment, which creates the asset's profile

and in turn leads to an optimised process of prioritisation (should the case arise). As previously shown, the OCTAVE is based on operational and to some extent technical aspects of risk assessment. For the purpose of this research, assessment considerations are extracted from this framework series.

ICAS Information Security standard

ICAS Information Security Standard complies with the Octave series and has an operational focus. The control is set based on previous steps of risk profile and asset identification. While its structure is similar to that of other standards, it contributes to the clarification and validation of the control selection stage.

PAS 555 standard

Equally as relevant, other standards such as the PAS 555 broaden the applicability of a framework from internal to external, thus considering an extended approach that verifies all associates' entities (e.g. partners, third party, suppliers) security measures. As well as other frameworks, it considers Asset Management (identification, measurement and protection) across all stages. Additionally, asset management is part of the risk assessment stage that incorporates threat management and vulnerability management. Therefore, it considers assets, the assets' exposure, and possible vulnerabilities. Moving on, the framework proposes mitigation measures that ensure people security, physical security, and technical security to assure resilience preparedness. Once again, the incorporation of all these components confirms that CsM is complex and in turn, combines information assurance and technology security (BSI, 2013a) and is therefore different from IS. To better understand the discrepancies of terminology, a comparison can be made with the ISO family series. For this research, elements such as risk assessment, mitigation, detection, and response are extracted from this framework. The recovery phase is excluded due to its operational and technical aspects.

IASME framework

The dynamics of cybersecurity challenges determine over the years a multitude of guidance and frameworks. However, few consider advocating this approach for SMEs. Whereas most standards are generic and address large organisations, the IASME framework offers useful guidance to assess, adjust, test effectiveness, and recommend security needs. Nonetheless, its tendency is operational and technical, differing from the scope of this research. For this research, the sub-domains of assessment as risk identification, assets evaluation, monitoring,

and continuity are extracted from this framework. Additionally, the score matrix that evaluates the maturity of an organisation's security is a good example to consider (for example, initial, minimal, in use, managed, control, and optimised).

Information Security Forum Standard of Good Practices for Information Security

Given the lack of attention paid to effective control of security models, the Information Security Forum Standard of Good Practices for Information Security (ISF, 2011) contributes through its focus on compliance and Asset Management. By initiating this approach, it shows an integration of strategic and operational structure through simplicity and efficiency (ISF, 2011). Regrettably, there is a divergence regarding what the framework proposes to do, and thus it addresses a significant part of its content to compliance (for example, references to policies and documentation) and omits an in-depth focus on other attributes, contrary to its initial statement to deploy a strategic model based on governance of risk. Another drawback is that even though it discusses IS, the fact that it refers to the protection of assets, people, processes, and technology is actually a reference to CsM. While the framework is more informative in this context, it is worthy to consider the benefits of the framework, respectively the potential of regulatory requirements to form a basis for assessment criteria and additional consideration of Asset Management. The underlying concept recommends a determination and classification of assets to determine the potential loss in case of an incident. While these steps have operational aspects, they also incorporate a strategic approach to identifying the purpose of CsM strategy before design and implementation. They also serve to determine the level of investment required based on the evaluation. As per derivations for the research *Framework,* compliance criteria considerations and asset valuation are extracted from this framework as a guide for assigning a value to organisational assets.

4.3.2.2.2 CsM vendor advisory-specific frameworks (voluntarily)

This subsection emphasises main practitioners' frameworks that are vendor-consultancy specific for a general comparison. Within this scope, Table 4-7 summarises main frameworks related to CsM under several terminologies such as focus and functions. As thus, derivations are subject to limitations.

Table 4-7 CsM frameworks of advisory-specific organisations

Issuer/year	Framework	Industry focus	Domain/s	Key function
Ernst and Young (2014b)	Cyber Program Management framework	Generic	IS: RM	Q2
KPMG (2015, 2016)	Global Cyber Maturity framework	Generic	IS: RM	Q3
PwC (2014)	Cyber Risk Management framework	Financial industry	IS: ERM	Q2
Deloitte (2015e)	Cyber Risk Management framework	Generic	CsM: RM	Q4
Grant Thornton (2016)	Cyber Risk Management framework	Generic	IT: RM	Q1

Source: The Researcher

As Table 4-7 illustrates, few consultancy organisations endorse good practices of risk governance. Further analysis of the frameworks underlines differences in their quadrant focus, ranging from adoption stimulation (Q1), implementation (Q2), maturity assessment (Q3) or maturity compliance (Q4).

Ernst and Young's Cyber Program Management Framework

Ernst and Young's Cyber Program Management (CPM) framework of 2014 focuses on implementation (Q2) and is based on IS and RM principles. Aiming to enhance performance, flexibility and scalability, the framework suggests that alignment of security with business is a feasible solution (EY, 2014b). The framework advocates a strategic approach to sustain a multi-tiered alignment of structure, culture, and risks continuously. Consequently, if an organisation has difficulties in synchronisation of architecture, operation, and awareness (EY, 2014 a, b), a strategic centralisation shall identify enterprise-wide risk exposure and in turn respond accordingly. While the purpose is to widely 'identify, protect, sustain, and optimise' an organisation's risk control, the framework is restricted to technological-centric and information assets protection. Therefore, the drawback of EY's framework is that although it considers IS, RM and their alignments, it refers mainly to a partial valuation of assets. It thus omits to address identification and protection properly; respectively an integrated approach.

KPMG's Global Cyber Maturity Framework

KPMG (2015) Global Cyber Maturity framework has a strategic and operational focus and differentiates itself through its consideration of six domains: human factors, leadership, governance, business continuity, operations, and regulatory considerations, all of which are led by enterprise-wide communications among all departments. Moreover, its function of assessment (Q3) helps organisations identify their cybersecurity maturity. Additionally, the initial framework from 2014 suggests that a cybersecurity framework should be embedded

in organisation culture and thus the strategic decision would be taken in a more informed manner. Hence the risk oversight strategy integrates all units/departments (KPMG, 2015). An additional version of 2016 placed more emphasis on boards involvement. While this framework is beneficial in understanding the maturity of strategic alignment, it remains dependant on being implemented together with other framework/s and thus mainly concentrates on promoting baseline practices of risk oversight (Q1) and maturity assessment (Q3). Apart from its partial applicability, it considers alignment through a strategic and operational perspective, with an emphasis on leadership and communication correlation with business continuity and crisis management, operation and technology, and compliance. Furthermore, KPMG's Global Cyber Maturity framework 2016 demonstrates consideration of information protection in the context of RM and omits to consider the wider spectrum of assets and enterprise security while also failing to explain communication and leadership deployment in the context of the framework.

PwC's Cyber Risk Management Framework

PwC (2014) Cyber Risk Management framework's main purpose is to encourage and support organisational resiliency, specifically regarding the needs of the financial industry. Its strategic approach relies on the involvement of management executives and aims to leverage an optimised governance that incorporates and correlates RM functions across the all the organisation. Consequently, it involves executive management, and its philosophy is based on the need for leadership in deploying and implementing the framework. Thus, the pillars of the framework are grounded on the provision of governance, the establishment of perimeters boundaries, identification of what needs to be protected, identification of potential dangers, and a plan to communicate and respond. In short, it considers its priorities, its response planning, resources allocation, and required investments. Its core function is therefore categorised in Quadrant 2 implementation and as such fails to address the key aspects of ERM (Q1, Q3, Q4). However, this specific framework it only partially addresses implementation (Q2). While it considers both capabilities of IS and ERM, in a business context it partially addresses cybersecurity hence it focuses only on IS and uses the term 'cyber'. Also, it considers two components yet omits to discuss their strategic alignment and how this approach is applied. Instead, it focuses more on operational aspects. As a result, the PwC's Cyber Risk Management framework represents an incomplete strategic alignment.

Deloitte's Cyber Risk Management Framework

Deloitte's framework provides insight into control and assessment to ensure against cyber threats, and does so based on 'three lines of defence': management, RM and internal audit. Although valuable, the assessment represents a partial perspective (Q4) of the research problem. Deloitte's framework reflects an exploration of channels of communication, RM capabilities, and deployment of an internal audit. The framework would have been more relevant if a wider range of components (not just people, processes, and technology) and more enablers were taken into account (e.g. cyberspace, practices, assets, information, culture). Apart from its consideration of assets valuation, an avoidance of pattern-based decision (IT-driven) would be recommendable. Nevertheless, involvement of board executives in incidents is unfeasible and operational driven. Perhaps executives involvement wold be justified only in exceptional cases of significant incidents. In such cases, the settled strategical proposal approach is contradictory. With this approach, Deloitte's Cyber Risk Management framework fails to state differentiation between strategic and operational elements. For instance, external threats are emphasised more than internal threats. Moreover, they promote a cyber prioritisation that is technically focused (e.g. forensic, incident response) and omit considering how they relate to business strategy, how they align, and how the framework is embedded in organisational plan, strategy, or policy. The framework also fails to grasp ERM fully and complements it with COSO's 2013 framework. The framework is mainly descriptive, with few considerations for the strategic approach (valuation, risk profile and risk appetite) and an incomplete distinction in how cybersecurity and ERM contribute together.

Grant Thornton's Cyber Risk Management Program

The approach described in Grant Thornton's framework may provide information about the association of cyber risk strategy aligned to business strategy. However, the entire content is IT-driven and focused towards the achievement of organisational performance. This in turn represents a weakness in contrast to the research Framework. There is no indication of how the framework will be implemented and thus it mainly fosters the adoption of a holistic approach (Q1). Although the framework encourages an enterprise-wide approach and calls for a management shift towards being integrated, there is an unclear differentiation between strategic and operational elements. Respectively, a technical component (i.e. policies, firewalls, assets management tools seen as key components of cyber risk management program) is, in fact, a confusion of strategic and operational components. Among the

relatively minor weaknesses of the programme are the fact that the terminology and meanings are insufficiently defined (e.g. cyber confusion with digital; cyber risk instead of cybersecurity; RM with ERM) and emphasise IT (thus, a silo approach). For instance, "ERM systems typically focus on data, systems and compliance without taking a holistic approach" (Grant Thornton, 2016, p. 7) and is defined as a reactive and siloed approach, seemingly a risk-based software perspective different from the strategic approach of ERM. The proposed consideration for security emphasises the second stage of cybersecurity development, respectively IS. Although IT-centric, the framework illustrates the context of security of information (e.g. customers' details, vendor data, trade secrets) and information systems, as well as failing to consider the wider security perspective of assets considered by modern cybersecurity (only consider protection of digital assets). In short, the approach is rooted in both IT and IS alignment to business and demonstrates positive consideration regarding modern cybersecurity through the inclusion of people protection. Overall, the Grant Thornton's programme (framework) is likely to be strategic due to its operational embedded approach and IT considerations. Additionally, the application of the programme is briefly discussed, and thus it covers a first stage, respectively adoption (Q1) and a silo perspective of adoption (performance).

While KPMG, PwC and Deloitte are guided by leadership and governance capabilities as their core functions, EY's framework adopts a different stance and articulates how performance can be attained by describing a sequence of steps that should be undertaken to achieve a performance in implementation. The consultancy frameworks advances leadership and performance attainment, implementation, and assessment/verification functions and distinctive terminologies (i.e. KPMG's framework is the only framework that emphasises 'cybersecurity'). Moreover, among all four frameworks, PwC's framework solely considers the financial industry.

4.3.2.3 CsM regulators' frameworks

Apart from the regulatory contribution from many laws and guidelines, regulators have also contributed to regulatory frameworks.

Information Assurance Maturity Model and Assessment Framework

The CESG Cyber Security Model is a unique model that incorporates details concerning how maturity can be achieved and how its compliance can be assessed (CESG, 2015). Although its addressability is directed at governmental bodies, its structure can be applied to

organisations. This model validates the framework of Luftman (2000) due to similarities and this in turn emphasises that an organisation's profile is significant. Besides this, it contributes to the assessment phase and therefore recommends a maturity assessment of leadership and governance, training, education and awareness, Information Risk Management, implemented controls, and compliance. In contrast, other standards and frameworks have addressed the assessment of risk controls. Thus, the Information Assurance Maturity Model and Assessment framework of CESG provides more than assessment, advocating a before and during preparation approach along with education and knowledge sharing. Nevertheless, it remains embedded in maturity assessment (Q3), dependent on ISO/IEC 27001: 2005 and oriented to a siloed approach of information assurance and RM.

4.3.3 Strategic alignment frameworks

Owing to the fact that the research regarding alignment is limited to IT business alignment (Karpovsky and Galliers, 2015), this subsection aims to demonstrate its roots and developments. Consequently, past approaches are analysed even though they mainly focus on the traditional paradigm of IT and in most cases omit security consequences. This additional subsection is complementary to CsM due to IT implications and an addition to an enterprise-wide alignment (ERM). As a result, the exploration of alignment paradigm identified that an array of approaches (such as social, strategic, operational and cultural) are disparate or compound as an organisational baseline, for a relational mechanism. This is to ensure quality assurance, sustainability, and performance. Table 4-8 below provides a brief outline of frameworks identified.

Table 4-8 Alignment neutral frameworks

Author/s/year	Framework	Domain/s	Key function
Baets (1992,1996)	Information System Strategic Alignment Model	IT: business	Q1
Henderson and Venkatraman (1990,1993,1999)	Strategic Alignment Model (SAM)	IT: business	Q2
Luftman (2000)	Strategic Alignment Maturity Model (SAMM)	IT: business	Q3
Reich and Benbasat (2000)	Alignment between business and IT objectives research model	IT: business	Q2
Bergeron, Raymond and Rivard (2004)	Gestalt model of strategic model	IT: business	Q2
Preston and Karahanna (2009)	IS Strategic Alignment: a nomological network	IT: business	Q1
Charoensuk, Wongsurawat and Khang (2014)	Model of Business Information Technology Alignment	IT: business	Q3
Mekawy, AlSabbagh and Kowalsky (2014)	Business-IT Alignment (BITA)	IT: business	Q3
Reynolds and Yetton (2015)	Business and IT Strategy Alignment in MBOs	IT: business	Q3

Source: The Researcher

In particular, the analysis of alignment was problematic due to its roots in IT and business alignment. Although not possible to investigate the relationship of CsM and ERM alignment, an observation on these frameworks provided an insight into the complexity of alignment. The findings support the view that alignment has consistent roots in IT and is thus fragmented into adoption (Q1), implementation (Q2), and assessment (Q3) phases. Moreover, the exploration of alignment frameworks identified various dimensions: strategic, structural, and cross-domain; strategic and operational; and social-strategic dimension. For this reason, the following subsections are organised based on their alignment dimension types.

- **Dimension One: intellectual (strategic) dimension**

Luftman's Strategic Alignment Model

Luftman's model differentiation is that it proposes to construct the assessment and categorise five levels of maturity. The practical approach (in contrast with Henderson and Venkatraman 1993 framework) proposes to assess an organisation's existing state and establish further actions based on results. For instance, the lowest maturity is on an initial ad hoc level that represents inexistent alignment. In a second level, a commitment process is initiated, upgrading to established focused processes (level three), improved processes (level four), and lastly, the ideal state of optimised processes. All these levels represent the organisation's level of maturity based on the evaluation. To increase maturity, an organisation must improve communication, competence, governance, partnership, architecture, and skills maturity (Luftman, 2000). Although the *Strategic Alignment Model* involves a contributing outline of enablers and inhibitors in the alignment process, it remains a partial perspective with a focus on assessment (Q3). Moreover, the alignment neglects to consider the security aspects in the business context being more concerned with evaluation rather than adoption, implementation, or compliance.

- **Dimension Two: Structural dimension**

Business and IT Strategy Alignment in MBOs framework

To justify the adoption of alignment, Business *and IT Strategy Alignment in MBOs* framework outlines the advantages and disadvantages of alignment for a multi-business organisation. Reynolds and Yetton (2015) analysed the potential of business and IT strategy alignment within the business departments (structure) and corporate governance. The findings suggest that it triggers economic value and competitive advancement. This might be explained by the use of the theory of profit that conditions the process of financial gain.

While the financial gain is an important driver, there are many other indirect benefits disregarded by the framework (e.g. unified valuation, unified risk prioritisation, efficiency, response, reputation). It can thus be suggested that the framework of Reynolds and Yetton is limited to IT and business strategy alignment and value creation. The limited focus suggests that the framework could have been expanded by including the IT and organisational strategies in the context of security; ideally through the means of CsM and ERM in order to contribute to enterprise-wide security. Another possible improvement to the framework could have been the strategic approach rather than a functional, structural, or dynamic alignment. It focuses more on structural alignment of governance, resources, and capabilities but is nonetheless valuable. The approach outlined by the framework recommends a silo approach to IT and a partial focus of alignment assessment (Q3), dependent on strategy and infrastructure.

Gestalt Model of Strategic Alignment

Some models such as those presented by Bergeron, Raymond, and Rivard (2004) focus on developing the applicability of six patterns related to structure and strategy. The research model considers many variables to fit (Gestalt theory) as a whole that lead to proper alignment (Bergeron, Raymond, and Rivard (2004). The Gestalt model of strategic alignment is based on six aspects of alignment: moderation, mediation, matching, covariation, profile deviation, and gestalts. Alignment of strategy and structure is assumed to be the contributing factor to organisational performance. One of the flaws of this framework is that it is grounded on the initial phase of 'computerisation' development. Alignment is tackled as a solution for business sustainability and performance. It only addresses the descriptive value of alignment for utility purposes and outweighs security considerations. Understanding the complexity of strategy and structure alignment is one of the contributions made by *Gestalt Model of Strategic Alignment;* hence it provides useful guidance and confirming that IT and organisational strategies bring benefits. Despite its contribution, it omits to consider the external and internal variables, the current situation of an organisation, and how the alignment can be measured. Therefore, it partially addresses the alignment implementation (Q2), being descriptive.

- **Dimension Three: strategic and operational focus**

Information System Strategic Alignment Model

The model of Baets (1992, 1996) recognises the value of intellectual (strategic) and operational dimensions convergence that relies on strategy and infrastructure processes

alignment. The framework suggests that the attainment of alignment necessitates well-defined instructions to provide support in the form of a ‘map’. Inappropriately, this recommendation does not apply to the framework developed in 1996, which progressed to a strategic managerial mindset. While the framework (described as a *model*) shows valuable contribution towards the alignment adoption in the financial industry, the underlying flaw is that in the current context, it is mainly evocative and acts as a precursor of good practices, with limited applicability regarding the adoption phase (Q1). Embedded in the context of IT alignment with organisational strategy, the framework has tended to focus on infrastructure and processes, and less on strategic implication, asset valuation or effectiveness measurement. Due to this framework having initially been developed in 1992, it emphasises the traditional view of IT integration, where strategy, infrastructure and processes need to be integrated into business activities. Nevertheless, it fails to address the later consideration for security.

Strategic Alignment Model

The *Strategic Alignment Model* is constructed based on intellectual and operational alignment since it focuses on strategy and infrastructure (Henderson and Venkatraman, 1993). The theoretical baseline of this model relies on the initial MIT 90s project (Reynolds and Yetton, 2015) and is noticeably focused on internal and external fit. It consequently analyses the alignment of IT and business strategy, along with the infrastructure and processes involved in the process. In short, the early perspective of the authors examines the relationship between the executive collaboration and processes alignment across all organisational levels. Henderson and Venkatraman assess the feasibility of the intellectual and operational paradigm alignment. The relevance of the initial framework version (Henderson 1989) is supported by the subsequent 1993 framework version that appears to be the most completed and most used. The improved version from 1993 (Henderson and Venkatraman) provided a deeper insight into the four perspectives of alignment: execution, transformation, exploitation, and focus. The additional version sheds additional light on the contentious aspects of strategy, infrastructure, and processes alignment. Although conceptual, the *Strategic Alignment Model* has served as a base for further research and supported the practicability of alignment indirectly. A limitation of using this framework is that all four types of alignment are descriptively discussed and disorganised regarding execution. Thus, organisations are advised to select one type from each of the four available

options. Moreover, the scope of the framework is limited to IT and business alignment and thus omits to integrate security aspects.

Business-IT Alignment Model

Mekawy, AlSabbagh, and Kowalski (2014) constructed *Business-IT Alignment Model* conceptual model that intended to validate SAM (Henderson and Venkatram's model) through the investigation of another perspective that combined the classic approach with Security Values Chain Model (SVCM). The additional integration of SVCM transformed the approach from intellectual to intellectual-operational alignment. The model provides insights into whether the role of organisational objectives, communication, competence, governance, partnership, architecture, skills, or shared vision are effective. Although beneficial, all components are underpinned through an intellectual-operational paradigm while also incorporating aspects of cultural and social paradigms. Despite the fact the *Business-IT alignment model* focuses on the alignment of IT with organisational objectives, the model intends to recommend a bottom-up rather than top-to-bottom (strategic) approach. Such an approach is based more on setting the directions based on maturity evaluations; even though a strategic approach first sets its target (directions) and then implements it, optimising and measuring its achievement in accordance with the initial target. Accordingly, a post-implementation assessment can be done. The recommended approach is the opposite, a fact that may lead to unclear objectives and strategies. Being more a prescriptive framework, it focuses mainly on benefits rather than how the communication, competence, governance, partnership, architecture, skills, and shared vision maturity contribute to a common control function (resiliency). The framework suggests a silo approach of IT with deficient consideration for an enterprise-wide security (e.g. RM, ERM, CsM). This leads to the conclusion that the framework of Mekawy, AlSabbagh, and Kowalski is valuable regarding the interconnection of components but incomplete regarding focus.

Model of Business Information Technology Alignment (BIA)

The *Model of Business Information Technology Alignment,* developed by Charoensuk, Wongsurawat and Khang (2014), reconfirms the long-term effects and benefits of alignment. The model sustains an interconnectivity between theory and execution, and argues that strategic and operational alignment are both equally imperative for the achievement of organisational performance (Wongsurawat and Khang (2014). In undertaking the construction of the model, the authors considered the model by Henderson and Venkatraman (1993) and Chan as well as that by Sabherwal and Thatcher (2006). Grounded on prior

models it incorporates shared domain knowledge, IT success, organisation size considerations, IT sophistication, and communication planning such as inhibitors and enhancers of performance. Charoensuk, Wongsurawat and Khang present a contemporary analysis of IT business alignment through various components, but as do many other frameworks, it omits to consider the wider effects of internal and external factors, assets valuation, compliance, strategy, infrastructure unification, and even risk factors (security).

- **Dimension Four: social and strategic (intellectual) dimension**

Alignment Between Business and IT Objectives Research Model

The social dimension paradigm is considered by Reich and Benbasat (2000) in the context of evaluating the perception and capability of executives' understanding and commitment to support the alignment. Within this dimension of alignment, the model focuses on communication, shared domain knowledge (social), implementation (operational), and planning (intellectual). Although the model estimated that social dimension has an impact, it is unclear to what extent the informal factors influence the organisation's objectives. There remains a paucity of how the social dimension impacts the strategic dimension, and more importantly how it will be assessed. Being more focused on sustainability through understanding and communication, the framework is limited to an IT business alignment and implementation (Q2) but with inexistent consideration for security.

IS Strategic Alignment: a Nomological Network Model

Preston's and Karahanna's model (2009) is based on the nomological action of language, knowledge, understanding, executives' involvement and effects, as well as possible inhibitors and enablers of alignment. The *IS Strategic Alignment: a Nomological Network Model* involves understanding the benefits of the social dimension of alignment on strategic alignment. The mixing of social dimension with a strategic dimension of alignment has mainly focused on executives' expectations, executives' interactions, and structural effects in the healthcare industry. Even though this is a way to portray the alignment factors (partial, Q1), there is no evidence of how the alignment is attributed to organisational objectives, strategies, policies, or procedures within the financial industry. Furthermore, this remains a silo approach to business IT alignment, and thus enterprise risks and cybersecurity needs to be updated/incorporated.

4.3.3.1 Main contributors of alignment

From the analysis of alignment literature, it has been identified that researchers very often follow two main models. The first approach is the conceptual SAM, which emphasises a perspective based on the alignment of an external and internal domain of business and IT. The second approach is SAMM of Luftman, an extended version of SAM.

Table 4-9 provides an overview of some authors that grounded their research on the initial two alignment models.

Table 4-9 Key models of alignment and followers

Literature stage	Key contributor/s	Model developed	Concept followers	Framework Quadrant
initiator	Henderson and Venkatraman (1989, 1990, 1993)	SAM (strategic alignment model)	Papp (1999); Luftman, Papp and Brier (1999); Burn and Szeto (2000); Smaczny (2001); Avison *et al*. (2004); DeHaes and Van Grembergen (2009); Gutierrez, Orozco and Serrano (2009); Charoensuk, Wongsurawat and Khang (2014); Gerow, Thatcher and Grover (2015); Coltman *et al*. (2015); Salaheddine and Ilias (2017).	Q2
contributor	Luftman (2000)	SAMM (strategic alignment maturity model)	Sledgianovsky and Luftman (2005); Sledgianovski *et al.* (2006); Luftman and Kempaiah (2007); Gutierrez, Orozco and Serrano (2009); Cheng (2010); Mekawy, AlSabbagh, and Kowalsky (2014); Luftman, Lyytinen and ben Zvi (2015).	Q3

Source: The Researcher

As shown in Table 4-9, the followers of the models reported significant consideration of two paths: implementation (Q2) and maturity assessment (3). A possible explanation is that the second model of Luftman builds its structure on the initial strategic model of implementation and extends it further with maturity assessment considerations, respectively Strategic Alignment Maturity Model (SAMM). Additionally, the table illustrates that significant consideration for the alignment paradigm exists; hence prominent literature following the initial paradigm of SAM (intellectual-operational). The basic premises of intellectual-operational paradigms are that they not only consider directions but also how those directions are implemented in business departments (addressing the theoretical and the applicability of them). Nevertheless, the initial two alignment models received various criticisms but remained main advocates of the alignment concept. Supporting this, many subsequent frameworks followed the theoretical concept of Henderson and Venkatraman (1993) and Luftman (2000) but adapted to become a different domain; for example, IS, CsM, RM or ERM. For instance, the extended model of Luftman's proposed to assess the alignment

maturity and explore inhibitors and enablers (Luftman, 2000). The merits of Luftman's model from 2000 is that it anticipates the alignment results and sustains an inclusive model of six components: communication, value, governance, partnership, scope and architecture, and skills. Many others have considered the model of Luftman's. For instance, the intellectual (strategic) dimension is evaluated and validated by Avison *et al.* (2004) since it proposes to test its applicability for financial services. Moreover, Luftman and Kempaiah (2007) updated and validated the original model through globally dispersed empirical research. Although the alignment had other research domains, the six domains are significantly considered in later frameworks.

In summary, it is evident that Henderson's and Venkatraman's model (SAM) represents the baseline for IT: Business alignment. Accordingly, this model is significantly enhanced by Luftman (2000) in his model SAMM. The later model, SAMM, combines empirical evidence and explores the practicability of assessment maturity implementation. Its structure represents an initial step for organisations by identifying the current state in regard to alignment and proposes the next move. Despite the initial limited focus of both models (SAM and SAMM), they remain valuable due to their orientation to strategic alignment even though subsequent research and frameworks have progressed from this initial focus.

4.3.4 Frameworks outline and gap identification

On the premises of previous findings of literature gap identification (Section 3.5, Chapter 3) this section addresses the issue of the knowledge gap by looking at available frameworks being driven by Objective 3 stated previously.

In cases of academics' frameworks, there seems to be a lack of supporting frameworks for CsM and ERM alignment. The available evidence consists of models or frameworks that consider the alignment through the perspective of IT alignment with business alignment. Indeed, it has considered the strategic aspects of it, but the domains are different from the purpose of this research. A similar approach is taken by a small number of models that analyse alignment from an operational perspective yet are still related to IT. Thus, to cover all aspects, the models were considered part and in isolation.

In cases of regulators, there is a lack of internal frameworks developed. However, it may be assumed that the regulators contribute directly through regulatory laws with expectations to apply already established frameworks rather than create their own. Evidence suggests the focus on the financial industry is scarcely considered by CsM and alignment and

predominated by ERM. It also shows that the domains are segregated in IT, IS, CsM, RM, and ERM. Moreover, the approach is fragmented on strategic, operational, and technical levels, a fact that illustrates a tendency to fluctuate. Although the strategic approach registers the most significant consideration, it is evident that all three domains failed to address the alignment of CsM and ERM holistically. From this it can be denoted that particular attention needs to be considered, hence the traditional view on IS still being unclarified. Moreover, the influence of industry and regulations and alignment to the main frameworks maintain a focus to RM as opposed to ERM (e.g. ISO 27k series, ISACA series, ISF standard).

Additionally, the scope of most frameworks is generic and does not address industry-specific needs. Apart from these various approaches, the drawback is that most academic frameworks are conceptual and have not been validated in practice. The academics' frameworks related to CsM are mainly conceptual in their focus and consider various factors such as environmental and organisational factors (Siponen and Willison, 2009). Consequently, their applicability appears to be under impracticable principles, and thus their applicability resides in theory.

Although there are many standards for CsM, standards such as The Open Group Architecture Framework (Togaf), Information Infrastructure Library (ITIL), or the Payment Card Industry Data Security Standards (PCI DSS) were intentionally omitted because their focus is specifically on technical aspects and not strictly regarding security attributes. They were, therefore, unsuitable to contribute towards the purpose of this research.

The case of alignment is particular and is mainly formed by academics' contributions to the field. The assessment of the literature on alignment shows that the main influential authors are Henderson and Venkatraman (1993) and Luftman (2000). Although the frameworks are conceptually constructed, they are validated by the studies and frameworks that have followed. In order to exemplify the frameworks approach, domains and categorisation, the following Table (Table 4-10) has been constructed by using a standardised form for evaluation (see Appendix E). The method was preferred to emphasise the research Framework derivations.

Table 4-10 Summary of research frameworks and derivations

Prior frameworks dimensions							
Strategic (S)			Operational (O)	Strategic-Operational (S-O)			
Domain	**Gap emphasis**	**Paradigms**	**Theoretical derivations**	**Author/s / Framework: year**	(S)	(O)	(S-O)
CsM	Strategy	IS: IT	Integrative risk governance Structural and operational alignment. Advocates optimised risk practices.	Posthumus and Von Solms (2004)	∨		
				Ma *et al*. (2009)		∨	
				IASME Standard (2013)		∨	
	Objectives	IT: RM	Justifies the holistic management of risks. Widens risk awareness.	COBIT 5 (2012)	∨		
				ISSA IT Security RM Framework (2004)	∨		
	Appetite	IS: RM	Situation awareness of risk profile. Focus on internal and external variables. Implementational guidance. Implementation directives. Baselines for implementation. Significance of structural alignment. Implementation performance evaluation. Reflections on risk resiliency practices. Transparency of control functions. Performing integrative functions. Strategic and operational alignment. Security integration within the strategy.	Web *et al. (*2014a)		∨	
				Saleh and Alfantookh (2011)		∨	
				BS ISO/IEC 27000:2016	∨		
	Leadership			BS ISO/IEC 27004:2009	∨		
				Octave Standard series (1999, 2003, 2007)		∨	
	Value			ICAS Information Security Standard (2012)		∨	
				BS ISO/IEC 27002:2013		∨	
	Performance			NIST SP800-39:2011		∨	
				ISF (2011)			∨
	Risk oversight			BS ISO/IEC 27001:2013			∨
				BS ISO/IEC 27015: 2012			∨
	Implementation			EY's Cyber Program Management framework (2014)	∨		
				CESG Cyber Security Model (2015)	∨		
	Benefits			HMG Security Policy Framework (2014)	∨		
	Risks culture	IS: ERM	Consolidates implementation guidance. Implementation coordination.	BS ISO/IEC 27003: 2010	∨		
				BS ISO/IEC 27005:2011	∨		
	Structure/architecture	CsM: RM	Internal and external risk resiliency Maturity assessment of implementation. Significance of performance attainment. Implementation through leadership.	Atoom, Otoom and Abu Ali (2014)	∨		
				BS ISO/IEC 27032:2012		∨	
	Challenges			NIST RMF 800-53 (2013)			∨
				PAS 555 (2013)	∨		
				Global Cyber Maturity framework (KPMG, 2015, 2016)	∨		
				Deloitte's Cyber Risk Management framework	∨		
				Grant Thornton's Cyber Risk Management Program	∨		∨
		CsM: ERM	Cybersecurity strategy aligned with organisation strategy. Integration of RM functions across the whole organisation.	PwC's Cyber Risk Management framework (2014)	∨		
ERM	Strategy	RM neutral	Uncertainty acknowledgement. Effective organisational governance. Internal and external factors variables. Implementation governance. Integrated processes and strategies.	Miller (1992)	∨		
				Ward (2003)	∨		
	Risk appetite			Ching and Colombo (2014)	∨		
				BS ISO 31000	∨		
	Risk oversight			BS ISO 31100	∨		
				FERMA standard (2003)	∨		
	Risk profile						
	ERM maturity	ERM neutral	Risk oversight and business strategy. Top-down versus bottom-up approach. Optimising risk oversight Optimising governance. Return on investment. Embedded RM practices.	Drew and Kendrick (2005)	∨		
				Shad and Woon (2015)	∨		
	Risk culture			COSO (2004, 2013, 2016)	∨		
				RIMS (2011)			∨
	Structural alignment			Casualty Actuarial Society (2003)			∨
				KPMG's ERM framework (2009)	∨		
	Compliance			Grant Thornton's Holistic Enterprise Risk Management (2013)	∨		
				EY's ERM framework (2015)	∨		
	Benefits			PwC's Comprehensive framework for assessing ERM (2015)	∨		

			Performance risk elements. Implementation maturity.	McKinsey's Enterprise-risk-management framework (2013a, 2013b, 2016)	∨	
Alignment	Strategic governance Culturally driven Continuity Integration Collaboration Challenges Performance Maturity assessment	IT: business	Strategy and infrastructure processes. Embedded across business departments. Ongoing alignment. Strategic and operational alignment. Performance assessment. Enablers and inhibitors. Enterprise-wide communication Unified strategies Shared understanding-unified strategy. Enterprise-wide risk culture.	Baets (1992,1996) Henderson and Venkatraman (1993) Luftman (2000) Reich and Benbasat (2000) Bergeron, Raymond and Rivard (2004) Preston and Karahanna (2009) Charoensuk, Wongsurawat and Khang (2014) Mekawy, AlSabbagh and Kowalsky (2014) Reynolds and Yetton (2015)	∨ ∨ ∨ ∨ ∨ ∨ ∨	∨ ∨ ∨

Source: The Researcher

In summary, this review of prior Frameworks (Table 4-10 above) shows that undertaking an additional literature evaluation establishes a complimentary derivate to support the Framework of this research. This review demonstrates the following literature shortcomings and gaps in the existing research:

(1) Granular approach towards CsM

Researchers tend to adopt a disjointed approach to CsM and in turn it addresses the research problem in isolation. As can be seen in Table 4-5 above, despite the fact that the strategic approach is the most prominent one, it has focused on other subdivisions. Whether rooted in cyber-related security development phases (computerisation-informatisation-cyberisation) or not, the cybersecurity discipline shows a fragmented legacy in terms of definitions and meanings. Accordingly, the prior legacy of the CsM frameworks are grounded on three granular types: IT, IS, IA, with a later influence of RM. Typically, these types of studies admit that information security evolves in a wider paradigm yet remain traditionally embedded. Opponents of cyber-related terminology reject the reformation in a new terminology but use the principles of it. For instance, in the case of academics' framework, the 2014 Holistic Cyber Security Implementation Framework (HCS-IF) of Atoom, Otoom and Abu Ali is the only framework employing cybersecurity terminology. The remaining frameworks are rooted in the traditional terminology of IS (with regards both terminology and meanings), yet both approaches fail to align their focus and consequently recognise who is responsible for security. This is partially addressed because the first approach remains traditionally focused while the second approach uses the old terminology but applies modern concepts of cybersecurity. The evidence found in frameworks related to CsM illustrates that

only the vendor-specific frameworks show a positive trend towards ‘cyber’ terminology adoption but still fail to adopt the full terminology, which is used only partially (e.g. Cyber Program, Cyber Risk Management framework) except in the case of Deloitte’s and KPMG’s frameworks. Interestingly another indirect determinant is the variety of information protection acts (e.g. European Data Protection Act and General Data Protection Regulation).

This category registers a variety of approaches and, surprisingly, only two of the academics’ frameworks are strategically developed, as opposed to the abundance of academics’ literature regarding cybersecurity. PwC’s framework is the only framework that considers both domains. The drawback of this framework is that it omits to explain, define and support the implication of alignment, and consider the alignment of ERM to business, in turn not undertaking a holistic alignment of CsM with ERM.

Mandatory specific, practitioner’s frameworks produced by industry associations have often been indirectly supported by regulatory legislation, which endorses due diligence practices, although without particular recommendation to a specific one. Previous CsM frameworks have incorporated different sub-domains of CsM and have shown the variations across academic, industry, and regulators. Apart from the Holistic Cyber Security Implementation Framework developed by Atoom, Otoom and Abu Ali (2014), all frameworks have partially considered security as they referred to IS aspects and had omitted the holistic CsM aspects. Even if the frameworks use a partial perspective, the core principles of security represent a partial solution and static baseline for good practices.

(2) Mirroring past approaches of CsM and ERM

Virtually, all CsM frameworks of practitioners have followed a similar pattern to ERM, and thus two identical types of practitioners: vendor advisory-specific frameworks and industry expert associations that in turn have produced two kinds of directions, standards, and frameworks. Regrettably, the standards of industry are mainly focusing on IS management, as do academic frameworks. Most often there is also a mirroring regarding framework stages and approaches (Hopkin, 2014). For instance, there is considerable similarity regarding the number (usually five) and order of phases (e.g. Ma *et al*., 2009; Saleh and Alfantook, 2011; EY, 2014; PwC, 2015).

On the other hand, vendors’ advisory organisations have shown thoughtful consideration towards cybersecurity, albeit considered from an RM perspective. This makes this statement excluding PwC’s Cyber Risk Management framework, which has reviewed both aspects

(ERM and CsM) yet remains without specific regards to alignment. Thus, such frameworks fail to state their integration directly. Since this research has explored alignment through an array of approaches, it has been concluded that literature addresses alignment from social, strategic, operational, cultural, social, and intellectual dimensions, and it uses these approaches as a baseline and as a relational mechanism.

(3) There is limited consideration of CsM for financial industry-specific frameworks

An indication that the financial industry has barely considered CsM and ERM alignment is only contrasted by ERM, which has received more attention over recent years. It has been identified that the domains are segregated in IT, IS, CsM, RM and ERM. Furthermore, the scope of most frameworks has been generic and has not addressed industry-specific requisites. Apart from these various approaches, the drawback is that most academic frameworks have been acknowledged as conceptual and thus not validated in practice. Academics' frameworks related to CsM are mainly conceptual in their focus and considering their applicability appear to be impracticable, hence their applicability resides in theory.

(4) Scarce consideration in studying the relationship between strategic, operational, cultural and social functions to manage the unpredictable.

Granting the strategic approach to be the most significant consideration, it has shown that all three domains failed to address the alignment of CsM and ERM holistically. From this, it has been denoted that particular responsiveness must be reflected, henceforth the traditional view on IS security is still unclear. Additionally, the influence of industry regulations and alignment to the main frameworks have maintained a focus to RM as opposed to ERM.

(5) Scarce consideration for alignment in practice

The identified evidence supports the key argument that alignment is developed mainly by academics' contribution to the field. The assessment of the literature on alignment shows that the main influencers are Henderson and Venkatraman (1993) and Luftman (2000). With reference to academic's contribution, regrettably, none of these frameworks demonstrate a complete approach. Some have partially addressed the problem, but others have lacked efficient applicability and in turn have focused more on documentation aspects rather than a way to act strategically in order to nurture a real strategic approach at an enterprise-wide level.

An adequate alignment requires an interrelated alignment of CsM and ERM management, strategies, planning, structure, processes, skills, competencies, and culture. Additionally, a unified risk oversight should be acknowledged at all levels, in order to instil communication and mitigation on a common ground throughout community involvement and social engagement within an organisation. Therefore, successful implementation of the Framework can reduce over-investment, effort, and overlap, as well as develop organisational awareness. As a result, in-house risk procedures could be formulated and sustained through a strategy based on enterprise-wide effectiveness.

The analysis of frameworks demonstrates that more aspects need to be articulated for a complete approach. Some partially address the proposed framework approach, whereas some apply them strictly as a documentation for compliance (fulfil obligation) rather than a way to act strategically so as to nurture a real strategic approach at an enterprise-wide level. It also suggests that security involves various layers and yet still focuses on information systems or computer security (IT-centric), where security incorporates a more complex array of components. Moreover, it demonstrates that priority of security decision is still seen from a silo perspective, resulting in a mismanagement of risks (unaligned). In contrast, a common governance infrastructure will create a 'common mechanism' that would prioritise it as a security enabler, support initiatives, unify planning, and prioritise investments based on current organisational needs (i.e. not on subjective departmental needs - IT department might have different investment security priorities than organisation security); thus alignment shall support identification of overall necessity on a multi-layered security basis. Moreover, the alignment shall improve the discipline and transparency of risk oversight across the whole organisation.

(6) Incomplete stages of frameworks

Another shortcoming of the frameworks examined is that they fluctuate in terms of completeness. Some focus on adoption and implementation whereas a significant number of frameworks analysed concentrate mainly on assessment. On the other hand, Quadrant four (Q4) registers insignificant considerations.

While Section 4.3 and its subsections discuss framework derivations (frameworks' contribution), Table 4-11 demonstrates the drawbacks of previous frameworks in order to emphasise what has been omitted and why the *CsM - ERM Strategic Alignment Framework* is relevant in today's financial industry context.

Table 4-11 Drawback of previous frameworks

Domain	Frameworks Author/s and publication year/s	Drawbacks identified
ERM	Miller (1992)	Mainly focused on pre-implementation aspects of RM.
	Ward (2003)	It mainly addresses the RM component implementation.
	Drew and Kendrick (2005)	Lacks clarity regarding on how the alignment of ERM with organisation objectives should be achieved. It mainly addresses the ERM component adaption.
	Ching and Colombo (2014)	Descriptive in its nature, limited to implementation aspects of RM.
	Shad and Woon (2015)	Focused mainly on ERM maturity (strategic and operational).
	FERMA (2003)	Incomplete due to its dependency on ISO Guide 73, partial focus (Q2) and silo practices of RM.
	Casualty Actuarial Society (2003)	Addresses only to the implementation of RM alignment with organisational strategy.
	BSI (2009a)	Limited to traditional RM implementation, neglect to consider the integration of cybersecurity.
	COSO (1992, 2004, 2013, 2016)	While it considers technology for administrative purposes, it broadly omits to aggregate; ERM limited.
	RIMS (2006, 2015)	Focused mainly on ERM maturity.
	KPMG (2009, 2017a)	Only focused on performance enhancement variable; addresses risk partially through the view of ERM.
	Grant Thornton (2013, 2016)	Mainly focused on risk cultural basis awareness; addresses risk partially through the view of ERM implementation.
	EY (2015, 2016)	It tackles a partial perspective of ERM implementation and omits the cybersecurity aspects.
	PwC (2009, 2015)	Limited to ERM neutral, neglects to consider the integration of cybersecurity. It omits the compliance aspects.
	McKinsey (2013a, 2013b, 2016)	It addresses a limited perspective of ERM adoption and implementation.
	HM Treasury (2009)	Generic framework recommended as an assessment tool to measure RM.
	HM Treasury (2004)	A guidance of internal control compliance which neglects to consider the enterprise-wide and cybersecurity aspects; IA and RM limited.
	Posthumus and Von Solms (2004)	Anchored in IS/IT implementation practices with RM.
	Da Veiga and Eloff (2007, 2010)	Implementation siloed perspective of IT and IS alignment to business objectives. Over-confidence in cultural impact.
	Ma *et al*. (2009)	IT/IS adoption and implementation anchored; no evaluation beforehand implementation.
	Saleh and Alfantookh (2011)	A structural and procedural focus which omits the strategic implications of IS and RM.
CsM	Atoom, Otoom and Abu Ali (2014, 2017)	Operational and technical focus of CsM. It fails to consider the ERM and its alignment and with organisational goals.
	Web *et al*. (2014)	It focuses on a siloed perspective of IS and RM adoption.
	BSI (2011a, 2013b)	Embedded in the traditional approach of information and information systems protection through RM.
	NIST (2013, 2014)	Applies the practices of RM and omits to consider the alignment of CsM, ERM widely.
	OCTAVE (1999, 2003, 2007)	Omits the holistic view of CsM approach by primarily considering the information assets protection through RM.
	ICAS (2011)	Operational focus of IS and RM maturity.
	PAS 555 (2013)	Includes operational and technical aspects CsM and RM. Maturity.
	IASME Standard (2013)	A generic framework that focuses on IS and IT implementation.
	ISF (2011)	Focus on compliance of IS and RM.
	Ernst and Young (2014b)	A silo framework that considers IS, RM and their alignments in the context of business objectives. It omits to address an integrated approach.
	KPMG (2015, 2016)	Attentive on maturity assessment and it shows a siloed perspective on information protection in the context of RM; neglects CsM and ERM.
	PwC (2014)	The security is rooted in the traditional IS and ERM implementation, thus impartial.
	Deloitte (2015e)	Mainly descriptive, IT and RM driven (pattern-based decisions) despite misusing cybersecurity terminology.
	Grant Thornton (2016)	Does not provide ample support for the assertion of cyber risks alignment to ERM, therefore represents a partial approach to IT and ERM alignment.
Alignment	Baets (1992,1996)	A traditional strategic perspective of IT alignment to business strategy adoption that omits to consider security.
	Henderson and Venkatraman (1990,1993,1999)	Limited to IT and business alignment unable to integrate security characteristics.
	Luftman (2000)	IT and business alignment maturity, thus unable to integrate security characteristics.
	Reich and Benbasat (2000)	Limited to IT and business alignment.
	Bergeron, Raymond and Rivard (2004)	Limited to the alignment of IT with the business strategy and structure for performance purposes.
	Preston and Karahanna (2009)	Restrained on IT and business alignment; a social and structural alignment which omits the security aspects.

Charoensuk, Wongsurawat and Khang (2014)	Mainly focused on IT and business alignment omitting the security aspects.
Mekawy, AlSabbagh and Kowalsky (2014)	A silo approach to IT business maturity alignment that omits to consider the strategic security posture.
Reynolds and Yetton (2015)	It considers a structural alignment of IT strategy and organisation strategy with no consideration for security.
44 Frameworks	

Source: The Researcher

On basis of the above (illustrated in Table 4-11), the research framework justifies its value and delimitations.

4.4 Conceptual framework

A conceptual research framework represents a construct that compounds various concepts (Maxwell, 2012), to support resolution of the research problem (Imenda, 2014). Moreover, it represents the paradigm shift perspective through which the researcher approaches the problem. Usually, the framework is defined as a 'model' compounded from *pieces* (Maxwell, 2012). Accordingly, the conceptual framework of this research is built upon five derivates (constructs): literature review (first derivate), systematic literature evaluation extracted from Chapter Three (second derivate), the research gap (third derivate), supporting theories (fourth derivate), and supporting frameworks knowledge gaps (fifth derivate).

Given the fact that the purpose, derivations, stance, and limitations of the proposed Framework have been previously discussed, the following first section provides only a brief reiteration in order to set the context. The second part presents the outcome of aforementioned derivates (literature review contribution, systematic literature review contribution, literature research gap, supporting theories, and frameworks gap) which synopsise the development motivation and relevance of the CsM - ERM Strategic Alignment Framework.

4.4.1 Synthesis of Framework derivations

With reference to the above-mentioned derivations and adopted approach, the framework represents a 'structure', 'system', or 'plan' that incorporates concepts, variables, interdependencies and interrelation of a phenomenon (Nilsen, 2015) that has as a purpose to argument the value of researching the issue, determination and proposed solution for the research problem (Maxwell, 2012). Thus, the framework for CsM alignment with ERM provides strategic means for the alignment of risk governance, strategies, objectives, appetite, planning, structure, processes, capabilities, competencies, and risk culture for the purpose of serving organisational mission and vision in a unified manner; along with the

preservation of resiliency that advocate the idea of rejecting the ‘organisational dissociation’. In other words, it embodies a representation of how strategic organisational statement (strategy) is to achieve its main mission.

In view of this, the strategy can be illustrated in the policy as a managerial mechanism (Miles *et al*., 1978). Consequently, its application is based on baseline expectations, managerial directions, and the establishment of strategic directions. Such an approach hones a unified management that endorses risk safeguards and that acknowledge identification, communication and mitigation on a common ground (e.g. ICT-related risks and enterprise risks must be recognised at an enterprise-wide level) for decisions and behaviours (Miles *et al.*, 1978). Therefore, through the implementation of the Framework, an organisation can lessen over-investment and efforts to adapt to internal and external changes (Miles *et al*., 1978), overlaps of functions, and much more. Furthermore, in-house risk procedures shall be formulated and sustained through a common strategy centered on the significance of enterprise-wide effectiveness.

The Framework proposes to support organisations’ risk governance procedures by emphasising strategic responsibility and leadership with the intention to seize opportunities, make risk-informed decisions, and contribute to the achievement of the resilience against enterprise risks and cyber risks.

The underlying development motivation of this Framework is grounded in the arguments of the aims of this research, namely:

1) To investigate the alignment of CsM with ERM within the financial industry.
2) To develop a framework that assists CsM with ERM alignment within the financial industry, supported by practical guidance for the implementation of the proposed framework.

On the basis of research aims, Table 4-12 below synthesise confirmatory evidence for the research problem.

Table 4-12 Research gap derivations

	Identified literature gaps
Literature Review	(1) Scarce strategic alignment literature that focuses on CsM and ERM alignment, (2) low level of maturity in the implementation of the alignment, (3) lack of bottom-up consideration of the concept,(4) lack of common terminology, (5) lack of common guidance for implementation and (6) low level of cyber risk awareness inside organisations, (7) lack of coherent theory.
Systematic Literature Evaluation	(1) A lack of clear terminology and definitions in all three domains, (2) a lack of practical alignment literature guidance (academics, practitioners and regulators), (3) a lack of common governance practices across all three domains, (4) scarce alignment literature that considers integration of CsM, (5) scarce financial industry-specific focus, (6) scarce consideration of regulatory bodies regarding the alignment processes, (7) a lack of clear practices towards ERM, CsM and alignment implementation, (8) the literature of CsM is fragmented among different domains, (9) granularity of CsM terminology encouraged various professional accreditation, (10) geographical dispersion of industry practices and procedure, (11) a discontinual temporal attention in research literature, (12) criteria considered by the literature of ERM varies between value, performance, appetite, culture, governance and each of them is addressed in isolation, (13) CsM still seen as an IT problem, problems treated in isolation, (14) ERM and CsM practices seen as minimum compliance (reactive measure rather than proactive controls).
Frameworks Evaluation	(1) Granular approach towards CsM, (2) Mirroring past approaches of CsM and ERM, (3) there is limited consideration of CsM for financial industry-specific frameworks, (4) scarce consideration in studying the relationship between strategic, operational, cultural and social functions to manage the unpredictable, (5) scarce consideration for alignment in practice.

Source: The Researcher

Within this context, Table 4-12 depicts the totality of gaps identified during the investigation of the research problem, a fact that validates the inconsistency and granularity of current theoretical and empirical research.

4.4.2 CsM - ERM Strategic Alignment Framework

The Framework derives from previous findings of the literature review (first derivate-contribution), systematic literature evaluation (second derivate), frameworks evaluation (third derivation), and research gap (fourth derivate). Based on these four derivations, the structure of the Framework is further compounded with another derivate, supporting theory (fifth derivate). The precursor to Framework implementation is understanding organisational goals, objectives, strategy, risk appetite, risk tolerance, acceptable residual risk, and alignment expectations. This is also the case for CsM and ERM. Consequently, a prior understanding can foster an effective alignment in accordance with organisation goals and objectives (Ezingeard, McFadzean and Birchall, 2007).

The *CsM - ERM Strategic Alignment Framework* constantly adapts to internal and external variables and its dependencies. As the Framework has at its roots five main functions (‘baseline expectations’, ‘managerial directions’, ‘established strategic directions’, ‘implemented managerial directions’ and ‘monitor and review’), to a large extent it advocates a sequential practice in context of requirement fulfilment, planning, control, and measurement as essential conditions.

To illustrate the above mentioned, Figure 4-13 below synthesises all five phases to outline their interconnectedness with CsM, ERM and alignment, and more specifically, their interdependence.

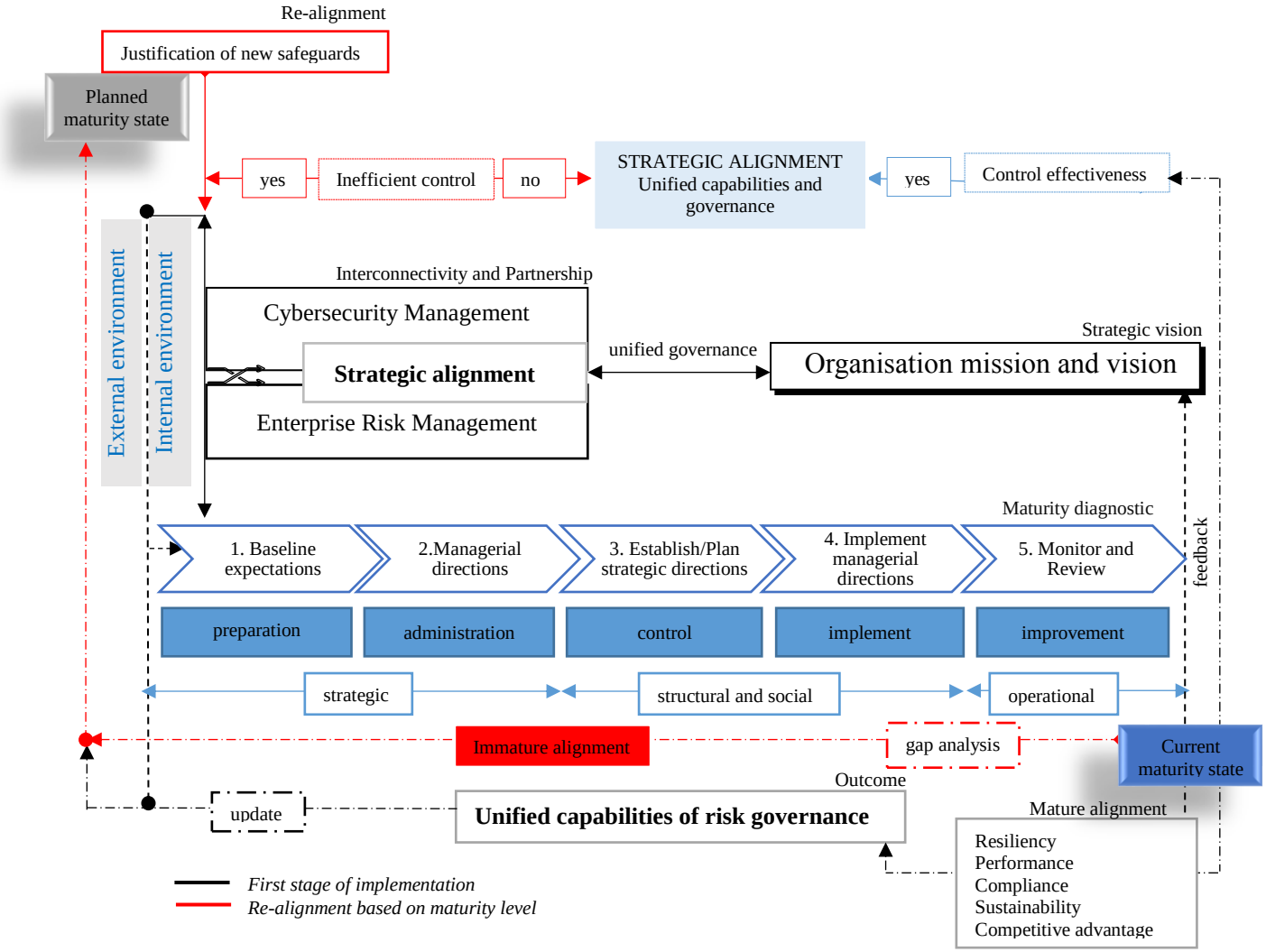


Figure 4-5 CsM – ERM Strategic alignmnet Framework

Source: The Researcher

As shown in Figure 4-13, the *CsM - ERM Strategic Alignment Framework* is grounded on the assumption of preparation based on demanded requirement, administration (diagnosis before implementation), control (change), implementation as a validation for proper directions and review (improve) phase ─ all in the form of cyclical phases. The implementation contains five different phases and is based on processes and an operation's adaptation to a common scope-achieved by the directions of strategic alignment). Although this 'preparation' phase is significantly discussed in academia, industry and regulation, the methodology needs a baseline of principles, context consideration (demographic and industry specification) along with an internal strategy to mandate implementation. If there are unclear statements and principles that define and mandate actions, the establishment of implementation is incomplete. Additionally, an unclear profile practice of an organisation is a drawback; the applicability starting point is thus unknown. An assessment that includes identification, analysis, evaluation, visualisation of what to protect, and designed value is the core step that guides the application of the Framework in an interrelated cyclical manner (Ching and Colombo, 2014).
The guidance how to use/operationalise the *CsM - ERM Strategic Alignment Framework* will be further discussed and presented in Chapter Seven, Section 7.4.

At its roots, the Framework compiles the coercive pressure of institutional norms along with variables and interdependencies of Contingency Theory. Such an approach aims to assure an organisation's review and optimises its practices in order to ensure appropriate strategic practices that warrant the fulfilment of organisational goals and mission. Therefore, the *CsM - ERM Strategic Alignment Framework* is driven by the paradigm of Contingency Theory and Institutional Theory by their commonality: alignment (Vorbeda *et al*., 2011). Although the contingency and institutional theories focus on different and partial aspects of alignment, the synergy of both strives to marry two facets of alignment as a whole (Greenwood, Hining and Wheten, 2014). By the complementarity and co-dependency of theories, the Framework compiles a double paradigm perspective of alignment to ensure that alignment is achieved by considering an internal fit towards an external fit (Contingency Theory), whereas Institutional Theory concentrates on achieving an external fit (e.g. recognition of conformity, external support) rooted on internal fit, which together can lead to a 'meta-fit' (Donaldson, 2008). More specifically, Institutional Theory defines the normative pressure on organisations to conform with a legitim 'pattern' of organisational behaviour (external expectations) and *homogeneity* of dependables on the basis of coercive pressure

(organisational values, normative rules, legitimacy, beliefs, principles, behaviour, ethics, and social systems). On the other hand, Contingency Theory refers to an internal alignment of culture, organisational design, processes, leadership, technology, size, and structural alignment to ensure organisational sustainability despite considering internal variations and aiming to adapt to external interdependencies.

4.4.3 Overview of framework functions

The sections that follow explain cyclically how the framework implications and propositions, help to understand specific characteristics that interrelate. Accordingly, these five phases are outlined below:

- Phase One: 'baseline expectations'
- Phase Two: 'mandate managerial directions'
- Phase Three: 'establishment of strategic directions'
- Phase Four: 'implement managerial directions'
- Phase Five 'monitoring and reviewing practices'

4.4.3.1 Phase One: 'baseline expectations'– the premise behind the first phase is that it represents the definition of strategic baseline expectations of an external environment from which principles and context derive with the determination to establish the drivers (purpose, limitation and constraints) and how alignment should be achieved. This first phase defines the 'purpose, outcome, and delimitations' of organisations within the context of theoretical legacy, regulatory prospects, or industry requirements (e.g. contractual, baseline), related to organisation, CsM and ERM.

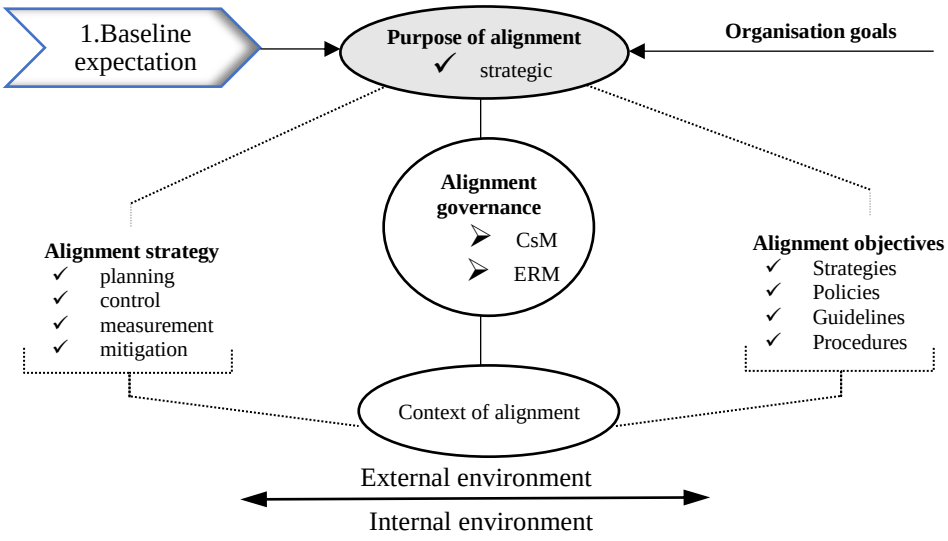


Figure 4-6 Phase One of the Framework: ‘baseline expectations’
Source: The Researcher

Anticipating the implications, Figure 4-6 displays the effects and interdependencies of an external environment within today’s business context. In supporting this view Casualty Actuarial Society (2003) and ISO 31000:2009 (BSI, 2009) recommend this initial step, recognising the utmost importance of this stage. By acknowledging external exposure and pressure, an organisation can advantageously adapt; a fact that facilitates an advanced preparation and understanding of industry and business settings, clarifies expectations, defines internal requirements, enables accountability, assures transparency of decisions, and determines justified strategic decisions (informed). Such acknowledgements help to improve/adapt/prepare in advance for constraints, interdependencies, or variations (Nair *et al*., 2014). Defined most often as *situational awareness* (Web *et al.*, 2014a), this approach facilitates clarification of expectation, requirement (accountability and transparency), constraints, and limitations through a macroeconomic view. The external context refers to the identification, analysis, and evaluation of different types of uncertainties from political, economic, social, technological, environmental, legal (PESTLE), cultural, regulatory, financial, or demographical. It is often considered as a classification system that enables a better understanding of whether the organisation’s approach, resources and resilience are sufficient (Hopkin, 2017). In short, deploying this phase facilitates prudent practice in understanding an external environment’s potential impact on internal organisational factors and lastly on the appropriate development of control function (Ma *et al*., 2009). It ensures a baseline in mandating, establishing, and measuring the Framework and helps a continuous adjustment in alignment with requirements and organisational goals.

4.4.3.2. Phase Two: ‘mandate managerial directions’- moving further, the second phase advances a facet of strategic risk control; it changes its focus from macro (phase 1) to micro dimensions that emphasise the internal strategy in alignment with internal requirements.
The idea conveyed in this phase is that it contains settings of internal directions in balance with identified external directions, defining how the appetite, structure, processes, responsibilities, and work commitment in a unified manner. Typically, the recommended approach is based on the alignment of CsM and ERM objectives, strategies, policies, guidelines, procedures for transparency, and prioritisation in accordance with the organisation’s goals and objectives. Therefore, an organisation is more proficient to state its attitude to risk (i.e. in the form of a documented policy) in accordance with all implied, based

on a predefined direction (BSI, 2009). Being a stated strategy, it mandates increased expectations of capabilities for implementation (BSI, 2016).

In addition to the range of activities included in this phase, it employs the identification risk of owners, measurement (performance), improvement (development), transparency, and compliance. A similar approach towards understanding the significance of the internal environment is considered by FERMA (2003) and by BS ISO 31000 (BSI, 2009), a fact that sustains the validity of this phase within the Framework.

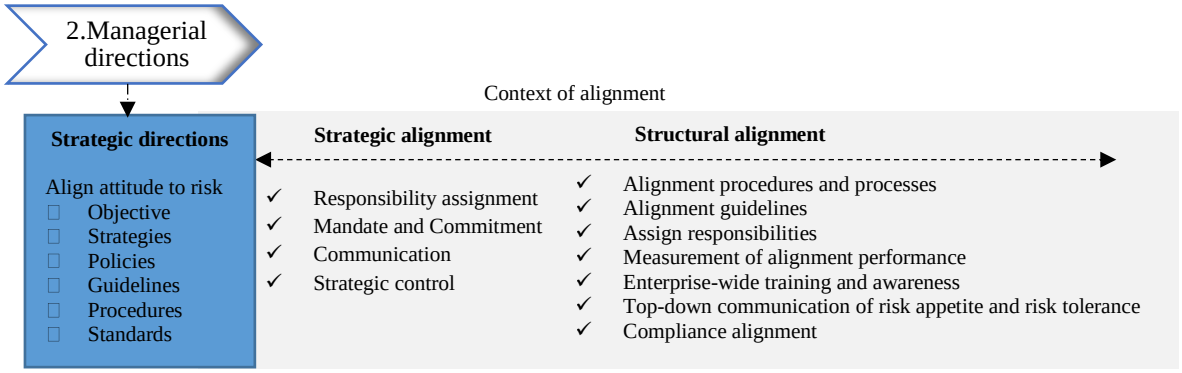


Figure 4-7 Phase Two of the Framework: ‘mandate managerial directions’

Source: The Researcher

For a visual representation, Figure 4-7 outlines a unified strategy that considers structural alignment based on strategic alignment and managerial directions. Moreover, it proposes a reflection on all components (purpose, objectives, appetite, processes, responsibilities, and expected performance in regard to risk) documented and stated in the policy. A policy illustrates a clear statement that clarifies responsibility and promulgates good practices (ISSA, 2004). Typically, its content comprises a description of an organisation’s attitude, directions, control mechanism, privileges and monitoring processes, all in accordance with objectives (CESG, 2012).

Even though the objectives set are seen by ISO 31000:2009 (BSI, 2009) as part of the ‘process-phase’, the Researcher considers that this phase is part of directions settings, thus acknowledgement of the philosophy, appetite and directions should be established in the mandate phase, so it can in turn trigger the design and deployment of actions beforehand. Likewise, Casualty Actuarial Society (2003) shows that ability to understand objectives and means of applying strategies lead to real vigilance and proper governance. Additionally, the inclusion of performance assessment, organisation risk culture, and communication of

alignment strategy can contribute to the establishment of a unified internal strategy of CsM and ERM.

Therefore, phase one and phase two only considered the driving principles that set directions before implementation and how strategic control prioritises goals (dependency, requirement) to foster efficiency and resiliency (Atoom, Otoom and Abu Ali, 2014).

4.4.3.3. Phase Three: 'establishment of strategic directions'- the third phase is a complex phase of the Framework hence it moves from examination and planning before implementation, towards the establishment of processes of strategic alignment implementation between CsM and ERM. As a starting point, internal contexts are considered and assessed which, according to ISO 31000:2009 (BSI, 2009), is a desirable approach that supports an understanding of organisational governance, structure, risk accountability, objectives, strategies, policies, capabilities, culture, methods, and/or tools used (standards, guidelines, models), and/or contractual and legal responsibility as proposed in ISO 31000:2009 (BSI, 2009). This approach appears to be the most commonly practised in academic and industry frameworks, despite some frameworks only containing this single phase (e.g. BS ISO 27005:2011; ISF Standard of Good Practices for Information Security 2011; IASME Standard for Information Assurance, 2013). Apart from internal context identification and risk examination, this category represents a cyclical deployment of processes in which strategic and structural alignment adjusts to ensure availability of resources and directions. The context refers to the assessment of internal and external uncertainties, interdependencies or variables that might affect organisational goals and mission. In correlation with the strategic alignment, the control function adjusts towards organisational objectives to ensure an enterprise-wide alignment. Figure 4-8 shows the correlation.

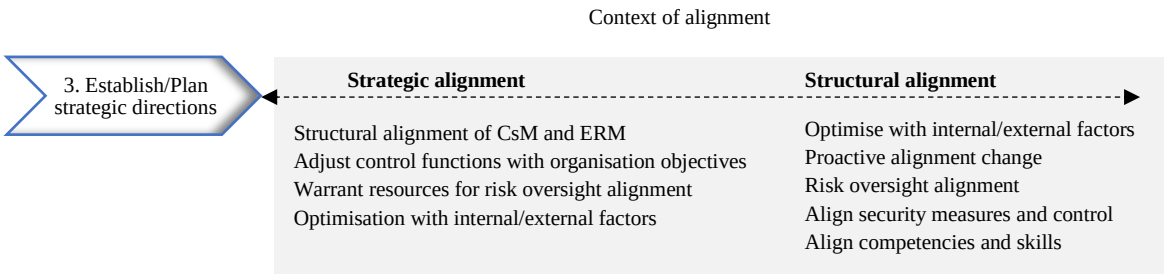


Figure 4-8 Phase Three of the Framework: 'establishment of strategic directions'

Source: The Researcher

As shown in Figure 4-8, Phase Three applies the directions of Phase One and Phase Two. In contrast to the first phase, which considered the macroeconomic aspects, Figure 4-8 highlights considerations for strategic and structural alignment enhanced with internal and external factors. Phase Three expresses the strategic directions as a plan for understanding that must be put into practice and which factors may enable or inhibit the alignment. Scrutinising critical business domains, assets, legal, regulatory, contractual requirements (e.g. third-party agreements, outsourced services), industry requirements, and expected protection and demanded protection from shareholders (i.e. BS ISO 27003:2010) (BSI, 2010) represents an acknowledgement and understanding of the Framework's capability within the context. Correspondingly, Saleh and Alfantookh (2011) specify that establishing the context, identifying current situations (assets, threats, vulnerabilities, and control), recognising the risk owners, location, or source of threats are all prerequisites in assuring flexibility of implementation. Miller (1992) recommends classification and categorisation of risks to understand the value and impact of a potential loss. Thus, confirming the context in the form of external and internal environment analysis can be done by using tools such as Strengths-Weaknesses-Opportunities-Threats (SWOT) to support the validity of an enterprise-wide profile (Casualty Actuarial Society, 2003).

While the main determination of the third phase is to establish how strategic directions are implemented, per total it is an optimisation of the context of alignment, of limitations, and of organisational capabilities. On this basis, the following phase moves beyond theoretical applicability, in the direction of an in-depth enterprise-wide implementation.

4.4.3.4. Phase Four: 'implement managerial directions' – overall this phase transfers the strategic guidance into an operational and social dimension that aligns with operations to deploy enterprise-wide alignment. It advances the mindset of different elements congruence (e.g. identification of organisational practice profile, assessment, alignment of processes, response, and communication) as determinants. Understanding how the strategic, structural, and social dimensions of alignment can enable or inhibit strategic enterprise-wide alignment is a precondition for achieving performance (Chan, 2002; Alecsić and Jelavić, 2017). To illustrate, Figure 4-9 below emphasises how the initial phases (Phase One, Phase Two, and Phase Three) migrate from the formulation of a strategy to achieve organisational objectives for the application of directions, respectively implementation.

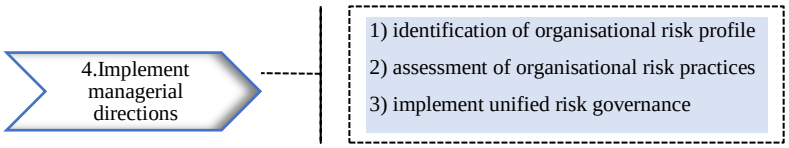


Figure 4-9 Phase Four of the Framework: ‘implement managerial directions’
Source: The Researcher

Figure 4-9 indicates that Phase Four relies on specific managerial directions balanced with the internal and external environment. More specifically, it emphasises the organisational adaptability to various variables mandatory to achieve alignment.

1) **Step One of Phase Four: Identification of organisational risk profile**

The first step, organisational profile, embodies identification of the practice profile that defines the status of an organisation, clarifies goals, and recommends advancement as well as determining an appropriate level of investments. The practice of *risk profile* is based on the initial Luftman (2000) strategic alignment maturity assessment model, which assessed the alignment maturity level based on five-phase models: (1) initial, (2) committed processes, (3) established processes, (4) improved/managed processes, and (5) optimised process. Apart from this, a similar model is RMM. It was developed by RIMS (2006) and has a similar format of five criteria: ad-hoc, initial, repeatable, managed, and leadership. Considering the above-discussed models, the current Framework adopts a simpler structure to evaluate organisational maturity on a scale of one to five and proposes the followings levels of categorisation:

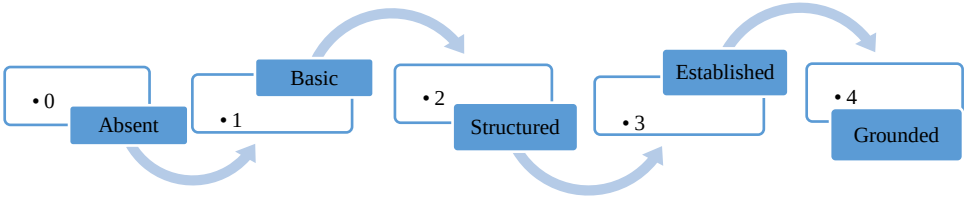


Figure 4-10 Maturity Diagnosis Model
Source: Adapted after Luftman (2000)

- Level zero – absent, there is a lack of strategic alignment implementation of CsM and ERM;
- Level one – basic, some kind of strategic alignment is planned, considered, or initiated;
- Level two – structured and implemented alignment, some form of risk approach is addressed through basic policies, processes, and procedures, but mainly on a silo basis;

- Level three – established complex policies, processes, and procedures developed. Past events used to learn, predict, adapt, and respond in a timely manner;
- Level four – grounded, integrated and aligned strategic policies, processes and procedures of CsM and ERM.

Based on the above criteria, the profile assessment supports the identification of an organisational profile (a), which determines the target profile (outcome) and further directions. Moreover, the difference between these two profiles reveals the organisational gap (NIST, 2014), which needs to be considered. A similar approach has been considered in other frameworks (e.g. Saleh and Alfantookh, 2011; Posthumus and Von Solms, 2004; NIST standard series).

2) **Step Two of Phase Four: Assessment of organisation risk practices**

After identification and categorisation of the organisation's practice profile, the second step is an assessment of the organisation's risk practices. The assessment is structured on a sequence of four steps: identify-analyse-evaluate and visualise (IAEV) key risks. Assessment determines further actions based on identification (risk, threat, and vulnerabilities), analysis and evaluation of facts (as seen in BS ISO/IEC 27005), assets and requirements (as seen in BS ISO/IEC 27003:2010) and their likely cause and consequences (as seen in BS ISO 31000:2009), controls, vulnerabilities, or likelihood of such, that underpin priority and actions.

The financial industry in particular is frequently being targeted and thus requires optimised strategies related specifically to industry risks, in parallel with an assessment of risks for tangible and intangible assets and assessment of digital and physical environment risks. Adopting an assessment based on four steps (IAEV) assures the avoidance of duplication of identification (I), analysis (A) and evaluation (E). There are standards (e.g. Casualty Actuarial Society, 2003) that repeat these phases (identification, analysis and evaluation) as they consider an additional phase of assessment and only a few incorporate all three phases (e.g. BS ISO 31000: 2009, BS ISO/IEC 27005:2011). However, IAE is all part of the assessment and such approach duplicates the steps. Apart from this clarification and systematisation of prior contributions, the Researcher contributes by providing an additional step: visualisation to expose the results of the assessment. Visualisation refers to the exposure of result, as a form of 'diagnosis' from where further decisions are taken in an informed manner.

The identify-analyse-evaluate-visualise (IAEV) assessment implies:

- *Identification* (I) refers to the capability to find, recognise, and outline risk exposure through the lenses of both CsM and ERM in accordance with the organisation. In a broader sense, risk identification aims to identify what can harm the organisation by focusing on potential loss and anticipating how, where, and why it can happen (as seen in BS ISO/IEC 27005:2011) (BSI, 2011).
- *Analysis* (A) process refers to a strategic mechanism of understanding the enterprise-wide risks and their level (BSI, 2011). For example, the ISO standard describes the analysis process based on criticality, vulnerability, and prior incidents encountered. The analysis can be undertaken through a qualitative method, a quantitative method, or mixed-method. The analysis is defined by Saleh and Alfantookh (2011) as a process of identifying the gap profile.
- *Evaluation* (E) compares the analysis results in order to identify the magnitude of risk (as seen in BS ISO/IEC 27005:2011) (BSI, 2011). To provide support, techniques such as Swot analysis, prospecting, PESTLE, or event tree analysis can be used (FERMA, 2003). Evaluation criteria: strategic value, criticality, legal, regulatory, and contractual requirement, as well as operational and business importance (BS ISO/IEC 27005) consider all these aspects by analysing the impact criteria (damage, disruption cost, value, operational, and regulatory effects).
- *Visualisation* (V) relies on identification, analysis and evaluation to visualise vectors, processes, assets, and actors, and to expose and communicate the value. This phase represents a process of asset value allocation that needs to be estimated through cost-effective analysis. Based on this evaluation, the investment cannot be higher than its value. The value needs to be estimated, classified, and visualised. As a result, based on the categorisation and classification pre-assigned security controls are applied in accordance with their value. This section must consider the potential loss, impact, reputation damages, and replacement cost. Visualisation aims to deploy decisions/respond based on the assessment. This step is based on the principles of assessment in order to determine the value of an organisation and elicit a means to protect it within the balance of security cost expenditure.

The concepts of risk in terms of value can be quantified through an assigned value of critical assets. Since the interest of a perpetrator is interlinked with the asset value, Fenz *et al*. (2014) suggest that a valuation of assets (inventory) provides a reliable estimate of which assets

might be targeted. This perspective underpins an effective allocation of resources, preparedness, avoidance of overconfidence, cost-effectiveness, and advice on safeguards. Generally, the valuation can be quantitative if it is based on cost (e.g. new acquisition/replacement cost, the cost of inoperability, opportunity cost, interruption, financial loss, and regulatory infringement) or qualitative (e.g. competitive advantage, reputation) as seen in BS ISO/IEC 27005:2011) (BSI, 2011). For instance, the valuation phase is considered by Saleh and Alfantookh (2011) to be a mechanism, thus representing an assessment of strategy, governance, controls, compliance, and organisational profile to help identify any gaps between the current profile and the anticipated target profile.

Additionally, FERMA (2003) standard suggests that the assessment phase should be documented and organised in a structured format with clear descriptions for further use. Therefore, the assessment of leadership and governance, training, education and awareness, and controls and compliance should be integrated (processes) and aligned (strategy) (CESG, 2015). Thus, the assessment can be in the form of qualitative, quantitative, or mixed analysis. Usually, assessment leads to prioritisation (Casualty Actuarial Society, 2003). For instance, Octave standard focuses on the assessment of information assets and develops a methodology to assess risk, organisation profile, and areas of concern, all based on analysis and followed by mitigation. Obviously, considering only the information assets represents an incomplete process. Thus, for a comprehensive assessment, asset management should be considered. This is a function that has the purpose of cataloguing and assigning a value to assets based on their sensitivity and criticality (ISSA, 2004).

Valuation compiling of physical and digital assets recommends inventory practices and ownership followed by asset classification based on type, sensitivity, value (criticality), and degree of assurance (BS ISO/IEC 27001:2013). In addition to this practice, organisations can develop a documentation regarding risk taxonomy (types of risks) in order to better make decisions (actions plan). In connection with the assigned value of assets and risk taxonomy, it can foster further necessary actions and informed decisions; a practice which ensures efficiency and transparency. Moreover, the acknowledgement of assets value, processes, infrastructures, information, or technology that might determine and facilitate a preparedness and anticipated view towards possible security incidents (negative) impact on an organisation’s daily activities (PwC, 2014).

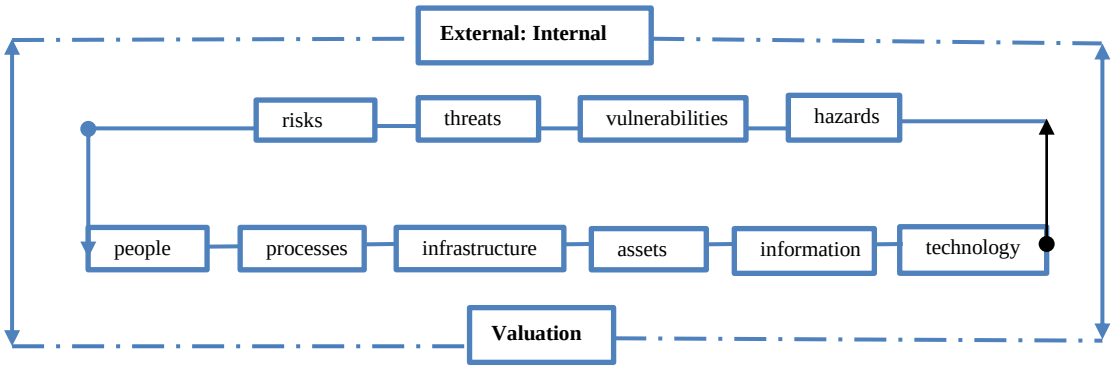


Figure 4-11 Valuation process (value identification of organisational assets)

Source: The Researcher

Regarding Figure 4-11 above, the process of valuation can be considered a diagnosis function that addresses valuation in order to prioritise and increase resiliency based on criticality.

3) **Step Three of Phase Four: implement unified risk governance**

Alignment process takes place in an established infrastructure. Thus, integration refers to different acts that together form the alignment. For instance, structural alignment relates to formal structures such as infrastructures/departments. Through these, an alignment can be deployed (Chan, 2002). Alignment of processes, decisions, reporting, employee's deployment, and prioritisation depend on strategic guidance. Thus, their common collaborative effect is significant (Chan, 2002). While this action is based on operational aspects, at its core lies the integration of CsM and ERM strategy to organisational strategy (contextualised in objectives, directions, appetite, and risk oversight in a centralised form). Additionally, a stimulation of aligned communication and acknowledgement concerning organisational strategy (vision, objective, and direction), implementation purpose, and results expected by each employee is believed to stand-in towards a successful result. Therefore, implementing a unified risk governance as a control function comprises of two steps (response and communication). These require a strategic alignment, structural alignment, and social alignment to address the risk governance enterprise wide. This phase is similar to the description of *risk treatment* mentioned in the Australian/New Zeeland Standard (2004), which defines the response step as a process of selection and implementation of measures to adjust risks. The Australian/New Zeeland Standard (2004) also clarifies that residual risk is the result of the intervention (response) and treatment phase (risk minus treatment). The main attributes of this step are based on knowledge and shared domain knowledge across the whole organisation (part of the frameworks). Obviously, this

implies communication which is another essential attribute that can foster performance in the alignment (Charoensuk, Wongsurawat and Khang, 2014). Interdepartmental communication (social alignment) and unified risk governance structure (structural alignment) ensure a continuous process of oversight and awareness across an organisation (cultural alignment). For example, Orange Book released by HM Government (2004) recommends risk identification to approximate likelihood and document activity accordingly. Risk treatment can use different strategies: avoid, accept, reduce/mitigate, and transfer (as seen in Casualty Actuarial Society, 2003; ISO 31000: 2009), and generally it selects and applies methods (ISO 31000:2009).

In cases where organisations may decide to transfer risk to insurance, this partially offers a solution because this option is only effective in part due to its limitations regarding financial coverage and because it does not have long-term implications for strategic organisational resilience. As a result, a false sense of security lulls organisations into believing they are taking adequate measures when adopting a policy without an organisational change (Websense Lab Security, 2015; Thakor, 2015).

'Respond' is a risk control function and refers to the amount of response that modifies a risk (BS ISO/IEC 27005:2011), respectively it is based on processes, policies, procedures, or guidelines to safeguard an organisation; for example, response capability can be sustained by increasing staff competencies, identification of necessary resources, culture, preparedness and a well-established strategy in regards to risks (as seen in BS ISO/IEC 27001:2013) (BSI, 2013). Additionally, the risk function 'response' can be complemented with an action plan (e.g. incident management or business continuity). Response through mitigation represents a treatment process with the purpose of changing risk (create resiliency) in close relationship to an organisation's policies, goals, and objectives, and stakeholders' expectations. Nonetheless, the fact that mitigation actions are taken brings a foreseeable remanence of risks. However, in such cases, post-mitigation, a risk remanence represents only residual risks. In other words, a risk that remains after measures have been taken (residual risk), one that should irrelevant, accepted or tolerable for an organisation (BSI, 2011). Nonetheless, this remains a phase that needs continuous monitoring and reviewing in order to assure that the mitigation measures ensure acceptable levels of predefined residual risks (Saleh and Alfantookh, 2011). Additionally, implementation of strategic controls ensures a risk governance quality as well as oversight and performance assurance (Chan, 2002; Atoom, Otoom, and Abu Ali, 2014).

4.4.3.5 Phase Five 'Monitoring and reviewing practices'

The fifth phase, '**monitoring**' refers to the process of continuous measurement of organisation risk approach, its strategies, applicability, and response. Based on this, further tasks are deployed, investment considered, and review tasks commenced. This phase includes documentation for further use of reviewing processes that depend on comparisons of practices with the predetermined baselines, past learned lessons, experiences, organisational cultural dimension, observations and research. Being a measurement category, it aims to assess and test how effective the implementation is (BS ISO/IEC 27004:2009) and to reinforce whether further improvements are needed. In short, measurement refers to the identification of a deviation between actual results in contrast to planned results (Aguilera, Judge, and Terjesen, 2018), and a means to improve risk control and practice. As an example, Figure 4-12 exemplifies the supportive role of monitor and reviews control function.

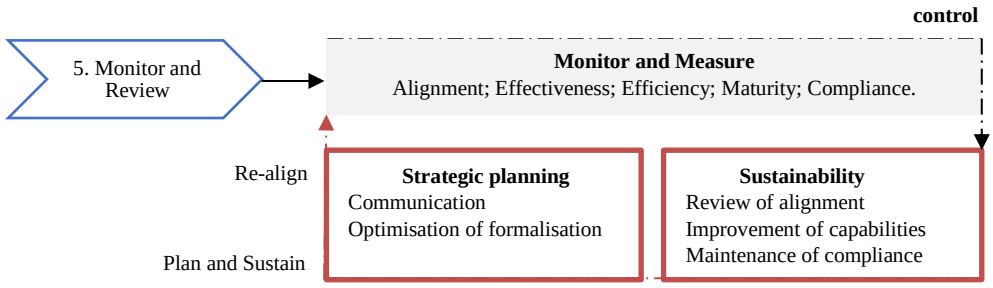


Figure 4-12 Phase Five of the Framework: 'Monitoring and reviewing practices'

Source: The Researcher

As can be seen in Table 4-12 above, the '**review**' phase embodies an "activity undertaken to determine suitability, adequacy, and effectiveness of the subject matter to establish objectives" (BSI, 2009, p. 7). Usually, the results from monitoring are compared against the recommended criteria from practitioners or regulators; for instance, ISO 31000:2009 (BSI, 2009) recognises the value of optimised, integrated, and, if necessary, modified control function. Henceforth, the monitoring and review processes are a way to validate whether organisational practice and performance is at the right maturity level. In some cases, organisations may choose to use tools to measure the results (e.g. Economic Value Added (EVA) and annual audits are used to reassess implementation.

Typically, a review phase relies on monitoring and continuing the process through two categories: 'plan' and 'sustain', which in turn comprise of another step to undertake the activity. Based on the results of monitoring, the review phase takes place, and plans are made

to optimise the identified weaknesses (e.g. communication, appetite, infrastructure, governance, policies, and procedures). In this manner, an organisation prepares to upgrade to a superior profile being influenced by plans and directions that have roots in an informed risk approach (Saleh and Alfantookh, 2011). Such an approach includes a strategic direction and preparation, but it can also include education, communication, capabilities, culture, and compliance among other means. Planning of continuous improvements has proven to be good practice (Luftman, 2000; Chan *et al*., 2006) that sustains the effectiveness of the Framework (i.e. from design, implementation, monitoring). Moreover, it assures that any flaws or weaknesses in the alignment process can be acknowledged, amended, and re-secured towards the positive outcome of alignment. Accordingly, re-assessment of internal control is recommended due to its interchangeable nature of an environment. A practice highlighted from early 1999 by the Combined Code (also known as Turnbull report) as it has played an incremental role in identification effectiveness flaws and gaps (The Institute of Chartered Accountants in England and Wales, 1999). Most often positive indicators of alignment effectiveness are stated in terms of common objectives achievement, acceptable residual risk, reduced incident frequency, reduced scale of loss, positive feedback from executives' surveys, maturity advancement from one level to another one, market share increase, maturity of formalisation and centralisation (Alecsić and Jelavić, 2017). The identified maturity level is often compared against industry baselines to determine the degree of control function effectiveness.

For the reasons mentioned above, *CsM - ERM Strategic Alignment Framework* incorporates all components in order to assure a security baseline for organisations.

4.4.4 Benefits of adopting the CsM - ERM Strategic Alignment Framework

Previous theory and practice of the strategic alignment of both CsM and ERM have a fragmented legacy. The findings of this research suggest even a misleading legacy in some cases due to unclear terminology, scope, and meanings. Much of the current frameworks revolve around IT, IS, or RM alignment. The *CsM - ERM Strategic Alignment Framework* is proposed in order to bridge the three literature gaps: as stated in Literature Review (Chapter Two), research gap found based on systematic literature evaluation (Chapter Three), and research gap framework evaluation (Chapter Four, Section 4.3). This Framework introduces and sheds insights on common governance across all three domains built on the research gap. While the Framework helps to avoid any duplication of efforts, it incorporates the modern CsM that adopts wider assets protection (not only partially as so in IS or IT) and

the wider principles of ERM; in turn combining together two risk controls and two risk oversights that often duplicate each other. Such practice has been scarcely considered**.** The lack of clear practices regarding ERM, CsM, and alignment implementation leads to a fragmented theory and applicability. The framework thus proposes to yield clarity through a unified governance that comprises both controls and oversight. The framework emphasises how profitable it is to assign value to intangible and tangible assets, something that has been omitted in some studies. It compounds a recognition of temporal trends and acknowledges its developments. Additionally, it clarifies both domains' theory and the definitions and meanings of terminology. Finally, it proposes to leverage an awareness of misalignment and value of collaborative effort.

The specificity of the Framework is that it extracts derivation from theory, current practices, and regulatory framework, as well as unifying external and internal pressures in a single way to coordinate in accordance to the identified maturity level of security (internal), expectations, and targets. It harmonises responses itself with the external pressures/influences. This is all done with the intention of ensuring that the Framework is properly optimised to both environments as well as being specifically adapted for the financial industry. It thus creates a common risk governance that holistically manage risks. The Framework contributes towards an understanding of how organisational appetite, culture, governance, risk oversight, risk profile, maturity, compliance, structure, performance, and leadership are dependent on a strategic risk governance; most often these aspects have been investigated previously in isolation.

Particular attention is paid to baseline expectations in order to embrace a prudential practice of risk oversight. The advantages of adopting the research Framework is that conformance, performance, sustainability, and effective strategic alignment between CsM and ERM are ensured. From its initial phase, the Framework proposes to identify the requirement—the minimal baseline expectations to which an organisation shall abide in order to ensure proper resiliency. It considers the external environmental pressures as a preparation method before implementation. The specificity of this phase is advantageous because it defines the purpose, requirement before implementation (internal and external), limitation and constraints. In other words, it supports a common purpose for CsM and ERM through strategic lenses that in turn align planning, control, measurement, and mitigation measures in one unified mechanism. Moreover, the alignment brings the benefit of defining a common risk profile, based on which the risk appetite is forged in accordance with organisational capabilities.

Additionally, unifying the principles of CsM and ERM supports a common culture and communication within the organisation. The *CsM - ERM Strategic Alignment Framework* is a solution to avoid duplication of strategies, policies, guidelines, and procedures.

Overall, the first phase of the framework anticipates effects and interdependencies of an external environment within today's business context, and acknowledges internal requirements and dependencies and prudence in order to ensure the effectiveness, sustainability, and resilience of an organisation in the long-term.
Furthermore, one of the benefits of Phase Two of the Framework is that it is driven by managerial directions to establish risk appetite, structure, processes, responsibilities, and commitment. Considering external and internal environment pressures prompt a rethink of what is expected and how it is expected to respond. The Framework puts forward the view that a clear statement which identifies an organisation's purpose and objectives, appetite, structure, processes, responsibilities, and commitment is a part of proactive practice. Accordingly, the advantages are that the expected 'norm' and result are defined beforehand in accordance with both external and internal expectations and thus legitimacy. The 'relationship' of CsM and ERM through alignment has the advantage that it delegates departmental communication to identify wider vulnerabilities in terms of structure and processes alignment. It also creates a mechanism that, once unified, has a common capability to respond to external vulnerabilities and threats. This implies that at their roots, both domains are driven by RM principles. Therefore, the alignment has the benefits of increasing the performance based on the response to threats. Confirming that the alignment creates collaboration between departments, the cost of risk awareness can be decreased instead of two different training sessions that refer to enterprise and cyber risks. When compiled together, this widens the understanding of organisational risk exposure. A similar practice can be applied to guidelines and communication campaigns. As such, the Framework advocates a common mechanism of control, monitoring, measuring, and ultimately a common solution to increase resiliency.

The Frameworks supports acknowledgement of management directions (driving principles: philosophy, appetite, and directions) beforehand and optimises as needed to predict strategic requirements. Once external and internal requirements are identified, managerial directions are acknowledged. These benefits of the Frameworks clearly delimitate what is expected, why it should be done, and how it should be applied. It renders dependence on a cyclical deployment of actions that, once omitted, might affect the achievement of organisational

goals and mission. Such a practice shall ensure that implementation is in accordance with organisation objectives, capabilities and limitations, identifying current situations (assets, threats, vulnerabilities and control), identifying the risk owners, location, the source of threats as well as leverage an enterprise-wide implementation security.

For instance, Phase Four of the Framework (implementation directions) is mainly based on the identification of organisational practice profile, assessment, alignment of processes, response and communication, and delivery of results. Once again, it supports an informed implementation which assesses organisational risk profile based on a maturity model diagnosis. On this basis, the advantages are that the organisation understands its current exposure and capabilities profile and can set strategic directions as well as implement corrective measures.

It is a continuous measurement of suitability, adequacy, and effectiveness of organisational risk approach, and thus its strategies, applicability, and response are advisable to assure value delivery.

Therefore, financial organisations should consider the adoption of *CsM—ERM Strategic Alignment Framework* to attain the following advantages:
(1) create a common risk governance for risk control and risk oversight to support achievement of the overall business strategy and objectives;
(2) define common objectives in balance with organisation goals and objectives (all domains are equally important);
(3) help avoid bias in decision-related to investments or budget allocation;
(4) define what will be protected (tangible and intangible assets);
(5) correlate capabilities of CsM with ERM whille risk appetite and tolerance is aligned with the organisational risk appetite, risk tolerance and acceptable residual risk;
(6) provide due care for risk oversight and in turn leads to competitive advantages;
(7) establishes compliance (unified mechanism ensures efficiency of risk oversight);
(8) develop a cross-domain knowledge;
(9) efficiently understand how risk can overlap and how it can be managed holistically;
(10) increase business performance due to increased risk resiliency;
(11) employ fewer as risk governance optimises use of resources;
(12) lower costs and reduce effort;

(13) maintain shareholders' and stakeholders' trust that the organisation is strategically led;
(14) unify safeguards and countermeasures, and in turn, minimise loss;
(15) provide awareness of Framework capabilities and in turn establishes proactive and continuous risk oversight;
(16) ensure continuous performance assessment;
(17) create a shared communication;
(18) promote a proactive strategy in achieving resiliency with careful consideration to internal and external requirements;
(19) be driven by a maturity-performance relationship;
(20) consider a varied spectrum of variables (strategy, structure, culture, organisational design, processes, leadership, technology, structural alignment, risk appetite, risk tolerance) that can impact the return on investment (ROI) and performance (Chan, 2002);
(21) consider operational dimension (e.g. processes, infrastructures, communication, competence, governance, partnerships, scope, architecture or skills) when implement the strategic alignment, respectively a structural alignment;
(22) consider cultural dimensions as significant determinant in implementation, hence the human aspects are a variable (informal procedures, norms, beliefs, behaviour, ethics);
(23) address industry-specific needs, most frameworks are generic and do not address financial industry-specifically (such as regulatory compliance for the finance industry);
(24) promote executives' involvement—being a top-down approach;
(25) recommend optimisation based on organisational needs;
(26) integrate shared risk oversight (unified capabilities of reporting, analysis and mitigation);
(27) ensure a continuous identification for internal challenges;
(28) perform assets valuation (known as 'value at risk' (VaR)) in conjunction with CsM and ERM in accord with organisational objectives. Thus, prioritisation of actions is made in alignment with all three components and ensures that the common valuation leads to an optimised response, whereas a silo valuation presumably lead to an incorrect response;
(29) ensure a coherent terminology and theory through a common strategy, policy and guidance;
(30) compounds a hybrid dimension of all four dimensions (Quadrant 1: Adoption-theoretical focus, Quadrant 2: Implementation, Quadrant 3: Maturity assessment, Quadrant: 4 Assesses compliance) in one single framework and thus able to act on its own as an integrative mechanism without additional support of other frameworks.

Overall, the *CsM - ERM Strategic Alignment Framework* benefits are accountability, transparency, self-preservation, and response preparedness to ensure that negligence is avoided, and less disruptive actions lead to organisational value (Posthumus and Von Solms, 2004; McKinsey, 2015; KPMG, 2016). Additionally, the formalised procedure triggered by the research Framework demonstrates that the due care for risk oversight is addressed and the collaborative efforts support the effectiveness of control.

4.5 Conclusion

Hence the Framework relies on derivations from Chapters Two and Three as a baseline in the development of this chapter. On these premises, this chapter has been further developed into three sections: 1) supporting theories, 2) prior frameworks derivations, and lastly 3) theoretical CsM - ERM Strategic Alignment Framework.

Regarding the first section, supporting theories are chosen based on the premises of governance, alignment, and coordination of interdepartmental control. Thus, Contingency Theory and Institutional Theory are driven by strategic contingencies and dependent factors within an internal and external environment. This agreement demonstrates inclusiveness of legacy support for the alignment mechanism that combines two approaches for a common and integrated purpose: alignment. Each of the theories has specific philosophical perspectives, and their association illustrates two different insights (institutional norms and variations of contingencies) with a commonality based on performance directed by sustainability (Contingency Theory) and legitimacy (Institutional Theory).

The second section concerns the examination of supporting frameworks through the lenses of academics, practitioners and regulators in order to understand the applicable procedures for all three domains (CsM, ERM and Alignment). Accordingly, compelling evidence in regard to ERM frameworks of academics has illustrated that their contribution represents a descriptive approach (lack of empirical evidence). Consequently, the applicable procedures of establishing an ERM framework are incomplete/immature and the need for a more realistic and practical approach has been argued. On the contrary, the practitioners' frameworks have shown practical consideration for implementation. Looking at how practitioners have addressed the issue, there have been two categories of supportive entities: practitioners' associations and vendor-advisory organisations. The voluntary implication of these frameworks refers to vendor-specific frameworks, which happen to have been tailored to the financial industry.

Overall, this chapter has addressed the research objectives: *to identify, analyse and critically evaluate academic, industry-based and regulatory literature regarding ERM, CsM and their alignment and explore the current state of the topic*, in order to understand the value of this research. Although the problem of risk exposure is difficult to eradicate totally, alignment can ensure due diligence (legally ensure avoidance of negligent practices) and determine appropriate governance to ensure a fewer losses. A more efficient manner to counteract cyber risk (namely, frameworks aiming to sustain this initiative) is necessary because a lack of safeguarding measures and awareness (due diligence) along with misalignment could result in liability disputes besides other negative effects on society as a whole. Furthermore, the framework proposes to support organisations in generating enhanced governance procedures for themselves (emphasising responsibility and leadership) and to seize opportunities centred on risk-informed choices, striving to contribute to the achievement of societal risk resilience regarding enterprise and cyber risks at all times.

In order to explain how this research has been undertaken (through which means, methods, and tools), the next chapter (Chapter Five) outlines in detail how the research problem is explored. Accordingly, a specific methodology is chosen in close relationship to the research aims and objective.

5. Chapter Five: Research Design

5.1 Introduction

Previous chapters have considered the literature as a baseline to address the research questions. This methodology explains how they correlate with the research questions (Bryman and Bell, 2007; Bryman, 2012). This chapter introduces the steps taken in the development and execution of the research. It contains a theoretical discussion regarding what a research methodology represents and how it consequently sets the researcher's priorities (Saunders, Lewis and Thornhill, 2015). '[B]usiness research may be defined as a systematic inquiry whose objective is to provide the information that will allow managerial problems to be solved' (Blumberg, Cooper and Schindler, 2004, p. 4); this quote mainly define what a research rationale is, respectively, if applied to this particular chapter, it explains how the 'systematic inquiry' is deployed.

This chapter is subdivided into sections which explain why specific research methods were chosen over others. Section 5.2 summarises the totality of components that were selected, Section 5.3 explains the research purpose type, and Section 5.4 which clarifies the research philosophy chosen. Sections 5.5 and 5.6 discuss the approach and strategy, and Section 5.7 outlines the methodology where research methods and techniques chosen are emphasised. Section 5.8 explains how the data was analysed. Sections 5.9 *et seq.* examine the research rigour, limitations and ethical consideration, and Section 5.15 provides a chapter conclusion.

5.2 Research design

In order to justify how this research commenced, the research design defines how its components (such as purpose, philosophy, approach, strategy, time horizon, research methods and techniques, and research boundaries) all intersect (Creswell, 2004). Additionally, a research design indicates how the research methods and analysis are applied (Bryman and Bell, 2011). Thus, Figure 5-1 below exemplifies the research design through the lens of the 'research onion model' of Saunders, Lewis and Thornhill (2015).

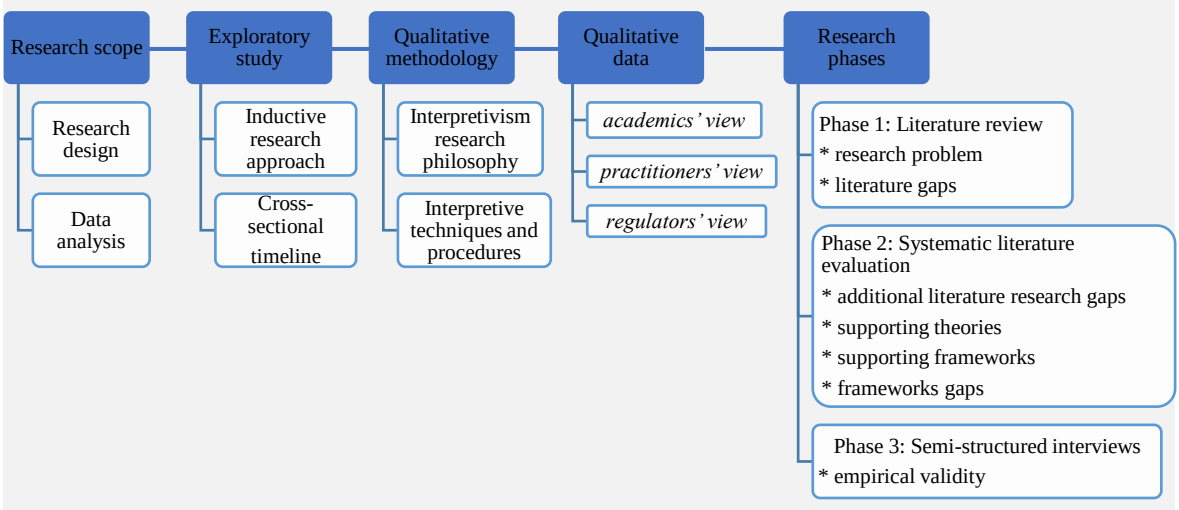


Figure 5-1 Thesis' Research Design

Source: The Researcher

A research design represents a planned sequence of steps (also known as sequential research design) that map together and contribute towards the research goal achievement (Robson, 2011; Maxwell, 2013; Leavy, 2017; Thomas, 2017), Figure 5-1 highlights how the research design is conducted and interconnected. A planned and detailed research design acts as a 'map' that assures research repeatability (Maxwell, 2013). Having demarcated the research design, this research serves to understand and explore the phenomenon. It does so through the adoption of a qualitative research design that intends to capture flexibility in responses and to foster in-depth answers and meanings (Silverman 2007; Leavy, 2017). With this scope in mind, the following data, tools, and techniques have been designated:

1) Secondary
   - Literature review
   - Systematic literature evaluation
2) Primary
   - Semi-structured interviews

By considering secondary and primary qualitative data, the research design explores the phenomenon under an inductive research approach. Regarding the time frame, this research is limited to research degree prerequisites. Consequently, it embraces a cross-sectional design to explore the phenomenon and the data is collected over a given period (Sekaran and Bougie, 2013; Saunders, Lewis and Thornhill, 2015; Bryman, 2016). This results in a methodological research approach, circumscribed by time whilst seeking to explore the past and current states of the phenomenon. On the other hand, the option to undertake a longitudinal study would be unsuitable for this research as it requires long periods of

examination (Saunders, Lewis and Thornhill, 2015). Regarding the research design selected, data analysis of both secondary and primary data relies on interpretive research philosophy driven by research questions.

5.3 Research purpose type

A research purpose type represents the outcome that a researcher seeks to produce (Blaikie, 2009) and in the case of social research, the most common types of research purpose are descriptive, explanatory, and exploratory.

This research adopts an exploratory design purpose because it seeks to investigate beyond explanation and reasons behind a phenomenon (Bhattacherjee, 2012). Consequently, by selecting the exploratory research type, this research aims to address how the research problem has been analysed in the past, and whether this research would provide a resolution (Sekaran and Bougie, 2013; Saunders, Lewis and Thornhill, 2015).

In contrast, adopting an explanatory or descriptive research purpose would only address causality and description and may therefore not render an enhanced understanding of the research problem. Concerning those mentioned above, it is obvious that descriptive research is unsuitable as it provides a significant amount of information about a specific phenomenon and its characteristics, in a detailed format, to contribute to the understanding of a problem (Bhattacherjee, 2012; Sekaran and Bougie, 2013). In a simplified manner, the profile of a phenomenon or a problem (Saunders, Lewis and Thornhill, 2015) can be considered but, if so, would be an incomplete approach towards the scope of this particular research. Likewise, adopting an explanatory research type would only seek explanations for a given situation; its main characteristics being rooted in elucidating the relationships amongst variables (Saunders and Lewis, 2012).

Regarding the limitations, neither explanatory nor descriptive research types are suitable. Consequently, adoption of an exploratory research type is appropriate and in turn, the research it proposes would move beyond mere identification and observation and develop into an exploration of further possible answers.

5.4 Research philosophy

A research philosophy (also known as a research paradigm) indicates the beliefs and assumption (Saunders, Lewis and Thornhill, 2015) based on which a researcher explains the nature of specific knowledge (Maylor and Blackmon, 2005; Bryman and Bell, 2007; Saunders and Lewis, 2012). The philosophical assumptions/beliefs refer to human

knowledge as epistemological assumptions (Saunders, Lewis and Thornhill, 2015) and how it interprets the reality. Another perspective is that of ontological assumptions, which refers to the problems encountered by a researcher (Saunders, Lewis and Thornhill, 2015) regarding his/her perception and how the research problem is perceived by others (Bhattacherjee, 2012). It usually relates to an external perception (Bryman and Bell, 2007). A third perspective of research philosophy is that of axiological assumption. This philosophy refers to the effects of researchers' values/ethics regarding the content of the research (Saunders, Lewis and Thornhill, 2015).

Referring to research philosophy options, general business study research can be based on several main types of philosophies: Positivism, Critical Realism, Postmodernism, Interpretivism, and Pragmatism. Selecting a Positivism philosophy would lead to research findings being based on testing a theory (Myers, 2013). Therefore, it is unsuitable for this research as it relies on 'cause and effect' and considers the use of hypothesis and quantitative measures to test a theory; not considering the perspectives of human interpretation and behaviour but instead considering it as an independent variable (Saunders and Lewis, 2012; Blumberg, Cooper and Schindler, 2014).

This research selects and adopts the philosophy of Interpretivism (also known as phenomenology) because this philosophy provides a practical and theoretical perspective of the phenomenon through an inductive approach. Interpretivism philosophy enhances understanding and explanation of the phenomenon through the eyes of individuals and their personal experiences (Blumberg, Cooper and Schindler, 2014; Gray, 2014; Taylor, Bogdan and DeVault, 2016). Interpretive research emphasises the connotation of meanings in a social context to understand the 'status quo' of a phenomenon (Myers, 2013). Such an approach seemed suitable and justified given the fact that there is scarce literature concerning the alignment of risk governance where practical insights and meanings prevail. Moreover, the practical facets endeavoured to explore and subsidise the interpretive philosophy perspective; henceforth the research intends to capture the views, behaviours, and understanding of the phenomenon (Thomas, 2017).

Adopting the interpretive philosophy and acknowledging the possible biases, the Researcher recognises that in order to achieve the research objective, self-reflexivity and neutrality represent an additional point to consider. Therefore, self-awareness can distinguish the way information might be misinterpreted due to Researcher 'positionality' in terms of own

beliefs, background, gender or ethnicity (Tracy, 2012; Saunders, Lewis and Thornhill, 2015; Thomas, 2017).

5.5 Research approach

A research approach represents the plans and the procedures upon which decisions are taken to underpin the collection, analysis, and interpretation of data (Creswell, 2014). Given the exploratory specificity of this research, the research approach is based upon an inductive approach because data collection and analysis intend to explain patterns, facts, causes, and meanings (Sanders *et al*., 2009; Blumberg, Cooper and Schindler, 2014; Gray, 2014; Saunders, Lewis and Thornhill, 2015). A particular characteristic of inductive research is that it is a theory building approach, which seeks to discover insight and understanding of the research context (Bhattacherjee, 2012). On the other hand, selecting a deductive approach would support a causality understanding of a problem verified through hypotheses testing (Saunders and Lewis, 2012). For that reason, by choosing an inductive approach, the results are drawn based on the discovery of meanings instead of testing hypothesis (as in the deductive approach) (Bhattacherjee, 2012). Consequently, the inductive approach is considered a 'bottom-up' approach, hence the result appears upon exploration of the research problem (Myers, 2013) and the theory is developed post analysis (Saunders and Lewis, 2012). Moreover, given the qualitative nature of the research, exploring a social phenomenon through an inductive approach is feasible for small samples of participants, respectively semi-structured interviews (Leavy, 2017).

5.6 Research strategy

A research strategy represents a significant component of the research design as it portrays the logic of which responses are identified (Mason, 2013). It is strategic in its nature because it emphasises the relationship between the research goals and how questions are answered (i.e. the strategic purpose of the planning of methodology). As the 'strategy' refers to a plan of action to be achieved and guided by a goal (Saunders, Lewis and Thornhill, 2015), the research strategies refer to methods and techniques employed to answer the research questions and thus set the research directions. Based on an exploration of various strategies, the research strategy was chosen on the acknowledgement of other possible means to respond to the research questions (Mason, 2013).

Commonly used tools are experiments, surveys, case studies, action research, grounded theory, ethnography, and archival research (Saunders, Lewis and Thornhill, 2015).

Experiments imply testing of theories through various means, usually in a laboratory-based format (Saunders and Lewis, 2012; Saunders, Lewis and Thornhill, 2015). The survey represents a structured research strategy of gathering data about a specific population (Saunders and Lewis, 2012). Ethnography refers to research that focuses on culture or social aspects of a specific group (Saunders, Lewis and Thornhill, 2015).

Adopting a grounded theory would be unsuitable as findings emerge from explanation (Saunders, Lewis and Thornhill, 2015) based on coding and contrast (Fisher, 2004). Likewise, action research is inappropriate as it involves participation as a learning process, and results are based on practical results (Saunders, Lewis and Thornhill, 2015).

Having considered the purpose and research strategy specifics of this research, data has been collected in accordance with the interviews limitations attributes.

5.7 Research methods (methodology)

Research methods represent the general guidance that structure the execution of how data is collected and organised (Jankowicz, 2005; Silverman, 2007; Bryman and Bell, 2007). More specifically, it defines the Researcher's preference regarding how he/she explores and proceeds in studying the phenomenon (Silverman, 2007). In short, it refers to the way the problem is perceived and how answers are pursued (Taylor, Bogdan and DeVault, 2016). Also described as a methodology (Silverman, 2007), it incorporates the research techniques as a means of applying the guidance through procedures (Jankowicz, 2005). Therefore, the methods for conducting the research embody the techniques and tools proposed for identifying, defining, interpreting, and analysing the problem (Bazeley, 2013; Bryman, 2016). Very often, research methods are in the form of the mono method, mixed method, and multi-method (Saunders, Lewis and Thornhill, 2015). In accordance with the research aims, this research adopts qualitative research methods as mono research techniques.

5.7.1 Qualitative research methods

This research adopts qualitative research methods for the reason that it implies a combination of multiple perspectives that are contextual and applied in practice; a fact that assures variety strength and validity of results (Blaikie, 2010; Robson, 2011; Sekaran and Bougie, 2013; Gray, 2014; Saunders, Lewis and Thornhill, 2015). The nature of this research is qualitative as it seeks to explore the qualitative aspect of concepts, and meanings based on qualitative interpretations (Mason, 2013; Leavy, 2017). Organised in phases, the first priority is given

to the literature review and systematic literature evaluation, followed by a second phase where qualitative data analysis is undertaken in a field exploration of the phenomenon through interviews. This represents a **sequential exploratory design**, which orders the sequence of the steps (Robson, 2011) that compound data for validation. Nonetheless, it concerns the qualitative rational. On the other hand, a sequential explanatory design would firstly use quantitative data and later on would use qualitative data for explanatory purposes (Robson, 2011).

The decision to make use of qualitative data stands to enhance the prospect of findings through the exploration of a range of perspectives gaining further insights and an in-depth understanding regarding the research problem (Robson, 2011; Rubin and Ruin, 2012; Creswell, 2014) and supporting compelling findings (Taylor, Bogdan and DeVault, 2016).

Moreover, by means of qualitative methods, research yields diverse viewpoints, thus enhancing varied and justifiable outcomes via responses obtained through semi-structured interviews and then assimilated all altogether.

5.7.2 Techniques and procedures of data collection

Data collection and data analysis are divided into two categories for transparency (desk research and field research) and follow a sequential exploratory design that relies of secondary and primary data.

5.7.2.1 Secondary data

Literature Review—Phase One

The first stage of the research investigation starts with a traditional literature review based on a manual selection of academic papers. Within the initial literature identification, the topic is broadly searched and researched, and once reviewed, the documents are allocated to a more specific area and themes (e.g. cybersecurity, RM, ERM, alignment). Although the search determines various results, an initial estimate of how many papers are available was unfeasible in this particular case because the data retrieval covered the research problem partially. Therefore, the selection of academic papers was made individually. Consequently, the research is interdisciplinary of three different disciplines. The exploration of prior research begins with an electronic database search, based on keywords and simple phrases. Later on, their complexity increases based on data extracted from analysed papers and phrases suggested by Internet search engines or research databases. Based on an inductive

approach, various key terms and phrases are identified, hence the disciplines' terminologies fluctuating over the years (See Appendix B). Once the keywords and phrases results are significant, the same keywords were used to create automatic alerts from electronic journals and Google Scholar to ease the volume of search and ensure an up-to-date access to new references. Accumulation of research sources/contributors continued through an analysis of references regarding the newly identified references. Based on identified references, a literature synthesis was extracted in the form of field notes (electronic and physical format). Through the field notes, the researcher registers summaries of scrutinised data. Following this, further meanings are extracted and evaluated (Zikmund *et al.*, 2013).

When carrying out this particular literature evaluation of academic sources, the main materials considered were electronic peer-reviewed journals. Books and conference papers were not included in the main analysis (see Table 2.8, Chapter 2) and the Researcher seldom referred to additional sources for definitions or secondary purposes. Regarding the resources used, in the case of practitioners and regulators legacy, various sources such as professional articles, reports, guidelines, policies, standards and laws were identified and reviewed. As a result, 169 academic papers, 91 practitioner's papers and 51 regulators documents (312 in total) were explicitly analysed. By employing the literature review, the scope of this stage levers answers to Question 1 and Question 2 of this research.

Systematic Literature Review—Phase Two

Consequently, the literature review of this research represents the rationale and the basis of further investigation. The systematic review's purpose is to 'locate, appraise, and synthesise' the evidence and solutions suggested by prior literature (Boland, Cherry and Dickson, 2013). The systematic literature review evaluates and interprets prior studies of scholars, practitioners, and regulators relating to the research paper's problem (Kitchenham and Charters, 2007; Boland, Cherry and Dickson, 2013). Therefore, data analysis relies on a thematic analysis that studies the qualitative nature of research through a pre-planned assessment protocol (Boland, Cherry and Dickson, 2013) in order to identify the current research state, limitation, and research gaps, and in turn to validate the position and contribution of this research. By adopting a systematic literature review, the analysis starts with 312 sources initially identified in the literature review along with additional references supplemented to sustain the validity of any findings and research gaps. In contrast to a literature review where research planning and exploration phases were at the core, the

systematic review phase focuses on mapping the key elements as well as evaluating and synthesising the findings in order to depict the various dimensions of the phenomenon (Greenhalgh *et al*., 2004). Owing to the research problem involving a broad field of research, the literature was explored thematically (commonalities, difference, typologies, and trends) in order to understand the prominent themes and correlations related to the research problem (Dixon-Woods *et al*., 2005). This supports understanding of the current research problem and how the identified summarised derivation can contribute towards the Framework.

Being qualitative research, data is explored through an interpretive philosophy in order to understand behaviour and attitudes towards the interchangeable use of terminologies and meanings, respectively the effects. Owing to the research problem being a broad field, the research theory is fragmented into few disciplines. The investigation aims to identify commonalities, difference, typologies, and derivations of current research trends. Therefore, both data selection and analysis were manually made based on scope, the research paper's questions that demarcated the inclusion, and exclusion criteria (Boland, Cherry and Dickson, 2013). Thus, the research is constructed on the review on qualitative evidence of academic journals, industry publications, and regulatory documents for a wider understanding of the phenomenon. Exploratory in its nature, the selection of papers is made through a database search (search string) but also through consideration of references from relevant publications identified regarding relevance, paradigm typology, research dimension, focus, strengths, limitations, key findings, contribution, and/or omitted components.

The additional literature review follows a specific methodology based on the Four-Quadrant Framework developed by Althonayan (2003). Optimised to the research problem, the Four-Quadrant Framework is adapted to evaluate the literature on four criteria: Quadrant 1: Adoption-theoretical focus, Quadrant 2: Implementation, Quadrant 3: Maturity assessment, Quadrant: 4 Assesses compliance. In this way, the literature was identified and categorised to support in understanding and evaluating existing literature concentration and limitations (Kitchenham and Charters, 2007). Additionally, exclusion criteria were based on research aims connection with the identified literature; the technical and operational focus was another exclusion criterion considered, hence the research focusing on the strategic views.

5.7.2.2 Primary Data

This third stage of data collection is focused on collecting primary data from interviews.

Collecting primary data through interviews

Semi-structured Interviews—Phase Three

The interview represents a research tool that elicits responses from respondents in the form of a discussion between one or more parties and the researcher (O'Gorman and Macintosh, 2014; Gilbert and Stoneman, 2016). Focusing on the research topic, an interview objective is to provide information about a particular phenomenon in the form of empirical data, respectively real-life experiences and insights (Eriksson and Kovalainen, 2008). In undertaking this step, the design of interviews can be typically unstructured, structured, and semi-structured. Considering the research goals, it seems unfeasible to undertake unstructured interviews in this research because the research objectives are specific. Even if unstructured interviews might elicit various and unforeseen information (O'Gorman and Macintosh, 2014), the format of the unstructured interview is flexible (open conversation) and thus unfeasible; henceforth the responses might be conducted by what an interviewee considers relevant (Bryman and Bell, 2011), and it might not necessarily abide by the question investigated. Using the unstructured interview, difficulties in developing meanings through comparisons may also evolve (Bryman and Bell, 2011).

Likewise, the structured interview is not appropriate for this research because its main characteristic is to assure production of significant data (quantitative). Although it is a fast method of gathering data and the risk of biases is low (O'Gorman and Macintosh, 2014), there are also limits such as inflexible conversation (standardised questions format), possibly inducing specific responses or allowing for some aspects of the phenomenon to be omitted (Bryman and Bell, 2011).

Lastly, the semi-structured interview seems appropriate to use for this research because it differentiates itself by its flexibility and versatility in gathering responses (O'Gorman and Macintosh, 2014; Gilbert and Stoneman, 2016) and thus it aligns with the research problem. Even though semi-structured interviews have a pre-formulated format of questions, it is flexible and allows the researcher to go in a specific direction (if necessary) during the interview as it wants to encourage the respondents to discuss openly (Myers, 2013). Probing and prompting are attributes permitted in this type of interview (Gilbert and Stoneman, 2016). Therefore, in some exceptional cases, where the elicited answers are partial or ambiguous, a repetition of the question or a slight rephrasing of the same questions/wording may yield a more accurate result (Sapsford and Jupp, 2008; Gilbert and Stoneman, 2016).

The semi-structured format is often referred to as an *interview guide* in deploying the interview and conversation (Bryman and Bell, 2011).

With the intention of incurring knowledge from practical evidence, the main interview method considered is face-to-face (individual interview) with senior executives responsible for risk oversight in different financial organisations. The benefit of the face-to-face interview is that it ensures direct contact with the respondents and can elicit open communication that prompts identification of a research dimension and attitude towards a social phenomenon (Gilbert and Stoneman, 2016). In addition, any doubts can be immediately clarified, allowing non-verbal communication, and thus questions can be adjusted and optimised in correlation to previous responses (Sapsford and Jupp 2008; Sekaran and Bougie, 2013). In as much as it has advantages, it can also have disadvantages such as a geographical barrier (Sekaran and Bougie, 2013), increased preparation, need for improvisation skills, effective communication skills, resource implications, and/or respondent inhibitions, to name but a few (Denscombe, 2016).

Alternatively, despite the advantages of a face-to-face interview, the Researcher is considering telephonic interviews as a secondary option to gather data. Hence, the research is not geographically limited, and a larger sample of respondents might be reached, in turn leading to more complex research (Flick, 2014). The decision to use two types of interviews is due to face-to-face interviews probably being unfeasible in some cases owing to the geographical dispersion, interviewee availability, time of reflection or even anxiety of some respondents (Robson, 2011; Gilbert and Stoneman, 2016). Furthermore, some studies suggest that telephonic interviews are more comfortable in terms of topic focus (Gilbert and Stoneman, 2016). Disadvantages of the telephonic interview are related to human-interaction and non-verbal cues or additional preliminary arrangements (call, messages) (Gilbert and Stoneman, 2016).

The interview format was elaborated based on preliminary results of secondary research results from the literature review and literature evaluation. The realisation of this approach rests on three motivations: first, an efficient interaction with the industry respondents; second, there is a collection of primary data that points out current trends and thus provides a means of comparison with previous data results; third, there is the possible identification of the missing *piece*, so to speak, that completes the whole picture through a qualitative and accountable perspective.

Therefore, the expert interview structure is created in a semi-standardised style, employing the open-ended question format to ensure flexibility in responses (Silverman, 2014). By undertaking a semi-structured interview, it assures consistency of answers by limiting deviations and strongly focusing on the answers themselves (Silverman, 2014). Moreover, it gives the interviewees flexibility when identifying new ideas/perspectives. Consequently, the Researcher wishes to take the opportunity to gain insightful information (tacit knowledge), as opposed to structured interviews where a researcher might predispose possible answers due to the open-ended nature of the questions. Although interviews are time-consuming, the format gains detailed feedback through questioning experts.

Having chosen these methodologies, it can be concluded that the research is based on qualitative methods and the feasibility of this proposed project is thus sustained by its explorative nature. Additionally, by applying two tools of data collection (face-to-face, telephonic interview (i.e. by Voice over Internet Protocol (Skype) or telephonic communication), the suitability seems to guarantee an alternative plan in case of an unfeasible method. Furthermore, the researcher's methodological approaches are to be interlinked to achieve the same goal and gain additional insight into the researched field (Flick, 2014).

Participant selection

The selection of participants was decided based on each potential participant's expertise, industry practice, and rate of response to interview invitation. Moreover, the pull of participants is strictly limited to being from within the financial industry (e.g. banks, retail banks, commercial banks, private banks, savings banks, postal saving banks, building societies, community banks, credit unions, corporate finance, mutual funds, hedge funds, mortgage brokers, clearing houses, finance organisations, and investment organisations).

Participant selection for both face-to-face in-person and telephone interviews is via:

1) Direct approach
    a. Identification of individuals that work within the Enterprise Risk Management, Risk Management, Information Technology, or Cybersecurity departments (whether other types of terminologies are used) was made. The criteria for selection was based on their direct involvement within one of the departments mentioned above, with focus on a managerial job position.

   b. Also, direct communication with a range of selected organisations was initiated and formal requests were sent.

2) Indirect approach, identification made through recommendations of peers (snowball and recommendations from professional associations; e.g. ISACA, International Information System Security Certification Consortium (ISC^2), RIMS, Global Association of Risk Professionals (GARP)). Targeting associations warranted that the respondents are affiliated and that the interview is targeted towards a precise specialised audience. Nonetheless, the respondents' selection criteria were also based on other criteria (e.g. industry, department, role superiority). In addition, specialised professionals from social media were targeted, and invitations were sent to members through open-wide communication platforms.

In this phase, the advantages of primary data collection (such as unbiased data) is that availability and originality add more value to the research, hence primary data representing a useful technique for identifying new valid data (Zikmund, 2013). Consequently, the sample is dispersed globally to steer and acquire meaningful and accountable primary data.

Sample population

The sample population refers to the selection of a minor set from a grand total (Saunders and Lewis, 2012) and can refer to people, organisations, places, products, services, and much more. For practicality, usually a specific sample that is considered representative is extracted rather than considering the whole total (Saunders and Lewis, 2012; Thomas, 2017). The total whole is labelled a 'sampling frame'. To extract the sampling (explicit sample) various techniques are used such as simple random techniques, systematic sampling, and/or stratified random sampling. The simple random technique refers to random numbers chosen, with the probability of any number selection (Saunders and Lewis, 2012). The second technique is systematic sampling, referring to a selection based on regular time intervals (Saunders and Lewis, 2012). The third technique is stratified random sampling and combines the previous two techniques while relying on geographical area separation (Saunders and Lewis, 2012).

In this research, the non-probability sampling techniques seem suitable hence there is an inability to define the total population within the financial industry on a global scale. Respectively, the sample of participants includes respondents from various sectors of the financial industry. Additionally, the geographical area location of respondents ranges from the United Kingdom, USA, Canada, Northern Ireland, Italy, Africa and Netherlands.

Along with quota sampling and purposive sampling (selected due to the correlation of respondent with research problem), the Researcher ensures that the sample can offer new insight, helpful in exploring the research question (Saunders and Lewis, 2012). Thus, this research uses non-probability sampling because the population is undefined since it would be impossible to define it globally and objectively. Secondly, it considers quota sampling as the respondents should correspond to specific characteristics (e.g. job position, expertise, industry). The purposive sample population selection criteria is based on job positions related to risk management or cybersecurity management. This criterion is considered depending on the organisation's governance structure. The pre-selection of the population is delimited regarding departmental involvement and does not include a specific rank/role as long as participants are top management executives that work in the financial industry. In addition, this research takes a gender-neutral position in selecting the sample in order to avoid any bias or discrimination. Undoubtedly, full addressability of investigation of all departments might underpin other aspects if gender is considered, different from the search purpose. For this reason, the investigation delimits its focus on ERM and cybersecurity comparative analysis and intentionally omits addressing all departments to ensure that the sample selection is associated with the research problem.

5.8 Data analysis

To respond to research questions, the qualitative data has been designated based on how appropriate it is for the research problem.

5.8.1 Qualitative analysis: interviews

The interview format is qualitative semi-structured, which can generate meaningful views of social reality (Mason, 2013) concerning respondent's perceptions of a particular context. While qualitative interviews are one of the most used methods in qualitative research (Mason, 2013), the results are dependent on the respondents' capabilities to interact and express an opinion and also the Researcher's ability interpret that which is narrated rather than what the interviewee says (Bryman and Bell, 2011). Moreover, the interview techniques are appropriate with the interpretive research paradigm because they aim to explore the qualitative dimension of the phenomenon and to reflect an additional dimension of the research problem. By this reason, selection of interview data collection relies on two complementarily techniques:

- Conducted in-person interviews (a number of 7 face-to-face interviews);

- Conducted by telephonic interviews (a number of 19 telephone interviews).

Such approaches have been adopted due to the geographical barrier as well as cost and time constraints. Likewise, many authors considered a combination of both in-person interviews and telephonic interviews to ensure additional views (e.g. Viscelli, Hermanson and Beasley, 2017). Distinguishing this dual approach is that it presents a variety of options in sample identification for the Researcher. Additionally, for accuracy, each interview follows an identical semi-structured format, where an interviewee's speech is aimed to be preserved through the use of a digital voice recorder.

Interview pilot study

Moreover, before the interview, a pilot test was conducted to ensure that the interview is appropriate regarding the questions' content and tone, the level of detail required in the answers, and the length of time needed to respond. The procedure was tested upwards to help prepare for exceptional cases; for example, should an interviewee refuse to record, or should the recording device encounter a malfunction. In this case, a pre-test also helped there to estimate the time length of transcription during the interview. Additionally, the pilot test was applied to validate the significance and clarity of questions. The pilot study was addressed to six participants: two academic and four industry experts from financial industry. As a result, from an initial 37 questions, two more were added to portray practicality of the phenomenon. 39 questions were finally refined and correlated with the Framework thematic and research questions; yet all aligned to the research aims and objectives. The first ten questions refer to organisational profile (e.g. geographical, industry, size) and to participant profile (e.g. role, job focus, experience, certifications) and experience to validate the quality of competences. The second part of the interview contains the remaining questions (29), which specifically address the research problem. Although the number of questions may seem high, during the pilot test, the results showed that adopting such approach can leverage a broader perspective of answers. The average time of interviews during a pilot study ranged between 35-75 minutes depending on the interviewee's characteristics.

To overcome difficulties in responding to the questions, some (22 questions out of 39) offered potential answers as pre-coded themes. However, before the interview, all interviewees were informed that the options available are mainly to open the discussion and alternative answers are welcomed. Henceforth interviews refer to 'inter' as an inside

perspective and ‘view’ specifies that it refers to an individual knowledge and experiences (Kvale, 2010).

To ensure reliability, the thematising and designing took place in the pre-interview phase, respectively a pilot interview (Kvale, 2010). Whereas interviewing, transcribing, analysis and verifying are phases of post-interview (Kvale, 2010). Correspondingly, pilot testing was used to evaluate comprehension of the research questions and their perceived relevance/validity for the chosen sample of respondents (Sapsford and Jupp, 2008).

Based on the feedback received from piloting the interviews, the questions were refined in terms of structure and meanings to better address real-world settings and research Framework format. For instance, for the format of question eight it seemed inappropriate to use ‘required’ (i.e. enforced/mandated requirement) and so the word was changed to recommended in order to infer that it is not mandatory. Likewise, question 11 was reformulated to clarify that it specifically refers to the attacks/level of threat encountered by the organisation. Question 12 was also reworded as it initially included ‘who is responsible’ and the question seemed to be misinterpreted hence it became common practice to state that for risk oversight and prevention all organisation members are considered responsible. In other cases, for example, question 13, clarification was needed to illustrate which type of departments were included (e.g. RM, ERM) in order to avoid biased answers. On the contrary, however, in question 14 a neutral word was used (risk control) to ensure that the question did not influence the answer. Instead, in question 15, when referring to a department name, risk governance was chosen. In the case of question 20, additional guidance was added to clarify what kind of response was expected. Likewise, question 24 was reformulated to clarify that it refers to the top senior executive and not to the perspective of other managers; executive board terminology was chosen instead.

5.8.2 Interview guideline

At its core, the interview structure is constructed based on the research Framework format and similarly relies on five groups of topics that query the contingency and extensive institutional applicability of CsM and ERM alignment within an organisational context, summarised in the below; see Appendix A for further details.

Phase One: ‘baseline expectations’ (strategic)

- Baseline expectations-preparation, understanding how risks are perceived through the perspective of internal and external factors;

- Cybersecurity Management, understanding behaviour towards risk;
- Enterprise Risk Management;
- Strategic alignment/ Interconnectivity and Partnership (purpose, objectives, strategy);
- Context of alignment (internal and external);
- Organisation mission and vision;
- Barriers;
- Benefits.

Phase Two: 'mandate managerial directions' (Administrative)

- Managerial directions;
- Strategic directions;
- Context of alignment.

Phase Three: 'establishment of strategic directions' (strategic-structural)

- Security governance, security programs, strategic alignment;
- Strategic alignment;
- Structural alignment.

Phase Four: 'implement managerial directions' (operational)

- Structure/Architecture;
- Process – to understand how an organisational risk exposure is dealt in the organisation;
- Accountability/responsibilities - understanding what they experience;
- Technology.

Phase Five: 'Monitoring and reviewing practices' – improvement (strategic-operational-structural)

- Monitor, measure, plan, re-align risk profile with risk practices;
- Barriers and limitations of CsM with ERM alignment;
- Benefits of alignment assessment;
- Recommendations and improvements – interviewee's general advice for experts that face similar issues.

The format of the interview avoids being intrusive or addressing sensitive questions. Therefore, the format focuses on strategic and governance aspects in order to understand how organisations generally plan their control. With all five phases being interrelated with the Framework thematic, it aims to ensure that all aspects initially identified are addressed in the primary data collection. In addition to correlation, post-interview notes were taken to

capture the immediate impression (Kvale, 2010). The Researcher transcribed the interviews verbatim instead of opting for selective transcription so as to ensure all information was gathered for later analysis (Gilbert and Stoneman, 2016). Transcriptions were reviewed to ensure accuracy and then put through NVIVO software. NVIVO software is a digital tool especially for the analysis of qualitative data. The transcriptions were out through NVIVO for information extraction through coding and thematic analysis. Moreover, the software package NVIVO is justifiable because it allows to store data, analyse, and retrieve the verbatim transcript of interviews at any later point (Barbour, 2014). By undertaking computer-assisted analyses as opposed to conventional analysis, the data derived is reduced (Barbour, 2014).

The interview contains some open-ended questions, representing un-coded questions (Sapsford and Jupp, 2008) which are open to variable answers that need to be categorised at a later point. Such range of answers offers various insight, which is not predetermined by the Researcher. By using a computer-assisted analysis for qualitative data, this research implements the method recommended by O'Leary (2014) based on five stages: (1) organisation of raw data, (2) storage and coding for reduction purposes, (3) thematic analysis for identification of concepts, patterns, interconnectedness, understanding similarities, (4) interpretation, and (5) theoretical visualisation of results and understanding. All of the aforementioned ascertain a systematic way of organising information, encoding the research translation of viewing facts (Boyatzis, 1998).

5.9 Research reliability

This criterion represents an expected quality level of techniques used (Bryman, 2016); for example, trustworthiness and accuracy of the methodology involved (Bryman, 2011; Mason, 2013). The research quality is critical for any research (Pellissier, 2007) because it represents the trustworthiness and reliability in all aspects of the research. Reliability is the degree of quality on which research can be replicated (Pellissier, 2007). It can refer to internal validity (findings vs. reality) or external (findings vs. other contexts), and thus the accuracy of methods represents the pillars in achieving reliable research.

Relying on rigorous research ethics, this research aims to assure its reliability based on objectivity and relevance as it employs the application of moral principles that rely on moral stance (Myers, 2013). Thus, this research is consistent, transparent, and accurate in listing its research strategy and methodology so as to assure research reliability. Accordingly, the

research content is in accordance to the research problem (which is based on the construction of theoretical foundation) and sustained by replicable methods and techniques. For instance, prior to testing the interview, a data collection protocol and interview guide were created. In the case of interviews, pre-testing of questions is an initial verification. This is followed by the interview's transparency and consistency, which is sustained by audio recording (tape recording) and transcribing techniques (Silverman, 2014), respectively in verbatim transcripts. Moreover, the Researcher considered note taking during the interview should recording be rejected by the respondent (Sapsford and Jupp, 2008). However, none of the respondents requested such practice.

5.10 Research replicability

Research replicability represents the possibility of another researcher replicating the research at another point in time and identifying similar results (Bryman, 2016). Thus, an accurate documentation of data collection and analysis can ensure credibility. This research considers this aspect along with precision characteristics of theoretical concepts (Bhattacherjee, 2012), considers parsimony (unique and own explanation of a concept/s) and acknowledges falsifiability (untruthful findings) aspects. However, the extent of replicability depends on the Researcher's reflection of legitimacy and ascribed characteristics as every person is unique and personal attributes, social skills, or research skills are different (Lewis-Beck, Bryman and Liao, 2004; Sapsford and Jupp, 2008). Therefore, the Researcher acknowledges these aspects and accepts these possible contextual and procedural variables.

To overcome possible procedural biases, the Research uses standardised interviews, aiming to use the same wording format, procedure, length, and sequence (Sapsford and Jupp, 2008) in all interviews in order to assure good practices.

5.11 Research rigour (validity)

The research criteria of rigour refers to the quality of contribution generated (Bryman, 2016) and denotes if the interpretations made by the Researcher are genuine and that they respect academic scientific standards (Bryman, 2011; Myers, 2013). It can be based on descriptive, interpretive, evaluative, or theoretical validity (Maxwell, 1992). Research rigour can also emphasise the trustworthiness of the whole process of data collection, analysis, and elucidation (Flick, 2008). Therefore, the rigour and quality of this research are based on the validity, transparency, and reliability of methods that in turn might yield various perspectives (Bashir, Afzal and Azeem, 2008).

5.12 Research delimitation

Delimitation of research can be defined as parameters of investigation that are intentionally restricted by the researcher to cap the inquiry to stay within a specific scope (Mertler, 2015; Molina, 2015). This research delimits its investigation through fieldwork delimitation and literature delimitation.

5.12.1 Fieldwork delimitation is related to the focus of the research in analysing the phenomenon as the research undertakes its empirical investigation focusing on specific fieldwork (financial industry). Accordingly, the strategic alignment framework might be optimised and used for other industries because the conceptual framework adopts a general perspective due to limited literature available regarding the financial industry.

5.12.2 Literature delimitation is defined by a non-technical focus although some technical aspects might be discussed. This research also undertakes an exploration through the nature of qualitative lenses of academics, practitioners and regulators. When undertaking the research, a mono methodology was selected. The nature of the research remains qualitative, hence the investigation focusing on exploratory dynamics and explanations for a phenomenon.

5.13 Ethical considerations

Having taken into account ethical concerns, the first phase of this research begins with reviewing the literature, where the research embraced transparent methods by paying proper attention to other research work in order to avoid possible plagiarism (e.g. note taking, source citation, source attribution) (Bloomberg and Volpe, 2015). Similar approaches apply to the second phase of this research (Systematic literature review), where similar considerations are applied.

For the third phase, which implies participants in research, an ethics approval from the university was mandatory. As soon as the procedure were established, the Researcher required authorisation from Brunel University Research Ethics Committee (UREC) to verify research adherence to respectable ethical practice, in accordance with the university's expectation for research ethics (Rudestam and Newton, 2014).

Additionally, it is worthy of mention that the financial nature of research is independent and self-funded. Accordingly, the research position is neutral about respondents and organisations under investigation. Furthermore, prior to the interview, all respondents

received the research documentation to ensure that their confidentiality and anonymity represents a significant aspect. Besides, the data gathered from respondents was provided on a voluntary basis and not based on constraints; informed consent is advisable along with a complimentary copy of written consent handed to participants in pursuit of reliable and ethical practice (Rudestam and Newton, 2014). In this way, Quinland *et al.* (2015) articulate that written consent can leverage a precise understanding and trust-building effect with participants because it provides confirmatory evidence that their ethical rights are carefully considered.

In the same way, Oliver (2014) emphasises that written consent would assure and confirm that the participants have been informed both verbally and in writing about standard information regarding the research. That is why all procedures (written, verbal, and recorded consent), the nature of research, methods, participant role, and risk exposure must be clearly explained before questioning commences. Moreover, the participant should be informed about potential risks (if any), benefits, time commitment, interview procedures, location, and if any incentives exist for participation (Rudestam and Newton, 2014).

Consequently, addressing ethical issues is undeniably a sensitive aspect of any research. Therefore, the content of the questions are general with no personal aspects or psychological aspects that might cause distress to respondents. In addition, the format of questioning avoids requesting information that can reveal sensitive information about their organisation. This means that questions are written in a professional format with the intention to respect confidentiality and anonymity aspects of both respondents and their organisations as discussed in advance.

5.13.1 Anonymity and confidentiality

Anonymity refers to personal information (i.e. identity or any details that might lead to individual identification) or precise information (e.g. location or other possible links) and this research aims to preserve and anonymise the participants (Cottrell and McKenzie, 2010; Fisher, 2010), who are only known by the Researcher (Rudestam and Newton, 2014). Thus, the Researcher takes the responsibility to ensure that personal information collected is organised under codified names/pseudonyms, or numbers.

When comparing aspects of anonymity with confidentiality, they tend to be interrelated by aspects of secrecy but are nonetheless different because anonymity refers to the concealed source of identity, whereas confidentiality relates to secure handling of information which

ensures that data gathered is used for the purpose stated and is stored securely (use of passwords, encryption, limited access, etc.) (Cottrell and McKenzie, 2010; O'Hara *et al*., 2011; Rudestam and Newton, 2014; Harding, 2013).

For this reason, anonymity and confidentiality in conducting the research should be continuously preserved and guaranteed to respondents as they represent a 'promise' that contributes towards the respondent's decision to participate (O'Hara *et al.,* 2011). Therefore, all procedures, methods, and risks were explained to participants beforehand in order to ensure transparent and unbiased results. Accordingly, based on proposed methods, the veracity of data collected ensures reliable research as ethical conditions are taken into account.

5.13.2 Research sensitivity/level of intrusiveness

The research may involve examining issues related to risk governance that could be sensitive to company management due to secrecy aspects. In this case, the participant will be assured that the research focuses on general aspects and all information will be used only for promoting good practices. Moreover, this information will be provided in writing and verbally to each participant. If the participant considers that the information requested is sensitive, the participant is free not to answer. Additionally, the interview will take place based on access granted through a letter of permission, addressed in advance to the organisation's management.

Moreover, under no circumstances did the Researcher request confidential information at any point as the interview addresses general questions that inquire personal opinion, experience, behaviour, and attitudes regarding elicit current industry practices. Participation was made on a voluntary basis, and all participants were able to cease their participation at any point in time. The Researcher acknowledged that some respondents might believe that current research might be interested in risk governance issues that could be sensitive to company management due to secrecy aspects. In this case, the participants were assured that the research is focused on general aspects and all information will be used only for promoting good practices. Moreover, this information was provided in both writing and verbally to each participant. If the participant considered that the information requested is sensitive, the participant was free not to answer.

Additionally, the interview took place based on access granted through a letter of permission addressed in advance to the organisation management. The participants were provided with the Researcher's contact details should they request further information or wish to make a complaint. The Researcher did not request confidential information at any point as the interview addresses general questions that inquire personal opinion, experience, behaviour, and attitude to elicit the current industry practices.

Having understood the responsibilities regarding the sensitivity of data protection, the Researcher adheres to Data Protection Act of 1998. Accordingly, the data shall be "used fairly and lawfully", "specifically for stated purposes", in an accurate manner, and "kept for no longer than is absolutely necessary". Additionally, the Researcher assures non-transferability of data to other parties and assures to encrypt data and to store it in a secure environment (Data Protection Act, 1998). Moreover, the research aims to respect the principle of ethics, therefore, to present results in an honest manner, avoiding any misinterpretations (Maylor and Blackmon, 2005).

5.14 Conclusion

In structuring this chapter, reflections for explanation and justification of methodological choices such as research purpose, philosophy, approach, strategy, methods, and techniques have been considered. Their selection was based on how appropriate they were for the research problem and research questions. This chapter justifies the exploratory research purpose based on the interpretive philosophy that underpins enhanced findings, the collection of data, analysis, and interpretation. An inductive approach has been selected due to its suitability for the research problem. The research strategy chosen is qualitative because it focuses on understanding specific situations (Silverman, 2014). The research design uses a mono research method to correlate qualitatively to enhance the explorative prospect of findings.

Henceforth, qualitative methods have been selected to explore different perspectives and offer an argument that explains and illustrates the findings, enhancing varied and sustainable outcomes through various responses, adopting a sequential research construction. Additionally, the findings of the Literature Review (Chapter Two) and Systematic Literature Evaluation (Chapter Three) formed the baseline for gathering empirical data. All three stages were selected with the purpose to support and complement the achievement of research aims.

This chapter concludes with a consideration of data collection reliability, rigourisity, limitations, and ethics in order to highlight the Researcher's acknowledgement of academic quality. Additionally, this chapter acts as a comprehensive guide regarding previous chapters but also as a basis for building the following chapter (Chapter Six, Collection and analysis of primary data), which conveys a real-world perspective.

6. Chapter Six: Collection and Analysis of Primary Data

6.1 Introduction

In this chapter, the research methodology guidance is used to address the research objectives and determine the extent of fulfilment. It introduces the research findings from the interviews and aims to contextualise the validity for the *CsM-ERM Strategic Alignment Framework*. In seeking to investigate the effectiveness and sustainability of CsM and ERM alignment in the financial industry, it employs a qualitative content analysis of research findings directed by the research objectives 1-4:

- Research Objective 1: To identify, analyse and critically evaluate academic, industry-based and regulatory literature regarding ERM, CsM and their alignment and explore the current state of the topic.
- Research Objective 2: To analyse the financial industry's environment and current practices regarding alignment.
- Research Objective 3: To review and evaluate the effectiveness of current CsM and ERM frameworks.
- Research Objective 4: To evaluate the potential and limitations of CsM with ERM alignment within the financial industry, supported by practical guidance.

Although content analysis leads to descriptive findings, the main research findings will be fed into a further phase of interpretation in Chapter Seven. This chapter represents a first phase, a derivate that determines the ground of the interpretive phase ─ thematic analysis.

6.2 Data analysis

To provide systematic retrieval of findings in this phase of research, a content analysis was employed to describe 'trends', 'patterns', 'frequencies', and 'relationships' among respondents' answers (Vaismoradi *et al.*, 2013). In this regard, qualitative content analysis categorises findings into *descriptive qualitative data* and in the same time into *descriptive quantitative* because it is quantifying the content analysis (Vaismoradi *et al*., 2013). During analysis the Researcher used NVivo 12 Pro, a qualitative data analysis software for processing and organising the data. As codes are labels that reduce the chance of repetition, minimising data (Ignatow and Mihalcea, 2017) was applied to all 26 semi-structured interviews in order to provide descriptive findings, indicating current practices within the financial industry as opposed to theory. To gain a practical insight into the phenomenon, the participants were selected based on their expertise. Most respondents were executives from

various financial institutions with either strategic or operational roles. Correspondingly, a balanced representation of senior executives was considered from both ERM and CsM managerial component, however there were many cases where an expert was familiar or responsible with both. Although the degree of balanced representation might be challenged, separation by coding delimitates research findings of initial analysis to ensure transparency and to delimitate the results. According to the codes identified, four themes emerged (as presented below):

1. Theme One: Respondent and Organisation Profile (Q1-Q9);
2. Theme Two: Enterprise Risk Oversight Maturity (Q10-Q16);
3. Theme Three: Cyber Risk Oversight Maturity (Q17-Q24);
4. Theme Four: Strategic Alignment (Q25-Q39).

In keeping this format, the same approach was applied before uploading the transcripts in NVivo, creating codes and sub-codes accordingly. This method was chosen to ensure that initial automatic coding (nodes) was sustainable across the analysis. From a total of 39 questions, 23 were semi-structured, and the remaining 16 were open questions that aimed to identify new research insights. Nevertheless, to ensure objectivity of the semi-structured questions, the format of questions offered an option for different/optional answers in alignment with the respondent's own views. These options for responses (open questions and semi-structured) were addressed this way to ensure a starting discussion point and illustration of comprehensive understanding of various interpretations of the phenomenon. Bazeley (2007) defines this process as a way of obtaining initial information to determine the nature of a problem.

Ensuing the above, the data analysis comprises the below themes.

6.2.1 Theme One: Respondents and Organisation Profile

To select the respondents four main criteria were used: financial industry focused, size of the organisation, seniority (in terms of their role with the organisation), and role-related to risk oversight. Based on the initial criteria, some respondents were identified and invited based on the professional network of the Researcher. Later on, due to recommendations of the initial respondents', other respondents joined and contributed (snowball sampling). This led to a number of 26 interviews with more than 18 hours of recording and above 80,000 words to be analysed. Table below gives an overall overview of respondents' codes, interviews duration and settings.

Table 6-1 Interviews particulars

No.	Respondent code	Duration	Words	Interview setting
1.	Respondent [1]	34:44	3087	In person
2.	Respondent [2]	53:76	1184	Call
3.	Respondent [3]	44:56	2785	Call
4.	Respondent [4]	47:53	4052	In person
5.	Respondent [5]	53.26	2634	Call
6.	Respondent [6]	49.25	3374	In person
7.	Respondent [7]	20.01	1912	Call and email
8.	Respondent [8]	44:10	2963	Call
9.	Respondent [9]	38:48	2963	Call
10.	Respondent [10]	58:07	3508	Call
11.	Respondent [11]	75:41	3924	Call
12.	Respondent [12]	58.65	2068	In person
13.	Respondent [13]	51:18	5027	Call
14.	Respondent [14]	37:42	3347	Call
15.	Respondent [15]	44:36	3292	Call
16.	Respondent [16]	26:38	2274	Call
17.	Respondent [17]	25:01	399	Call
18.	Respondent [18]	49:15	3716	Call
19.	Respondent [19]	45.03	3278	Call
20.	Respondent [20]	33:10	2154	In person
21.	Respondent [21]	37:56	4415	In person
22.	Respondent [22]	14:42	670	Call
23.	Respondent [23]	44:44	3172	Call
24.	Respondent [24]	60.03	6842	In person
25.	Respondent [25]	31:42	2989	Call
26.	Respondent [26]	41:19	4811	Call
Total 26 interviews		Duration 1123:40 min [18 hours, 43 minutes, 40 seconds] 18:40:40	80400 words	7 face-to-face 19 calls

A key point of Table 6-1 is that interviews ranged from being face-to-face interviews to telephone-based interviews (7 face-to-face and 19 telephone interviews), which gave the Researcher a mixed overview. Although additional approaches were possible, the 80400 words content allowed a thoughtful overview of the research problem in practice. Furthermore, the following subsections discuss the respondents' profile in more detail.

6.2.1.1 Demographic data (Q1)

Addressing Question 1 (Q1) the results showed that respondents were from seven geographical areas. Respondents were predominantly UK-based (58%). However, it must be considered that in some cases, roles and responsibilities were acknowledged to extend beyond the main UK-based headquarters (expected in Subsection 6.2.1.4).

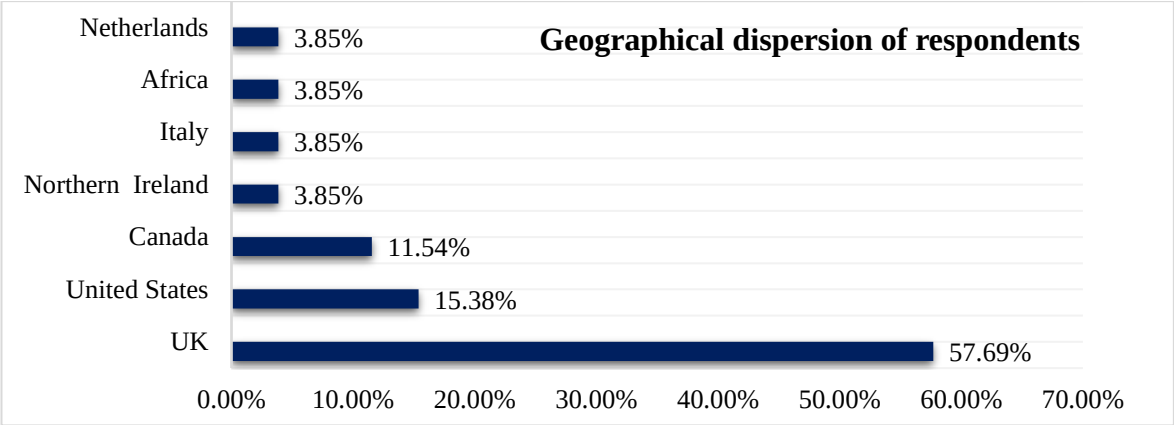


Figure 6-1 Respondents main geographical residence

As shown in Figure 6-1 the majority of respondents are UK-based, followed by Canada and the United States preponderance. However, this mainly represents headquarters affiliation, hence responsibilities of some circumvent geographical borders.

6.2.1.2 Organisation sector (Q2)

Aiming to understand in much detail the nature of the financial industry in which the respondents operate, Question 2 articulates that despite being part of the same financial industry, organisations have different activities, respectively different sectors, and thus various challenges and opportunities. Figure 6-2 (below) presents a depiction of results with three main types of institutions and two secondary subcategories, correspondingly:

- Depository institutions (e.g. retail bank, commercial bank, private bank, savings bank, building society, credit union);
- Insurance and pension fund institutions (e.g. insurance organisations);
- Brokers and investments institutions (e.g. asset management, investment banks, corporate finance, mutual funds, hedge funds, mortgage brokers, clearinghouses, finance organisations, and investment organisations);
- Depository and Brokers and Investment Institutions;
- Others.

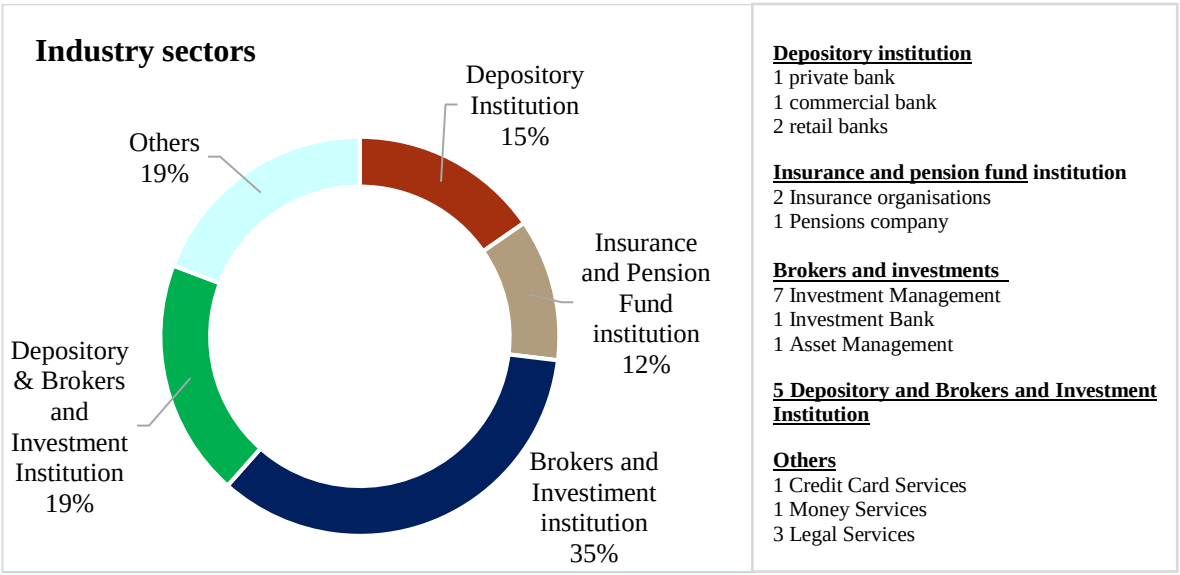


Figure 6-2 Financial industry dispersion per sectors

It has been identified that financial industry dispersion per sectors varies. For instance, brokers and investment institutions register the highest domain of activities with 35%. However, this percentage is higher given the mix of a depository institutions with brokers institutions (19%), which were treated as a different type of organisation due to their dual-characteristics. This overview of industry dispersion helps one to understand the diversity of respondents' affiliation, and thus implications.

6.2.1.3 Organisation size (Q3)

Organisation size of participants is another aspect to consider when receiving views. Consequently, measuring a company involves paying attention to many other characteristics such as assets, revenue turnover, annual growth, profitability, among many other features (Dang, Li and Yang, 2018). If we refer to some respondents that are part of broker and investment institutions with large global footprints, the size might be irrelevant, hence its size can be defined by other means, e.g. revenue turnover. In short, it should be considered that the number of employees reported by respondents is mainly for informative purposes, indicating that respondents are part of an organisation large enough to consider investing in risk oversight.

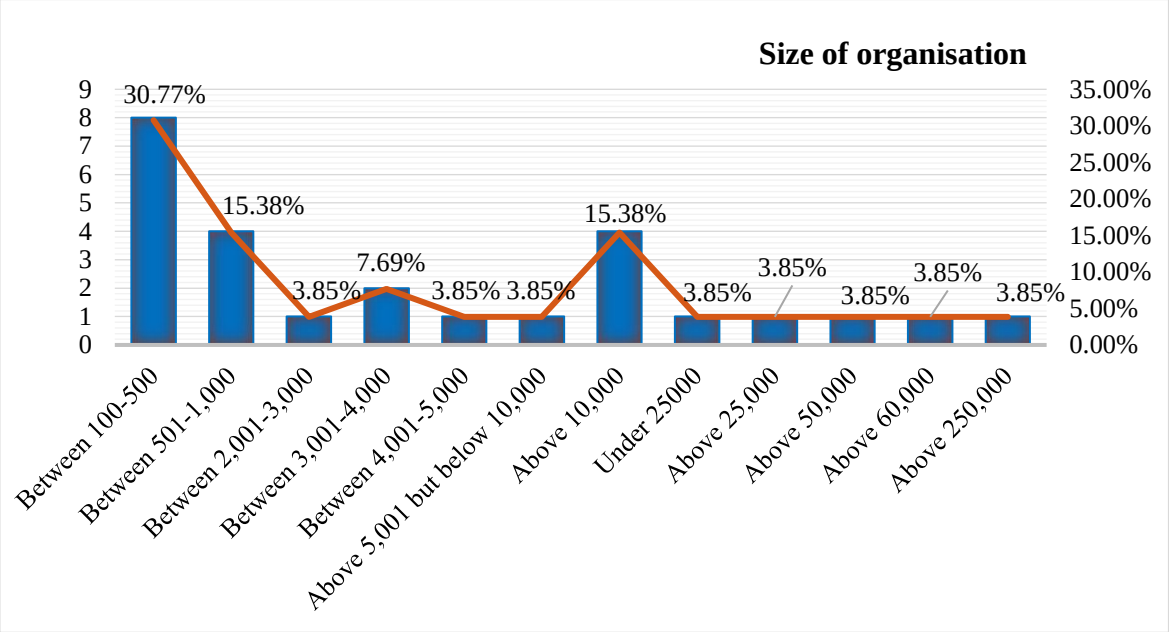


Figure 6-3 Size of sampled organisations

Table 6-3 shows that the sampled organisations' size varied and thus only four categories scored higher percentages. The category of organisations was between 100 and 500 employees (30.77%) with 8 out of 26 respondents. The second group of organisations scored a significant percentage, 15.38%, and the organisations were made up of 501 and 1000 employees. Equally, the third category saw above 10,000 employees (15.38%), followed by a fourth category that had between 3001 and 4000 employees with 7.69%.

To conclude, Figure 6-3 shows a breakdown of main categories and also a breakdown of remaining categories. These results demonstrate that the sample chosen comprises both small and medium enterprise as well as large organisations. However, as discussed previously, given the nature of some financial organisations' business model, the number of employees may not necessarily reflect a realistic size of an organisation.

6.2.1.4 Respondent's roles (Q4)

Seeking to assess the respondent's accountability and implications of responsibilities, this question 4 was considered. However, given the nature of CsM and ERM disciplines intersection, a clear separation of Respondent's roles was unfeasible because roles intertwined in some aspects of strategic or operational capabilities. This relates to literature the mentions duplication or intertwined fields.

Table 6-2 Interviewees' roles within the organisation

Interviewees' roles	No.	Business Unit-related
Chief Information Security Officer (CISO)	4	CsM
Chief Revenue Officer	1	Business
Director for Information Security	1	CsM
Director within ERM	1	ERM
Global Head of Information Security Risk and Compliance	1	CsM
Group Head of Strategic Initiatives	1	CsM-ERM
Head of Corporate Services	1	Business
Head of Cyber and Technology Risk	1	CsM
Head of Cyber Insurance and Oversight	1	CsM
Head of Risk	2	ERM
Head of Security and Information Assurance	1	CsM
Information Security Officer and Operation Risk Strategic Lead	1	CsM -ERM
IT Controls Manager	1	CsM
Operational Risk Information Security Officer	1	CsM
Operational Risk Manager	1	ERM
Policing Governance Manager	1	Business-ERM
Principal Cyber Security Engineer	1	CsM
Senior Audit Specialist	1	Business-ERM
Senior Manager	1	Business
Senior Manager of Cyber Risk	1	CsM
Senior Operational Risk Manager	1	ERM
Vice President Security Architecture	1	CsM

Table 6-2 provides an overview of respondents' roles (even though provisional and demarcated through the lenses of CsM and ERM job-relation), registering 14 respondents as having CsM related roles (53%), 5 respondents (19.23%) with ERM related roles, 2 respondents (7.69%) with both business and ERM related roles , 2 respondents (7.69%) with both CsM and ERM related roles, and lastly 3 respondents (11.54%) with other business-related roles. Noticing possible misunderstanding of respondent roles and responsibilities, Question 5 extends analyses this issue.

6.2.1.5 Respondents responsibilities (Q5)

While previous questions investigated the terminology and/or role label, this question seeks an understanding of the respondents' accountability regarding risk oversight. Such analysis seeks to highlight practical experience whilst also delimiting the expertise and grounds of shared practices. Granted that the selection process of respondents was made on rigorous criteria, these findings add additional legitimacy for respondents' views. With a total of 48-word selection frequency elicited in defining roles, the majority of those who responded to this question felt that they have dual or triple roles, focusing on various aspects of risk governance.

Table 6-3 Respondents responsibilities

	Focus	Word frequency	Relative frequency
Initial practice attributes allocated by Researcher	Audit	4	8%
	Compliance	4	8%
	Education/awareness/training	3	6%
	Enterprise-wide risk control	7	15%
	Implementation – operational	4	8%
	Implementation – strategic	7	15%
	Risk control	11	23%
	Risk assessment/measurement	8	17%
	Total	**48**	**100%**

As shown in Table 6-3, respondents reported a focus on *risk control* (23%), *risk assessment/measurement* (17%), *enterprise-wide risk control* (15%), and, in some cases, implementation – *strategic* (15%). To acknowledge these variations in terms of roles and responsibilities, a statement by Respondent [13] is outlined:

> "I'm really focused on enterprise risk controls. From my perspective, I'm focused on governance and overseeing risks across my organisation, making sure that we have the right controls in place and that we're getting the right measurement and assessments for risks."

Even Respondent [18] subscribed to that idea that responsibilities within an are complex:

> "As a director, I'm mainly responsible for overseeing the overall information security programme. From a governance, risk and program development perspective, I'm ultimately responsible for the overall enterprise information security of the bank."

Likewise, Respondent [24] stresses a similar view:

> "So, I look after strategy and strategic initiatives for the group. [I'm the] Group Head of Strategic Initiatives. The role title does not necessarily reflect what I do, so, I actually have three roles. So [for] strategic initiatives, [I] also serve as adviser between groups and I effectively go around trying to fix things wherever may pop up, so [it's] bit of a multi-faceted role."

6.3.1.6 Respondents amount of experience in current role (Q6)

To further ascertain rigours and legitimate validity of respondent's opinions, Question 6 extracted the timeline with current organisations. The outcome is illustrated in Figure 6-4 below.

Figure 6-4 Respondents years' experience

The analysis of Respondents experience identified that a vast majority of respondents had been in their given role for fewer than five years (36.62% under 1 year, 19.26% at least 1 year but fewer than 5 years, 34.62% at least 3 years but fewer than 5 years), cumulating a total of 88.47%. In short, only 11.54% of respondents had been in the given role more than 5 years.

6.2.1.7 Respondents total amount of experience in similar roles (Q7)

Although Question 6 grouped respondents' experience with their current organisation, respondents were further challenged to disclose similar experience in order to draw the final conclusion regarding seniority in terms of dealing with risk oversight. As such, initial analysis might represent only a partial interpretation. Such differences are shown below in Figure 6-5.

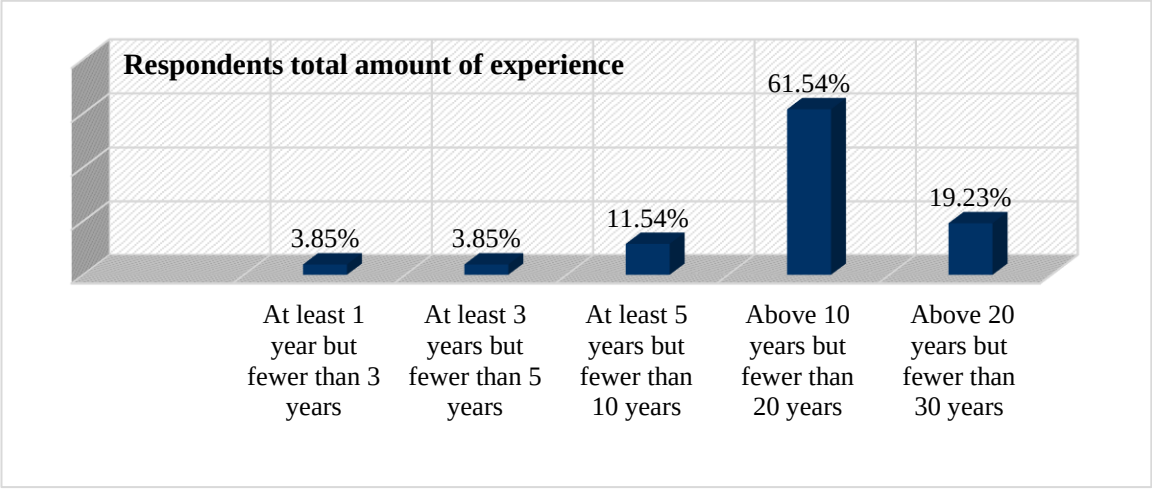


Figure 6-5 Respondents total years of experience

From the data in Figure 6-5, it is apparent that the length of time determines that 61.54% of respondents have more than 10 years' experience but fewer than 20 years. Less than 20% of

respondents served for a longer period of time. The results of this background examination probe that respondents have experience and expertise with designated responsibilities.

6.2.1.8 Respondents professional credentials (Q8)

As a continuation of confirming respondents' credentials, respondents were asked if their current role is conditioned by specific industry professional certifications. At the same time, the question deemed to identify and understand key suggested 'literacy' for both ERM an CsM. Figure 6-6 below elicits a breakdown regarding organisations' pressure for certifications.

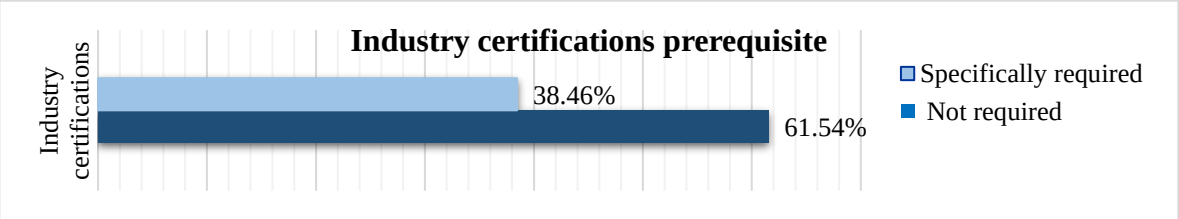


Figure 6-6 Industry certification prerequisite

Given the abundance of industry-based certifications related to risk oversight (RM, IS), it is believed that adherence to a certification baseline positively enhances a candidate and validates suitability for a certain position (Pym, 2014). In the light of reported views, it is conceivable that certifications are not mandatory (not required 61.54%).

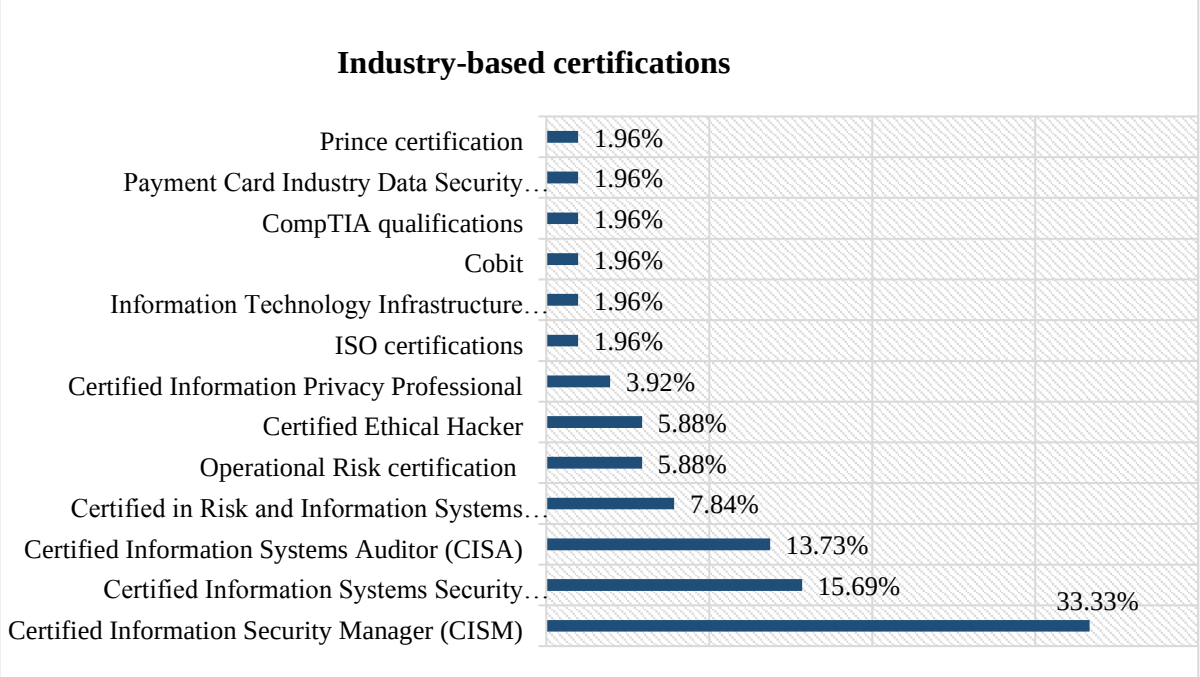


Figure 6-7 Industry-based certifications

Figure 6-7 emphasises the industry's certifications undertaken by respondents. Findings illustrated in Figure 6-7 have challenged some of the conclusions drawn in previous questions, arguing that the prerequisite of certifications is indirectly mandated. While voluntarily and *not specifically required* (as stated by 61.54% of respondents), the general agreement was that certifications are 'recommended'. Respondent [9] noted that: "[it] definitely is recommended but not required". Supporting this view, Respondent [19] sustained the same argument when, saying that while not officially required, organisations elect a set of requirements internally. Within these lines, it was clarified by Respondent [11] that:

> "Generally, what happens, although [it] is not ultimately required with all of us working in enterprise, and one of the conditions of employment, [is that] we have to get certifications."

It is interesting to note the view of Respondent [13], which reconfirms the certification paradox. Respondent [13] does not have a certification, however it delegates such expectations as a pre-requisite of employment:

> "Our goal is to make sure that we find people who do hire the right people, and that we've got the right framework."

Respondent [24] believes that one possible reason for a growing interest in industry-based certification utilisation is the creation of a risk resilience baseline that, among many other things, develops a common language. Although not regulatory mandated as stated by Respondent [4], it seems indirectly mandated by industry practices (e.g. ISO 27001 certification for organisations). Thus, Respondent [5] and Respondent [26] state that organisations prefer those sorts of certifications and they do encourage and facilitate training to gain the qualifications. Overall, this section originated from the assumption of strategic leadership theory, which suggests that organisational effectiveness represents a reflection of senior executives' competencies (Zhao, 2018).

6.2.1.9 Respondents interaction with risk governance (Q9)

Following an assessment of experience and expertise, Question 9 essentially defines the respondent's interaction with risk governance within the given organisations. This position offers a holistic understanding of the respondents' accountability limitations and explores any potential outcome framed by designated roles and expressed views. To enable a synthesised view, the Three Lines of Defence Model's principles were accepted (Table 6-4).

Table 6-4 Roles categorisation in alignment with Three Lines of Defense Model

Roles categorisation in alignment with Three Lines of Defense Model					
1st Line of Defence		**2nd Line of Defence**		**3rd Line of defence**	
Internal controls measures		Risk management and control oversight		Audit	
Risk assessment	Respondent [9]	Risk management and control oversight	Respondent [3]	Audit	Respondent [6]
	Respondent [12]		Respondent [4]	*Relative frequency 3.85%*	
	Respondent [19]		Respondent [14]		
Risk control	Respondent [25]		Respondent [15]		
Risk mitigation	Respondent [10]		Respondent [16]		
Operational management			Respondent [23]		
Operational management	Respondent [7]	IT and Cyber Oversight			
	Respondent [8]		Respondent [2]		
	Respondent [21]		Respondent [5]		
	Respondent [26]		Respondent [17]		
Management control			Respondent [18]		
Management control	Respondent [1]		Respondent [22]		
	Respondent [11]	Compliance			
	Respondent [13]	Compliance	Respondent [20]		
	Respondent [24]	*Relative frequency of 46.15%*			
Relative frequency of 50.00%					

R=Respondent

Figure 6-8 Roles categorisation in alignment with Three Lines of Defense Model

As illustrated above in Figure 6-4, respondents' interaction with risk governance was categorised into three main themes, 1st line, 2nd line and 3rd line. The Three Lines of Defence Model was considered a guide for defining respondents' designated activities because of the multiple responsibilities mentioned. The Institute of Internal Auditors' Three Lines of Defence (3LoD) is a regulatory benchmark for operational risk governance specifically for banks. Consequently, the principles of (3LoD) are defined by the Basel Committee for Banking Supervision and systematic structure is significantly encouraged (Luburić, 2017). All three lines of defence interrelate and aim to support proper functioning by designating roles, functions, processes, and support structured coordination that endorse accountability (1st line), control and oversight (2nd line), and assurance (3rd line) (COSO, 2015). In short, the rationale of using the Three Lines of Defence Model was because many respondents made reference to it and also because it is a predictable practice for the financial industry.

6.2.2 Theme Two: Enterprise Risk Oversight Maturity

This section seeks to determine sampled organisation's maturity in order to evidence the rationale of research. To establish whether enterprise Risk Oversight is mature, seven questions were addressed (Q10 - Q16).

6.2.2.1 Organisation preparation against risks (Q10)

In addition to establishing respondents' credentials, Question 10 queries the preparation against risks of sampled organisations. Results clarify an organisation's position in terms of preparation against risks concluded by respondents. They emphasise how susceptible organisations are in terms of challenges regarding security preparedness. To this end, findings ensue security maturity in for main states: proactive, reactive, ready, and unprepared. Table 6-5 below shows the proportion of different categories.

Table 6-5 Current security maturity

Current security maturity							
Proactive		**Reactive**		**Ready**		**Unprepared**	
Respondent [7]		Respondent [1]		Respondent [2]		Respondent [5]	
Respondent [8]		Respondent [9]		Respondent [3]		Respondent [6]	
Respondent [11]		Respondent [10]		Respondent [4]		Respondent [18]	
Respondent [14]		Respondent [12]		Respondent [13]			
Respondent [16]		Respondent [17]		Respondent [15]			
Respondent [22]		Respondent [19]					
Respondent [24]		Respondent [20]					
Respondent [26]		Respondent [21]					
		Respondent [23]					
		Respondent [25]					
Total = 8		Total = 10		Total = 5		Total = 3	
keyword	**rf**	**keyword**	**rf**	**keyword**	**rf**	**keyword**	**rf**
strategy	6.79%	risk control	14.55%	compliance	5.57%	maturity	3.02%
governance	7.98%	standards	2.63%			silo	3.51%
oversight	5.39%	financial risks	5.65%				
management	19.50%	cautious	1.88%				
framework	7.19%	reputational risks	7.54%				
culture	4.86%	regulatory risk	14.55%				
appetite	3.94%						
Proactive relative frequency=55.65%		**Reactive** relative frequency=32.25%		**Ready** relative frequency=5.57%		**Unprepared** relative frequency=6.53	
rf=relative frequency							

Table 6-5 shows that on a maturity curve, security is achieved when proactive practices are implemented. Current security maturity was confirmed by 55.65%. 32.25% categorise organisation maturity as reactive (i.e., defensive), focusing on mitigating the risk rather than proactively preventing it. Another 5.57% of respondents indicated that they are prepared. However, unfortunately, it is unexpectedly difficult to categorise these answers due to a lack of information. This result is somewhat counterintuitive; hence only 6.53% declare themselves as unprepared. In the literature, there is evidence that organisations continue to struggle to align RM with strategy (AICPA, 2018). Such issues emerged argues preparedness

against risks, hence it is misleading to label organisations as proactive or reactive (e.g., Respondent [2], [4], [3], [13] and [15]). As well, Respondent [4] noted that:

> "Significant, we are very well prepared and that's been driven by our clients that expect all of their suppliers to have good risk management processes in place and good information security protection in place. So, the field has changed over the last few years and more and more clients, particularly financial services clients, are driving forward the requirements for their suppliers to have security in place."

Respondent [18] explicates that:

> "Honestly, it's quite a challenge in most industries. It should be better in financial industry, but I would still rate our quite low in terms of our maturity level. Risk management at enterprise level is one of the key five [strategies] identified by the board of directors."

In addition, Respondent [5] emphasises a paradox of preparedness:

> "Very well prepared because is a very process-oriented organisation because of the regulation. But from implementation point of view, a lot of improvement [is] needed. There are a lot of gaps that needs to be taken care of. This [preparedness] it's in early phase."

'Maturity' for some respondents means different things. For instance, Respondent [11] places value on maturity in perspective of culture and preparation against risk. Whereas Respondent [7] describes security maturity as a good level of cyber and technology risk of frameworks, processes and controls, speaking a common language, being driven by risk appetite, risk tolerances, and risk profiles. In this regard seven derivates were identified as being proactive: governance, oversight, management, framework, culture and appetite, and management (the latter reaching the highest value with 19.50%).

Some other respondents indirectly describe their approach as reactive (32.25%) when defending the organisation. A reactive risk control means that mitigation is deployed post-incident and is rarely planned. Although this practice may seem of concern, it remains usual practice for some organisations (Society of Actuaries, 2018). Respondents [1] and [10] believe that because financial and regulatory risks have been emphasised, risk control became reactive mainly to factors.

While the first category of respondents warns that organisations align to pressure, Respondents [9] and [25] assess security vulnerabilities, understanding how the system works and comprehending data flow, list of gaps or issues, and assignment. In this regard, Respondent [20] recognises that preparation for risk is not as good as reacting to the risks.

In addition, Respondents [21] and [23] suggest creating a contingency plan in addition to risk monitoring.

A further derivate of cautiousness was reported by Respondents [12] and [19], who subscribe to the school of thought that being cautious in business is imperative; hence banks being subjected to many regulations. Another perspective on being reactive is heightened by Respondent [17], who is concerned about reputation as a main issue in deploying mitigation. In conclusion, organisation preparation against risks varies between reactive and proactive. It may be assumed that principles of modern risk oversight have a tendency to be applied (e.g. CsM, ERM).

6.2.2.2 Velocity of risks/attacks encountered by organisations (Q11)

Formulating a link between risk exposure, capabilities, and risk appetite is the ultimate challenge to determine organisational safeguards in overtaking excessive risks. This aspect was shown previously in Table 2-2, Chapter Two. Correspondingly, previous studies have shown that risk appetite is an essential determinant in weighing up decisions for risk exposure because it ensures that risk remains within established boundaries (Manigent, 2011; Deloitte, 2014a; Protivity, 2012; PwC, 2015; COSO, 2016). Thus, in estimating risk exposure, risk appetite is trivial for recognising maximum acceptable risk (Oliver *et al.*, 2018; Oliver Wyman, 2018a). Consequently, risk appetite is a determinant in deploying risk oversight framework; thus, incorporating diverse roles (i.e. being a risk statement, a metric that set boundaries and lastly a 'warning indicator') (Oliver Wyman, 2018a).

Question 11 focuses on examining the scale of attacks encountered by organisations in order to understand levels and types of exposure; besides, it appraises if capacity to risk is within risk appetite. Insights drawn from examination are synthesised below (Figure 6-8).

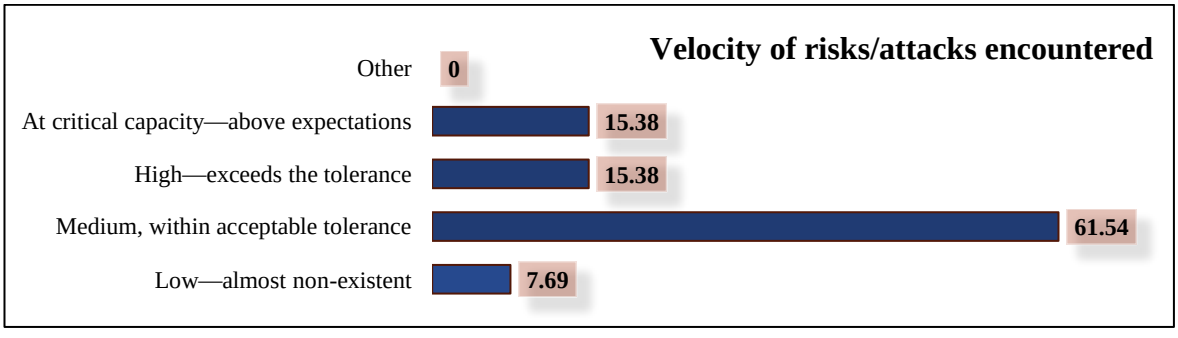


Figure 6-8 Velocity of risks/attacks encountered by organisations

Figure 6-8 illustrates that most respondents (61.54%) self-diagnosticated velocity of risk as medium, within acceptable tolerance. In addition, these results also show that both *exceeding*

tolerance (15.38%) and *above expectations* (15.38%) register similar results. 15 out of 26 respondents reported that risk is within acceptable tolerance and has not exceeded the agreed organisational risk tolerance.

However, Respondents [3], [8] and [9] envisage that risk exposure of the financial industry will continue to increase. Respondent [7] articulates that: "We are targeted, almost minute by minute on a daily basis." While Respondent [24] stresses that:

> "I think in terms of risk velocity, it's going up. That's the reality of it."

Despite control and measures in place, Respondents [10], [13], and [16] believe that financial institutions remain visible. Of more concern, Respondent [23] feels that attacks might be underreported:

> "I think that we have to distinguish [this] because, I would say, [it's] medium, but at the same time, when you think about cyber risk, all organisations are subject to a number of risks and sometimes, they don't even know they are the target[ed]. So, I think that from [a] conscious point of view, that it is not the reality. The reality is that the level of risk that we are facing every day is high, but we don't know."

When asked whether organisations are targeted, only 7.69% of the respondents reported that the velocity of risk encountered by their organisation is low. Respondents [2], [11] and [12] substantiate risk as non-existent. Respondent [12] clarifies that sensitivity in the market has increased and is, in turn, amplifying the velocity of risk. Also pertaining to high velocity, risk appetite became a parameter in systematically defining risks acceptability and allocating controls (PwC, 2018). The problem of dealing with risk systematically has also been emphasised by Bogodistov and Wohlgemuth (2017).

6.2.2.3 Managerial component/department responsible for enterprise risks (Q12)

Question 12 questions the names of departments that carry a duty of care/responsibility regarding enterprise risks. Owing to organisations possibly having various ways of defining risk oversight approach, respectively the department's name, respondents were challenged to express which unit/department is responsible for planning, organising, leading and controlling risk, respectively to minimise the effect of risks in a centralised, unified and systematic way; either physical risks, environmental risks, strategy risks, financial risks, intangible risk (cyber) or any other business-related risks. Descriptive data was generated for various variables, as described below (Figure 6-9).

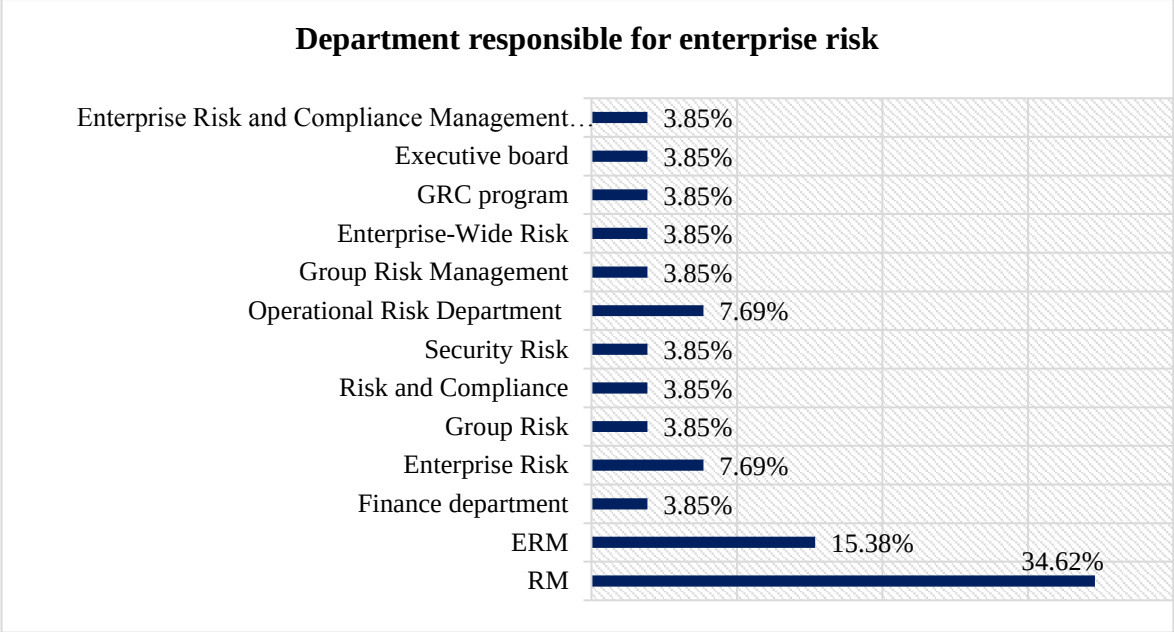


Figure 6-9 Department's responsible for enterprise risk

The themes identified in these responses show that RM remains among the most significant department name, as declared by 34.62% of respondents. A second theme that emerged is ERM, with a lower value of 15.38%, followed by Operational Risk Management (7.69%), and Enterprise risk (7.69%). Assuming department names reflect risk oversight principles, these variations among responses demonstrate and reiterate the ERM paradigm evolution; respectively the roadmap from reactive towards proactive approaches regarding risks. For instance, taking the example of a finance department, risk and compliance and operational risk management demonstrate the early origins of traditional/siloed RM, meaning that risk arises at a departmental level and are dealt with separately (Berry-Stölzle and Xu, 2016; Slagmulder and Devoldere, 2018); thus, characterised by a sided perspective. For example, Respondent [14] said: "You can call it two things, either risk management or operational and enterprise risk." This shows that the risk function has a tendency towards operation, reactive rather than strategic, and proactive. Respondent [21] added:

> "So, risk management, with the risk function… so… we have the risk officer, and under that, we have the risk management team, below that there's operational risk, credit risk, and market risk. However, we do not have an enterprise risk management."

When asked to describe the RM function, Respondent [5] stated:

> "It depends from company to company. In this company the usual RM has three different teams in broader perspective. One is like [a] finance team that do[es] RM from [a] financial perspective. And then [there] is a legal side; the legal team takes care on more like… how the risk is in theory (in terms of patent and intellectual

> property and those kinds of stuff). And then is a cybersecurity risk, pretty much from an infrastructure side of things."

Overall, these results indicate that ERM remains immature, with a lower value of 15.38%. This is in line with other research (Mensah and Gottwald, 2016; Viscelli *et al.*, 2017; Althonayan, Matin and Andronache, 2018) who indicated stagnation of ERM in a developmental stage. Only a few examples show that some other organisations are proactive and show openness in adopting the Governance Risk Management and Compliance (GRC) paradigm, which is suggested to be the next paradigm wave—an advancement of ERM (Althonayan, Matin and Andronache, 2018).

6.2.2.4 Risk governance maturity (Q13)

The central issue addressed here is how respondents describe the overall status of risk governance maturity (e.g. Risk Management, Enterprise Risk Management) in terms of their organisation protecting against its risks (on a scale of 1-5, 1 representing the low value on a level from 1 to 5). The results obtained are displayed below in Figure 6-10.

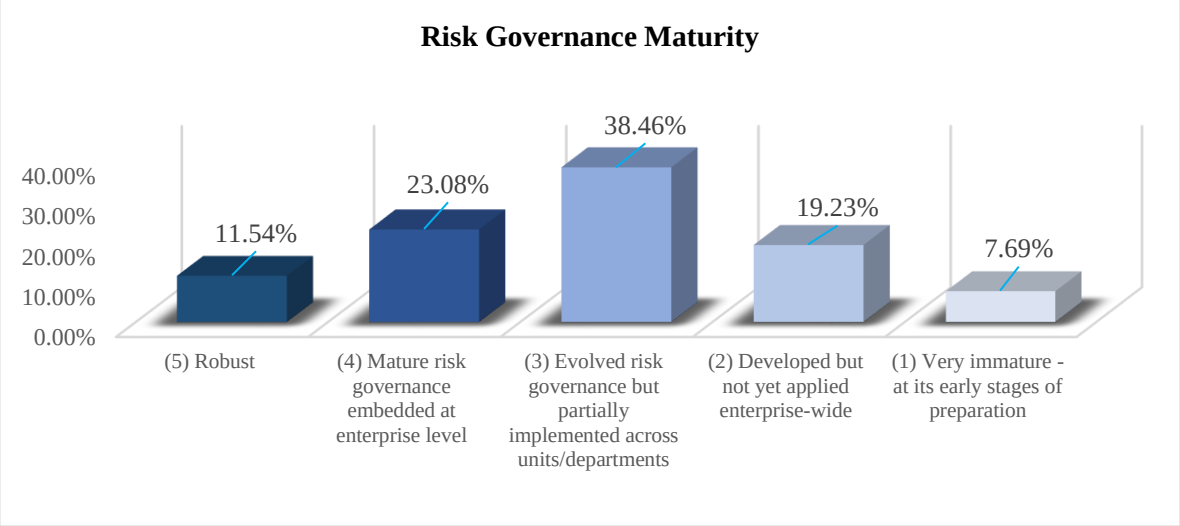


Figure 6-10 Risk governance maturity

As shown in Figure 6-10, 38.46% of respondents consider that risk governance is *evolved but partially implemented across units/departments* (3). 23.08% state that mature *risk governance[is] embedded at enterprise level* (4). 19.23% of respondents define maturity as *developed but not yet applied enterprise-wide* (2), whilst only 11.54% declared themselves to be *robust* (5).

Evolved risk governance yet partially implemented across units/departments was justified by Respondent [13]:

> "I think it's interesting, we look at it from a couple [view] of components. I think we look at it as a common governance tool [view] to make sure that we're understanding. It is a risk control function there's (no doubt that we're trying to identify, isolate the risks), and there is leverage as a governance tool. But in other areas, compliance requirement is also a key driver, making sure we are binding by whatever the regulations are in certain jurisdictions. So those three things are the drivers [common governance tool, risk control function and compliance requirement]."

In addition, Respondent [15] defends the scale of maturity by stating that:

> "I think it would be based on departments[maturity], certain departments are more organised than others, so I would… overall… I think… we are evolved at risk governance, but it's partially implemented, making it level 3."

7.69% are at *very immature - at its early stages of preparation* Respondent [21] argued:

> "I am going to be honest, [it is] very immature. So I was saying we are a bank that lives in the 21st century but operate in a pre-financial crisis at most. So executive management believe we only have to focus on making money, making the customer happy and [manage] financial risk, but not what the regulator is saying. We have to focus on the non-financial risk in terms of reputational, regulatory staff impact and customer impact. So, we have [a] journey to go on. The plan is always easy."

Within these lines, Respondent [6] further justifies that a lack of a framework in place for managing risks and measuring risks hinders maturity. Respondents [7], [8], [12], and [14] argue that the development of maturity stems from the framework, policies and standards, conduct and culture (institutional and contingency). In summary, this review demonstrates that risk governance maturity is yet to achieve its maximum potential. Appraising organisations' maturity reflects literature's comment on RM/ERM maturity frameworks (discussed in Subsection 4.3.1, Chapter Four).

6.2.2.5 Account of organisation risk governance (Q14)

ERM has established a strategic approach that incorporates a compound of existing strategies, resources, technology, and knowledge that leverage enhanced capabilities for evaluating and managing uncertainties (Hoffman, 2009; Burnaby and Hass, 2009). Moreover, the main purpose of ERM is to determine risk, to measure, to mitigate, and to proactively manage risks in order to meet organisational objectives (Francis and Richards, 2007; Hoffman, 2009). Literature suggests various definitions of ERM but, despite a significant contribution from scholars, a common agreement has not been reached (See Section 2.4, Chapter 2). In other words, having roots in RM paradigm hinders the potential of ERM. Nonetheless, there is evidence that the siloed practice of RM is being abandoned due to the regulatory pressure of the post-financial crisis of 2008 and general RM

inefficiency (Mensah and Gottwald, 2016; Althonayan, Matin and Andronache, 2018). The question remains whether the respondents adopted the traditional RM or advanced implementation of ERM. Therefore, to develop a deeper understanding of how risk governance is perceived by respondents, the below Table 6-6 synthesises the main findings.

Table 6-6 Components of organisation risk governance

Theme	Sub-theme	Sub-theme description	Sub-theme word frequency	Relative frequency
Strategic governance 45.16%	Governance	Common governance tool	11	17.74%
	Strategy	Supportive business strategy and objectives alignment tool	3	4.84%
	Prioritisation	Effective strategic prioritisation (operational efficiency) tool	14	22.58%
Performance-centric 11.28%	Differentiation	Competitive advantages advocate	3	4.84%
	Value	Value creation tool	3	6.44%
Risk resiliency 43.56%	Control	Risk control function	10	14.52%
	Compliance	Compliance requirement	9	14.52%
	Knowledge	Cross-domain risk knowledge	9	14.52%
3 Themes	Total=8 Sub-themes		Sub-themes frequency=70	Total =100%

Unfolding the role of organisational risk governance, the respondents' answers have been categorised into three main themes: strategic governance, performance-centric, and risk resiliency. Despite addressing the question to 26 respondents, the frequency of sub-themes was higher because some chose multiple options. *Effective strategic prioritisation* (22.58%) is the top constituent for organisational risk governance. Secondly, *common governance tool* (17.74%) reconfirms the construct of ERM, something that is in alignment with literature (see Section 3.5, Chapter 3). Thirdly, the respondents appreciate that ERM is a *value creation tool* (6.44%) and within these lines Respondent [2] reassures that:

> "Definitely [ERM is] a value creation tool because you need to know where to direct your resources, which areas, which issues to object first."

The above arguments are also indicated by Sax and Andersen (2018), who declare ERM an 'enhancement' tool for value and performance through systematic management of risks. Likewise, Respondent [24] said:

> "ERM is a central risk governance tool. It's the governance and management of risk across the organisation …that's the 'vehicle' that ERM is - that is the platform, and that is the language that everyone should be speaking. In an ideal world that would be what the ERM should be."

To another extent of risk resiliency, Respondent [11] considers that:

> "Enterprise Risk Management almost acts like a government regulator."

A view that is partially confirmed by Respondent [3]:

> "In most cases, it's a compliance requirement, it's a ticking box of Sarbanes-Oxley point of view, or it's a more general audit requirement to have, a risk function that extends into the security."

The findings suggests that compliance requirement has become an audit exercise for some organisations. Whilst this finding did not confirm the ethical accountability of reasons of why traditional RM emerged towards ERM, literature emphasises that instead of being an exercise, the Sarbanes Oxley Act makes executive management accountable and mandate RM principles on daily basis to ensure integrated practice and cross-functional resiliency (Kerstin, Simone and Nicole, 2014). Respondent [14] highlighted the potential usefulness of ERM by stating:

> "I think ultimately you've got to look at ERM as a set of processes that exist at all levels of the organisation to do a number of things. One is to give out risk from an enterprise perspective as in you break across silos and you think end to end, you also think more holistically about how risks are being managed tat an organisational level. So you take an aggregated view rather than looking at events in their isolation or any other individual events in isolation…[ERM] support business strategy and value creation."

For some respondents, the main focus is compliance due to the industry being highly regulated. Issues pertaining to banking in the past in the UK, regulation, and observation of regulation have gone up. Media impact and reputation have become a starting point for achieving compliance. The view of Respondent [8] is that succeeding compliance leads to competitive advantage, and so on.

Moving to strategic governance emphasis, Respondent [1] concluded that ERM's role is, among other things, to support business strategy alignment. Moreover, any mismatch may affect the business strategy and its objectives. Likewise, Respondents [13], [11], and [25] think that ERM is a risk control function with shared responsibility. The risk is co-owned by each business unit; for instance, wealth management and corporate banking own the risk but ERM will prescribe how they own it and how quickly they must mitigate and remediate that risk.

6.2.2.6 Main determining factors to implement risk governance (RM/ERM) (Q15)

Defined as 'critical success factors' (CSFs) by Olivera *et al.* (2018), the determining factors represent a baseline for understanding what is needed for achieving a successful

implementation of ERM and what is the basis of transformation. Then again, CSFs are dependent on variables such as people, processes, culture, leadership style, technology, and organisational strategy. It was also suggested by Althonayan, Matin and Andronache (2018) that the evolving risks landscape is another important variable to consider. Below, Table 6-7 provides a synopsis of the research findings.

Table 6-7 Critical success factors' in implementing ERM

Theme	Sub-theme	Sub-theme description	Frequency	Relative frequency
Internally 42.87%	Objectives	Corporate strategic objectives	2	2.86%
	Initiative	Organisation's own initiative	3	4.29%
	Strategy	Business strategy	1	1.43%
	Appetite	Risk appetite	3	4.29%
	Leadership	Senior management leadership	2	2.86%
	Lessons	Post-financial crisis lessons	4	5.71%
	Culture	Organisational risk oversight culture	6	8.57%
	Requirements	Shareholders' requirements	5	7.14%
	Oversight	Organisational risk oversight	2	2.86%
	Audit	External and internal audit expectations	2	2.86%
Externally 57.15%	Threats	Evolving threat environment; external factors	2	2.86%
	Expectations	Customers' expectations	5	7.14%
	Competition	Competition	7	10.00%
	Regulation	Regulatory requirements	21	30.00%
	Standards	Standards/Frameworks-driven	3	4.29%
	Reputation	Reputational impact	2	2.86%
2 Themes	Total=16 Sub-themes	8 new sub-themes (blue colour) 22.86% 8 initial sub-themes (black colour) 77.14%	Sub-themes frequency=70	Total =100%

From an initial 16 available options, 3 sub-themes were confirmed and another 2 identified as nil, hence the responses to these questions being non-existent. Sub-themes (a) *Consultancy organisations*, (b) *Insurance prerequisites*, (c) *Laws*, (d) *Organisational internal norms*, and (e) *Practitioners' recommendations* received zero answers. In turn, three of them ((c), (d) and (e)) were absorbed by related sub-themes due to the terminology similarities. For instance, sub-theme *Regulation* was preferred instead of *Law* (Respondent [11] confirms the confusion). A similar assumption can also be made in the case of *Practitioners' recommendations* shift in *Standards/Frameworks-driven* sub-theme, which covers a much broader spectrum of industry expectations and guidelines. Instead, *insurance prerequisites* and *consultancy organisations* do not seem to be factors that impact implementation of a risk governance and thus are overall nil.

The most striking result to emerge from the data is the identification of new determinants/drivers on which an organisation decides to implement a risk governance (RM/ERM). Despite being identified in literature (see Section 2.8, Chapter 2), the new determinants were not included in the interview format. However, they came to light through respondents' answers as proof that aligns with previous literature.

The evidence presented has shown that 8 out of 16 sub-themes are emerging issues reported by respondents (blue colour). The sub-themes of *objective*s (2.86%), *strategy* (1.43%), *appetite* (4.29%), *leadership* (2.86%), o*versight* (2.86%), *audit* (2.86%), *threats* (2.86%), and *reputation* (2.86%) recurred throughout the analysis. New sub-themes were not particularly prominent in the interview data. However, as a compound they represent 22.86% of the main factors. Additionally, some respondents indicated other determinants: profile of the organisation (Respondent [26]), fear of loss (Respondent [3]), the duty of care (Respondent [4]), internal policy (Respondent [9], and risk oversight structure (Respondent [23]).

Following the example by Olivera *et al.* (2018) that exemplifies the ten main success factors in implementing ERM, the Researcher chose to emphasise only the top 5 factors being conditioned by the low relative frequency of sub-themes:

- Regulatory requirements (30.00%);
- Competition (10.00%);
- Organisational risk oversight culture (8.57%);
- Shareholders' requirements (7.14%);
- Customer expectations (7.14%).

It has been found that regulatory requirement is the most significant factor and one strength of this is emphasised below by Respondent [24]:

> "[The] financial services sector is unfortunately (or fortunately even) under regulatory pressure. Regulatory pressure is always at the top of the list because, long and short of it, the regulators are the ones who probably have the most… the biggest stick to give away. They're the ones that are going to cause the most amount of pain financially - whether it is pulling your banking licence, or they give you a large fine because that cuts your profits and then the shareholders' profits… domino effect."

Likewise, Respondent [11] asserts that:

> "We are heavily scrutinised by government regulators (overall banking health, Ministry of Finance, Fin track…). That's probably the biggest driver, we want to be compliant with laws. That is our greatest determinant. I would link regulatory pressure with the law."

Despite the fact Respondent [25] prefers to simply argue compliance by stating that: "I think it's probably going to support our business strategy for what we do", these statements show that organisations discern good practice of risk oversight under the strict pressure of regulations. As an example, Respondent [14] shared similar views considering compliance an element of governance. However, there is literature which mentions compliance as a business decision rather than a driver. Furthermore, a second critical success factor was identified: competition (10.00%) that drives good practices. Respondent [18] describes competition as one of the biggest drivers hence the financial landscape is complex, and the market is dynamic. While compliance and competition are important, Respondent [23] re-orientates consideration towards the importance of meeting customer expectations:

> "I would say organisational risk oversight structure is important. Then, customer expectations, which links to standard framework; because if you are active in certain businesses, I think that having a risk management framework is… you know… the stuff that you have is standard…a necessary framework that can lift trust and reputation."

The ideal situation of a customer-centric approach reveals the necessity of multiple factors to drive ERM. Most often, they are interrelated (i.e. to meet expectations good standard practices need to be implemented). Subsequently, Respondent [24] emphasises a synopsis of the above view by articulating that:

> "One of the main ones [determinants] is customer expectations. Our clients are customers/counterparties who have a certain level of expectation that we maintain and manage. But if we substitute risk under the ERM to a level that is acceptable and the reason for that is very simple—[it] is: it's a chain effect, (we're not an island), so when institutions connect to another institution, to another, ripple effects can appear if you fail on something."

Despite the importance of external factors (compliance, understanding of competition, meeting customer expectations), there remains a paucity of evidence for internal factors. The only significant factors identified were the *shareholders' requirements* and *risk oversight culture*. These findings are not surprising given the fact that other research has shown significant consideration for the regulatory impact on implementing ERM. The evolution of ERM was discussed in Section 2.3, Chapter Two, and it explains why the financial industry received significant confirmation from industry and regulatory pressure to incorporate RM in organisational governance (Kerstin, Simone and Nicole, 2014). From this, it can be understood that it is reasonable to expect ERM robustness given the financial industry's past failure and potential ripple effects across the world's economy (Mikes, 2009).

However, despite a significant focus by respondents on aligning with regulations, Respondent [10] was among the few that advocates the importance of organisational objectives achievement as a scope of having the risk oversight. In short, ERM seems 'induced' by regulations, making practices mandatory and thus replacing an organisation's own initiative to adhere to risks practices (Sax and Andersen, 2018). This is an important issue for future research, hence good practices are significantly driven by regulations and less by the initiative of financial institutions to implement ERM. This aligns with Althonayan, Matin and Andronache (2018) regarding organisations' own willingness to implement and improve their risk oversight.

6.2.2.7 Main barriers that hinder a successful implementation of RM/ERM (Q16)

Question 15 demonstrated that despite onerous regulations and various barriers to implementing ERM, organisations have also registered positive effects post-implementation (see Section 2.4, Chapter 2). ERM is viewed as an integrative mechanism that drives a unified risk oversight that supports organisations to deal with a multidimensional spectrum of risks in a holistic way (Sax and Andersen, 2018). Despite its recognised value, ERM currently remains immature in terms of implementation, thus effecting an organisations' performance, viability and resiliency (Althonayan, Matin and Andronache, 2018; McShane, 2018). Consequently, understanding what hinders proper implementation is the first step to understanding what is required by ERM maturity (Mensah and Gottwald, 2016; Viscelli *et al*., 2017).

Despite the benefits, the interviews produced evidence which highlights that sampled organisations have different results in implementing ERM. Since each organisation is unique, its performance is correlated with all factors. As a result, the ability to adapt and optimise ERM continually creates a difference yet continues to remain a challenge for some organisations. Likewise, Althonayan, Matin and Andronache (2018) and McShane (2018) found that even though good practices are adopted, this does not mean that the best practices are generated. Barriers in implementing ERM hinder not only the implementation of ERM but also its maturity (Sweetening, 2011). Having considered initial findings of literature regarding barriers in implementing ERM (Section 2.4, Chapter Two), research findings confirm their validity.

Table 6-8 Inhibitors in implementing ERM

Theme	Sub-theme	Sub-theme description	Frequency	Relative frequency
Recourses 32.39%	Cost	Implied costs	5	7.04%
	Time	Implementation time	1	1.41%
	People	People availability	2	5.63%
	Skills	Skills set	4	5.63%
	Technology	Technology	3	4.23%
	Data	Data quality - incomplete info	5	7.04%
	Structure	Organisational structure	1	1.41%
Direction 9.86%	Strategy	Strategy	3	4.23%
	Leadership	Senior management support	4	5.63%
Capability 43.66%	Risk Assessment	Risk assessment and review	4	5.63%
	Prioritisation	Prioritisation and workload	4	5.63%
	Culture	Risk culture	6	8.45%
	Maturity	RM maturity function	7	9.86%
	Procedures	Procedures	1	1.41%
	Communication	Interorganisational Communication	2	2.82%
	Education	Lack of educational awareness	5	7.04%
	Accountability	Accountability-role delegation	2	2.82%
External pressure 16.90%	Risks and Threats	Emerging risks and their velocity	5	7.04%
	Practice	Standards and frameworks	4	5.63%
	Competition	Competition	1	1.41%
	Regulations	Regulatory demands	2	2.82%
4 Themes	21 Sub-themes		Sub-themes frequency=71	Total =100%

Table 6-8 illustrates lower values regarding inhibitors of ERM and discloses a potential association among inhibitors. Upon initial observation, it can be assumed that there are not any significant inhibitors to be considered. As previously identified in literature, the correlation between inhibitors as a compound demonstrates ripple effects and a broad spectrum of factors that can hinder ERM.

These findings broadly support the work of previous research in this area linking the value of understanding the benefits by way of thoughtful deliberation about what hinders ERM. As a result, it has been found that there are four main themes and 21 sub-themes that were significant for respondents. The low values of some sub-themes are impressive but not surprisingly so, hence them most often interrelating with each other. The highest values registered are an organisation's capability-related, respectively sub-theme *RM maturity* (9.86%) and *risk culture* (8.45%). Followed by *implied cost* (7.04%), *data quality* (7.04%)

—which refers to information regarding risks — *lack of education* with 7.04%, and lastly *emerging risks and their velocity* with a value of 7.04%.

RM maturity (9.86%) received the highest consideration from respondents. Respondents [12], [13], [14], [17], [20], [21], and [25] were among the ones that support the consensus idea of RM maturity. Risk culture (8.45%) is a multi-layered factor that demands both strategic and operational guidance. In this respect, Respondent [14] used the following argument:

> "There are a number, of possibly cultural issues. What I mean by that, I mean the actual risk management risk functions within organisation, sometimes they don't understand what the business need and want and therefore [are] not very usable in terms of getting to extract the benefits of risk. So, I'd say it's probably a cultural thing. The other thing is conflicting priorities. Everyone's got day jobs, and everyone is busy, [under] over-capacity and under-resourced, and to actually give proper risk management takes time, resource, and investment."

Respondent [23] exemplifies another side of culture that interrelates an organisation's vision and educational awareness, as well as skills and knowledge:

> "I think, one of the main inhibitors could also be the culture because … I will make an example…one of the components of an ERM system is the data loss collection tool, so you should log the events, risk events… However, sometimes employees are scared about notifying an error because they think that this would be used against them or in a negative way or affect their performance."

Investment in *skills and knowledge* of employees is a common factor mentioned in literature. Skills set (5.63%) is another inhibitor. According to Respondent [21], not having the skills set affects the understanding of what risk is and what is the purpose of it, and what is the value, affecting the deployment of a suitable solution. If the sub-themes of *risk culture* (8.45%), *skills set* (5.63%), and *lack of education* (7.04%) and *inter-organisational communication* (2.82%) were all absorbed, a total of 23.94% would be obtained and that percentage is in turn particularly **people-centric**. Rodriguez and Edwards (2010) conclude a similar remark. From this result, it can be assumed that 23.94% of ERM is rooted in people's capabilities. This association of four elements help to visualise, if quantified, the relationship and ripple effects. Capturing how the suitable solution to risk ought to be deployed, the results also exposed a surprising reference to *data quality* (7.04%) in ERM implementation. In fact, Respondent [10] asserts a practical view from their organisation:

> "I think that what might impede [ERM implementation] is not being aware of the risk. The biggest risk is not knowing what risk you have, identification and definition of risk and communicating [the risk]. Really, the first thing is to properly identify

> [the] risk. Emerging risk is part of the agenda, is standard. I think that accurate information is the key."

Additionally, Respondent [12] stated the relevance of having quality in data/information in combination with technology support and people, arguing that:

> "Quality of data, if [you] don't have good quality data, all the RM will not have a clear vision. That is the biggest to challenge …to get timely, granular and good quality data. Second is technology, if you don't have good risk systems, either in-house or bought from somebody else, you can't do much. Even if you have data, if you don't pass it through processor and risks engines, that doesn't help. [Also], you need to have people who understand that data. And finally, you need an internal acceptance of what RM can do. That can it deliver, buy-in?"

Consequently, using inaccurate, unreliable, or incomplete information may have top-down consequences in an organisation. Solutions may differ if risks are underestimated or overestimated (e.g. funds, mitigation, prioritisation, resource allocation, technology). For instance, a key component for organisations is understanding *emerging risks and their velocity*. Respondent [15] concludes that:

> "Risk is something that always happens in the future, it hasn't happened yet but knowing what could affect the future… making the business aware, so they can take risks by adjusting their decisions based on forecasted risks."

Predicting risks implies an appreciation of risk history which can help an organisation prioritise against major risk factors, except sporadic events (Allan *et al*., 2012). Apart from forecasting, risks quantifying shows a relative frequency of 7.04%. The main difference is detailed by Respondent [24]:

> "When you look at risk management, particularly in financial institutions, each risk is tied to a dollar sum, that dollar sum translates to something that will impact your capital reserves. It's very easy to say, hey there's going to be a denial service attack, how much is going to cost you? What is the actual loss of denial services? You have to estimate or 'guesstimate'."

Cost may also be considered a barrier when believe that the benefits of ERM controls are lesser than the invested cost (AICPA, 2018). Being able to qualify and quantify those risk types as pragmatic intangible is pivotal to good ERM. Likewise, Respondents [3] and [23] believe that it is difficult to place any quantifiable number either in terms of percentage probability or regarding impact into incidents and therefore being able to scale what annual loss expectancy. The downside is an underestimation of risk as stated by Respondent [3].

6.2.3 Theme Three: Cyber Risk Oversight Maturity

This theme comprises of seven questions centred on the identification of existing cyber risk oversight maturity. Since maturity is argued to be immature (see Subsection 4.4.1, Chapter 4) the following sections investigate the realism of the argument.

6.2.3.1 Main managerial component/department responsible for cyber risks (Q17)

Cybersecurity paradigm has advanced and so far, undergone numerous stages over the years, ensuing in a fragmented theoretical legacy (Althonayan and Andronache, 2018). Althonayan and this Researcher have expressed concerns about the effects of discrepancy in terminology and connotations; and more specifically how misperception may trigger continual misuse of terms, respectively ripple effects regarding comprehension of the meanings, purpose, and value of cybersecurity. A lack of standardisation in terminology and meanings leads to ambiguity (despite literature having some points in common). To date, there has been little discussion about cybersecurity. This is because it has been addressed in literature under numerous appellations (e.g. Information Security Management, Information Security Risk Management, IT Management, IT Governance, Information Computer Technology Security, Information Technology Governance, or Cyber Risk Management). This research question was proposed for transparency purposes in order to clarify under which category the sampled organisations abide. Differences between the above mentioned are illustrated below in Figure 6-11.

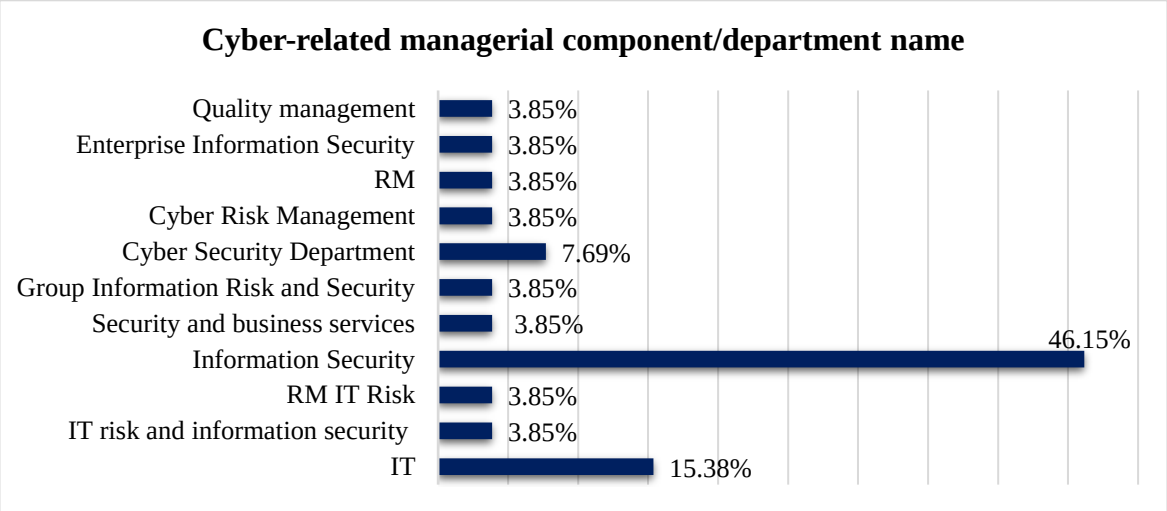


Figure 6-11 Variety of departmental names for cyber-related risk oversight

Evidence highlighted in Figure 6-11 indicates an initial assumption of fragmented meanings of cybersecurity. The analysis retrieved 11 categories that define or are related to the same component. This analysis is centered on exploring how organisations define their

departments, assuming that the name is related with the practice of risk oversight. Grounded in IS legacy, this finding demonstrates that 46.15% of organisations sampled remain grounded in an IS perspective and 15.38% was registered for IT. Notwithstanding, these delimitations of IS and IT evoke the cybersecurity roots. One of the strengths of these findings is, however, a predicted trend toward a cybersecurity paradigm. Taken together, the *Cyber Security Department* (7.69%) and *Cyber Risk Management* (3.85%) reach a total of 11.54%; thus, supporting the notion towards adopting cybersecurity terminology. Commenting on the ambiguity of cybersecurity meanings, Respondent [8] argues that:

> "The framework I work [is] under Information Security framework (where cybersecurity is an element of that). So, IS wise, [it] goes across the whole enterprise. Because that covers IT and normal activities. The cyber risk is very focused on web offering. There's information security, IT security and cybersecurity. And the cyber is the small one within the next one, with[in] the next one. The cybersecurity would be under IT security. Obviously, I report under IT. My area would be IT Security."

Interestingly, the above argument of Respondent [8] calls for clarity and supports the initial findings from Section 2.6, Chapter Two, which discusses the consequences of using a non-unified terminology for cybersecurity.

6.2.3.2 Main determining factors to implement CsM (Q18)

This section presents the rationale of implementing CsM by consensus of drivers. In line with Raban and Hauptman (2018), the determining factors reflect both positive and negative attributes. Cyberspace became the 5th element of human activities (the other four elements being land, sea, air, and space) in 2018, and as such opportunities and vulnerabilities are of serious consideration due not only to security but also economic implications (Amilevičius, 2012). Results show that from an initial 13 determinants suggested, two were nil (consultancy organisations, laws), with zero answers and another two were absorbed by other codes (i.e. *practitioners' recommendations* added to *Standards/frameworks driven; internal organisational norms* compiled with *risk oversight culture).*

Table 6-9 Main determinants in implementing CsM

Theme	Sub-theme	Sub-theme description	Frequency	Relative frequency
Internal pressure 40.81%	Initiative	Organisation own initiative	7	14.29%
	Appetite	Risk appetite for cyber	2	4.08%
	Culture	Risk oversight culture/internal norms	5	10.20%
	Awareness	Cyber awareness/education	3	6.12%
	Requirements	Senior management or shareholder requirement	3	6.12%
External pressure 59.18%	Threat	Cyber threats velocity and complexity	8	16.33%
	Regulation	Regulatory pressure	7	14.29%
	Technology	Technology advancement	3	6.12%
	Competition	Competition driven	3	6.12%
	Reputation	Reputation driven	2	4.08%
	Standards	Standards/frameworks driven	6	12.24%
2 Themes	11 Sub-themes		Sub-themes frequency=49	Total =100%

Consistent with literature, data analysis found that *cyber threats velocity and complexity* (16.33%) is among the highest determinant in implementing CsM; secondly, *organisation own initiative* (14.29%); thirdly, *regulatory pressure* (14.29%); fourthly, standards*/frameworks driven* (12.24%) and; fifthly, risk oversight culture (10.20%). In regard to main determinant factors to implement CsM, Respondent [15] assert that:

> "The biggest [challenge] one is the velocity and complexity of cyber threats. Keeping up with pressure is challenging and daunting but also technology enhancements. There's a lot of technology change that is happening within the company and each of those technology changes brings on their own share of cyber threats."

Respondent [5] sees a people-centric strategy as a main pillar, recommending an optimised training granting that:

> "You have to train the people on multiple layers. You know, it's not like you have one training, like phishing training and some sort of training that is very general training for computer security. For developers, you need to have secure development, secure-coding training. For other managers, they need to have a different training. So, training would be more versatile in cybersecurity."

Moving on from people-centric strategy, Respondent [10] adds another line of thought by stating that:

> "The things you do to mitigate people risks this year are very similar to the ones that we did 20 years ago. As the approach to cybersecurity is moving all the time, (the systems are changing; the Internet nature is changing), online trading means people can be in different jurisdictions."

In addition to having cyber resiliency and cyber awareness, Respondent [14] emphasises risk appetite for cyber because in the respondent's view, it is a key determinant for how much people, money, and technology is utilised. Supporting the view of Respondent [14], Respondent [4] articulates that making sure that risk appetite is accepted and understood enterprise-wide is a cornerstone in organisational culture.

The finding above demonstrates that what CsM represents varies among respondents. While five main determinants have been identified (threat, initiative, regulation, standards, and culture), some other respondents (such as Respondents [18] and [25]) argue that dependency/collaboration with a third party and clients demands certain elements of risk oversight to be in place and thus represents an additional element to be considered. Other responses to this question included factors such as mass media (Respondent [1]), risk governance (Respondent [16]), value creation/ business value (Respondent [2]), insurance pre-requisites (Respondent [25]), risk profile (Respondents [26]), and loss of money (Respondent [8]). Nonetheless, these issues were not particularly prominent in interview data.

6.2.3.3 Main barriers to hinder successful implementation of CsM (Q19)

As previously mentioned, cyber risk puts pressure on financial institutions. Owing to cyber exposure and the increased surface of attack (i.e. increased number of devices, increased number of users, variety of networks), financial institutions chose various strategies for dealing with risks. As there are problems in defining the discipline, accordingly inhibitors vary. Referred to as a *computerisation-informatisation-cyberisation paradigm shift* (Althonayan and Andronache, 2018), cybersecurity has become an integrative discipline that places information security under its umbrella. Despite a trend towards advancement of cyber resiliency, however, antecedents of the discipline remain and sustain fragmented practices ingrained on IT and IS. When challenging respondents to define the main inhibitors in implementing CsM, the below key inhibitors were identified.

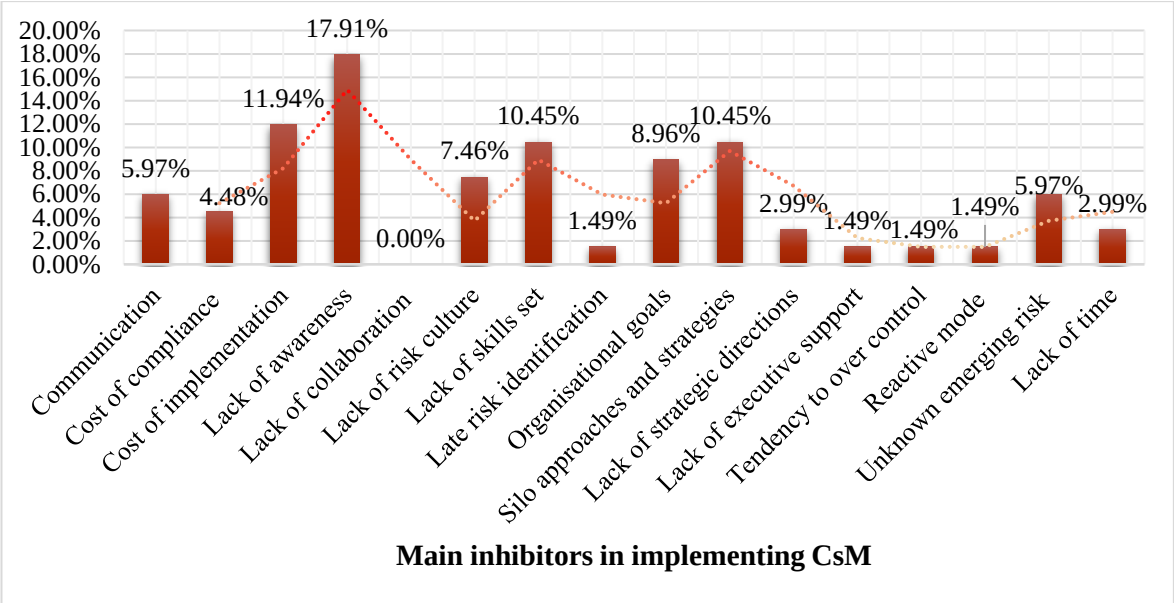


Figure 6-12 Main inhibitors in implementing CsM

Figure 6-12 shows an amalgamation of results, which at certain points connect and interrelate with each other. A number of six key criteria resulted in inhibiting CsM:

(1) **Awareness**, 17.91% of respondents agreed that a *lack of awareness* among employees is affecting deployment of implementation; Respondent [5] finds that:

> "Awareness, it's [a] critical thing here because even though people who know IT, they might know computers very well, but still they might not know a lot about cybersecurity a lot. So, there's a lot of awareness that is necessary."

Respondent [10] added that:

> "Not learning lessons from other people experiences and not staying up to date, I think those would a be two key inhibitors in my view."

This concluded that value of risk awareness and education is acknowledged by some as being a significant inhibitor for CsM.

(2) **Cost**, 11.94% agreed that *cost of implementation* impeded CsM proper implementation. When considering costs, Respondent [11] refers to the cost of strategies. Whilst Respondent [15] affirms that cost and quality of implementation is the biggest challenge:

> "I think the biggest challenge is the cost; the cost of implementation. And the other is quality. [If] you develop something that doesn't quite effectively meet the challenge, for example, you develop a new tool and that really is not effective to meet the challenge or the velocity or complexity demanded by the situation… that is one of key challenges.

Likewise, Respondent [20] reasons that costs of implementation for cybersecurity require lots of tools and lots of people who have experience and sufficient resources. Whilst Respondent [4] refers to cost for both implementation and cost of compliance, indicating that benefits are lesser than the cost.

(3) **Skills**, 10.45% of respondents believe that a *lack of employees' competencies* affects ERM. For instance, the view of Respondent [18] reasons that:

> "The biggest challenge is ourselves, including myself. Sometimes as a person, as a human, it's a very serious risk. Awareness is a big component of any type of risk. Particularly [in] cyber we fail a lot. It's a very dynamic and you know, [it's a] knowledge driven industry, [and] we don't have enough qualified resources internally in the region."

(4) **Silos**, 10.45% of respondents mention *silo approaches* and *silo strategies* (two initial sub-themes merged).

(5) **Misalignment**, 8.96% of respondents point towards *misalignment with organisational goals*;

(6) **Culture**, 7.46% of respondents blame *lack of enterprise-wide risk culture*.

In addition, a small number of respondents indicated that communication (5.97%), and the cost of compliance (4.48%) adds an additional burden for organisations. These findings indicate some of the problems encountered in the extant of literature research remain valid (See Section 4.4.1, Chapter 4). Little attention has been devoted to the impact of a *lack of strategic direction*, *weak support of management* (organisational dysfunctions), and *late risk identification.* Of much concern is that respondents disregarded a lack of collaboration. Perhaps contrary to expectations, collaboration is defined by respondents through lenses of silos (e.g. Respondent [1]).

An important issue that emerged from data was that respondents who reported low levels for some inhibitors also reported lower levels for four additional new categories that were omitted to be stated in the questionnaire:

- Tendency to over control (1.49%);
- Reactive mode (1.49%);
- Unknown emerging risk (5.97%);
- Lack of time (2.99%).

The majority of respondents disregarded time-constraint. Thus far, Respondents [8] and [9] believe that security cannot move fast enough, and often the expected speed is unlikely to reflect the capability of getting the right security.

From interviews with respondents, findings entail two streams: 1) six key inhibitors are significant in deployment of CsM implementation; 2) additional low value might be significant if all compounded together (e.g. lack of strategic direction (2.99%); weak support from management (1.49%), and tendency to over-control (1.49%)). All of the latter are strategically related.

6.2.3.4 Cyber incident handling (Q20)

With regard to departments/units and the practical side of risks, this question aims to appraise how an employee from any department would handle a cyber incident. In analysing the interview data, the significance of cyber awareness emerged as an important aspect in maintaining an organisation's resiliency. Henceforth a potential attack represents a risk of which organisations are aware. The security practice endorses a view that eventually any organisation will be targeted (Deloitte, n.d.; International Monetary Fund, 2017) and thus it is necessary to have a proactive strategy of preparedness or worst-case scenario, an efficient recovery. Regrettably, for the financial industry, most incidents end with financial losses (International Monetary Fund, 2017). Referring to a cyber incident as a predefined control the role of this question was to understand the maturity of control and enforcement of policies. Baskerville (2014) portrays incident handling through the lenses of the prevention paradigm (proactive) and response paradigm (reactive, defensive). The prevention paradigm assumes that risks are predictable, measurable, and persistent. In other words, predefined controls can be applied. However, when risks are unknown, it transposes into a response paradigm, which is a defensive control that is assumed to be 'unpredictable, non-measurable and transient' (Baskerville, 2014). Findings show that there is satisfactory data that recognises the human-element as an integrative part of cyber resiliency. This is in line with the initial findings of Subsection 4.4.4, Chapter and Subsection 6.2.3.2, Chapter Six.

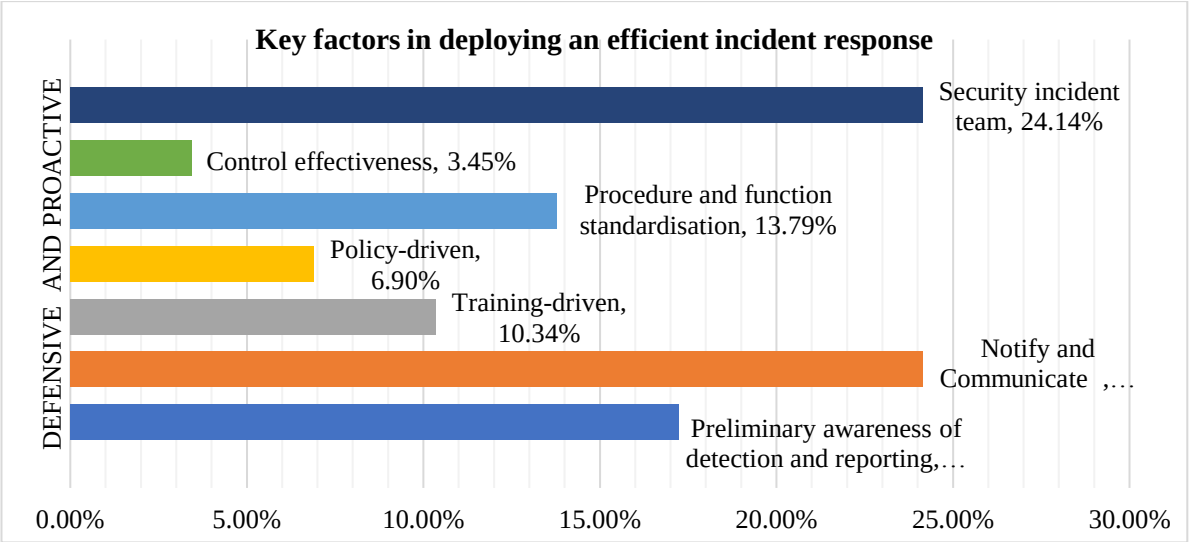


Figure 6-13 Cyber incident handling key aspects

The above findings suggest the respondent's views on what constitutes the key success factors in deploying good security practice is to have i) a security-incident team (24.14%), ii) a dedicated channel of communication (24.14%), and iii) preliminary awareness of detection and reporting (17.24%). In this regard, Respondent [2] stresses the importance of a defined team whilst Respondent [18] discusses preliminary awareness of detection and reporting by declaring that:

> "The biggest preparation tool is to have basic awareness to know what are the types of treats. We do a continuous employee awareness campaign to help prevent fishing and social attacks, and the first thing they need to do is to think twice before they do mitigation. And if there is anything suspicious, [they] usually call our IT help desk to guide them on what the next course of action needs to be. So that's another kind of practice we are trying to develop."

These comments provide evidence that awareness is important in practice, and secondly, that interconnectedness exists within organisational culture and its perception of security. When discussing awareness value, Respondent [24] stresses that:

> "We have a very solid awareness programme because for us, the employee is the first line of defence, so it's very much…if something happens, this is what you do, you tell someone, whether you think it looks stupid or your overreacting…you will never get in trouble for raising alarm, even if it's false alarm."

The notion of *notification and communication* of an incident (24.14%) is equal to having a *security incident team* (24.14%) and is described by Respondent [15], a principle to be followed by each employee. Accordingly, processes and procedures may vary depending on the type of incident, comments Respondent [20]. Confirming that culture plays a significant

role, Respondent [21] recommends the adoption of a "no-blame culture." This would involve employees being encouraged to indicate issues without facing potential disciplinary action afterwards. This recommendation by Respondent [21] pertains to the *training-driven* theme (10.34%) in building cyber resiliency capabilities. A related view is also supported by Respondent [16], who understands that regular training is a key control.

The results provide reasonable evidence that frequently most organisations have incident plans in place, owned either by the IT department or centralised cybersecurity team. Thus, there is an incident response plan that dictates the responses of individuals. In this regard, Respondent [5] recommends that procedure and function standardisation is imperative. Moreover, it reiterates the people-centric value and its educational and awareness preparedness in the process of cyber resilience and sets skill proficiency.

6.2.3.5 Side effects of poor cyber risk oversight (Q21)

Considering the broad spectrum of risks and cyber threats, respondents were asked what the most unwanted effects of poor risk oversight within their organisation are. This allows the Researcher to comprehend what they value more. Henceforth a side effect is considered when an action or lack of action has a partial or total impact on an organisation's objectives (Dobson *et al*., 2011); it can have direct or indirect effects regarding losses. Direct impact means that there has been a direct loss that can be quantified in monetary terms. Opposing this, the indirect side effects mean that effect is hard to be quantified or predicted (e.g. damage to reputation, trust, goodwill, source allocation, expenditure) Iyengar (2007). It represents an unanticipated loss that aims to cover the cost recovery of related operational capabilities (Yvengar, 2007). Figure 6-14 below illustrates the proportion of indirect and direct side effects of poor risk oversight, either in IT, IS, or CsM.

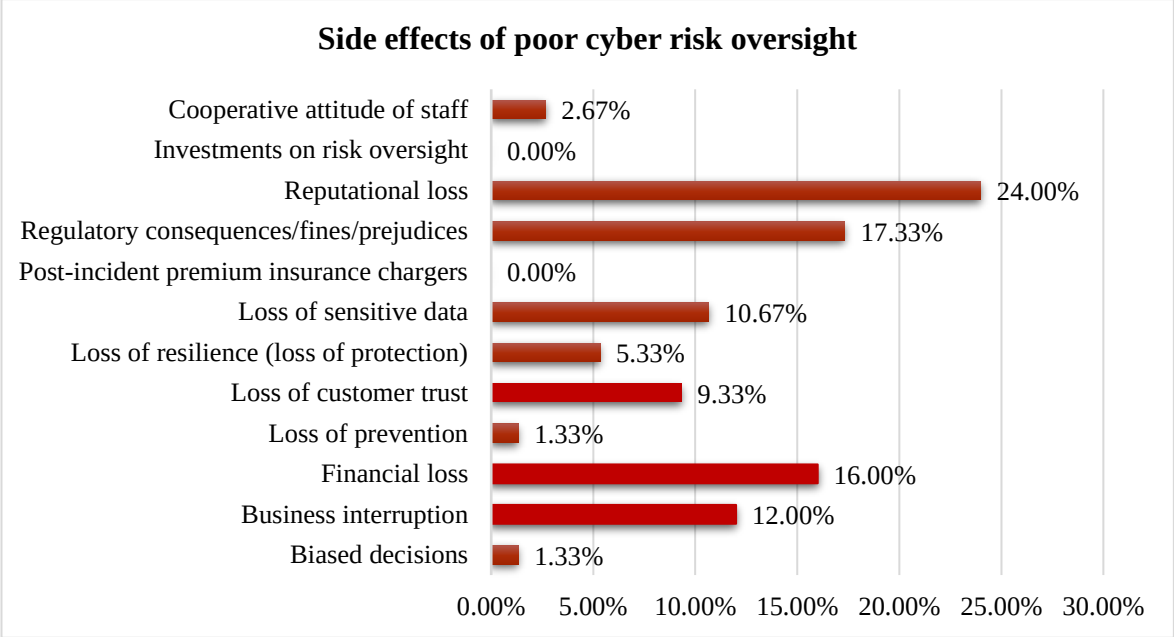


Figure 6-14 Key side effects of poor risk oversight

As Figure 6-14 shows, there is no significant difference among the top adverse effects. Three main side effects have been identified: reputational loss (24%), regulatory consequences (17.33%), and financial loss (16%). 24% of respondents reported strong evidence of side effects on reputation. Consequently, all side effects are interlinked, losing reputation might mean that regulatory consequences are generated. 17.33% of respondents confirmed the regulatory impact. Intertwined, financial loss (16%) is the third side effect articulated. *Business interruption* (12%) or *loss of sensitive data* (1.67%) relate to losing *customer trust* (9.33%). This leads to the conclusion that that poor management can damage or erode an organisation's reputation. ERM has a cross-functional role that aims to protect brand name equity. Reputation is an intangible asset and a key element that supports the achievement of objectives (as stated by Gatzer and Schmit, 2016). Considering the reputational risk and its layered effect constitutes the baseline for approaching the risk strategically, respectively ERM downsising risks. Respondent [13] propounds the view that:

> "For us as a financial service, reputation loss is absolutely so critical. In that we work so hard to build a brand and build trust with our customers, with our partners that to me, [it] is the most paramount. Regulatory consequences and fines and those types of things could come out of that, but, in [the] financial services, reputation loss is very difficult to regain."

This argument is further delineated in the quotation of Respondent [24]:

> "So, your reputation is tied to your revenue, your reputation is tied to how you regulate. So I'd have reputational risk right at the top of the areas of concern. Stuff like a business interruption and customers who go away…they're not happy about

> your reputation. So there are all kinds of side effects of that top tier, and your reputation is anchored by what you promise your customers. They could choose. Reputation: it's got so many cascade effects. And you can't get it back; you can spend one hundred and fifty years building it up and lose it in fifty minutes."

A similar view was identified by Lowe, cited in Wakefield (2014, p. 235), which stated that "it takes twenty years to build a reputation and five minutes to ruin it". Addressing the problems of reputational loss, similarities with loss of customer trust (10.67) have been detected. Trust and reputation are found to be linked through lens of trustworthiness (Jøsang *et al*., 2007). Despite being two different terms, reputation refers to how an organisation is overall perceived while trust refers to reliability. While much attention has been centred on defining reputation, Jøsang *et al.* (2007) state that it is a 'measure of trustworthiness'. Altogether, an indication of this relationship is stated by Respondent [14]:

> "What we are selling is trust and expertise. Failure of risk oversight can lose customer trust. Customer trust is difficult to build up. [It] can be lost in a day. Number one, loss of customer trust."

Financial loss (16%) is the third unwanted side effect for an organisation. A closer look at the data indicates that they are intertwined with one another as stated by Respondents [13], [15], [19], and [21]. Additionally, Respondent [21] substantiates that:

> "If you lose customer trust, they start leaving your bank, and that will lead to a financial loss. Reputational impact [is] the same. If you're on the front cover of the Telegraph saying that there was cyber-attack and we didn't do anything about it, that will lead to a lack of customer trust and again lead to financial loss."

What is interesting about this research finding is that it corroborates various side effects and highlights a domino effect. Literature defines this effect between variables as 'systemic risk' (Smage, 2014; Armenia *et al*., 2018; Marotta and McShane, 2018). Surprisingly, respondents disregarded effects such as loss of resiliency, probability on investment on risk oversight (0%), and a potential increase on premium insurance charges (0%). The value of *insurance* (0%) may suggest that the sampled organisations have not encountered incidents that affected premium fees.

6.2.3.6 Utilisation of industry frameworks (Q22)

In managing cybersecurity strategy, organisations rely on various frameworks, security management programmes and/or standards in order to cope with their exposure to a wide range of cyber risks. In particular, the scope of this question was to determine which are most used and what the rationale is. Figure 6-15 reveals the main findings.

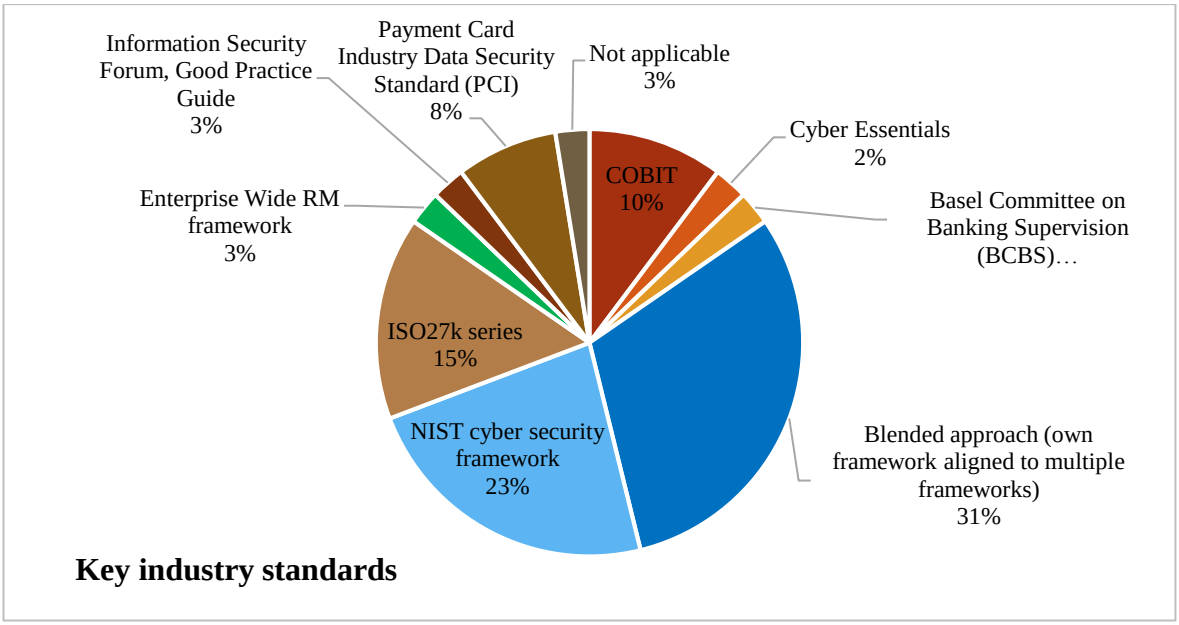


Figure 6-15 Key industry standards/frameworks used by sampled organisations

Findings indicated that a considerable amount of organisations use a blended approach (31%). This means that 31% of the sampled organisations preferred either to use a mix of standards and frameworks and/or create their own frameworks that warrant security baselines. Findings showing conjunction with many frameworks are reported, for instance, by Respondents [11] and [22] as a positive correlation in using the good practices of the ISO 27000 series, COBIT, and NIST cyber security frameworks. Equally, Respondent [18] uses the same frameworks as a point of reference and refers to them as being 'customised'.

Nonetheless, Respondent [13] argues that:

> "I think we certainly are connected with many of the industry standards but really we have created our own. Our business is unique, our platforms is unique, and you can't just take it off the shelf. We certainly pay attention and learn and look at those, our industry standards for certifications around things that we have to comply with."

This is in agreement with Respondent [9]:

> "My organisation needs to adhere to many types of frameworks and standards, and so on, so my organisation has pulled all this material together from various different frameworks, and developed an internal system that we follow internally."

Additional research findings outline the second interpretation of security baselines; 23% of sampled organisations abide by NIST cyber security framework (without considering cases where organisations use a blended approach). Respondent [24] refers to the current approach:

> "So, we do have a core reference to NIST, we do recognise other frameworks where particularly in other regions…where a regulator will say they rely on COBIT, so we

> have to pivot and talk their language. The good thing is you can translate roughly across all the frameworks. We anchor quite firmly on NIST, but we flex where we need to."

The third category of response signalled use of the ISO 27000 series (15%). Respondent [5] justifies the use of the ISO standard, stating that:

> "I think [that] ISO [standard] is good from and internet perspective because NIST is much more in the USA. If you want to sell a product on the Internet market, probably you want to think of ISO."

Although the standard partially denotes consideration of the boundaries of standards, it chiefly refers to multiple jurisdictions under which organisations activate. These findings show that respondents have a clear preference for optimised frameworks that are internally built yet compatible so as to produce proof and adherence to a number of external frameworks and feasible for multiple controls. In conclusion, although these findings are consistent with previous research, they differ slightly because previous results reported in the literature indicate many other frameworks and standards (e.g. OCTAVE series, ICAS Information Security standard, PAS 555 standard, IASME framework) that have been omitted by respondents (see Subsection 3.4.2, Chapter 3 and Subsection 4.3.2.2, Chapter 4). Additionally, another drawback to the findings is that calculating the use of the frameworks remains limited due to using a blended approach. Consequently, NIST and ISO standard usage is assumed to have higher values.

Furthermore, from an initial number of seven framework series related to CsM identified in the literature, only three have been confirmed by empirical findings (e.g. ISO series, NIST cyber security framework, Information Security Forum Good Practice Guide). As, some mentioned standards were either IT-centric, technical-related, or operational-related (COBIT standard, Payment Card Industry Data Security Standard (PCI), Cyber Essentials), the Researcher disregarded them hence are being out of scope for research.

6.2.3.7 Benefits of cyber risk oversight/CsM (Q23)

Regarding implementation benefits of cyber risk oversight (*terminology used by Researcher because CsM was not applicable to all respondents*), respondents were asked to comment on which return on investment (ROI) their organisation focuses more; specifically, ROI terminology was used on the assumption of benefits metrics. Generally, ROI is a quantifiable metric (2009)—the difference between investment and return. Showing effects of risks, ROI is measured by the ratio of savings as saving cost is a central value (Hall, 1999). Leaving aside the quantifiable metrics, Brotby (2009) suggests another view regarding return on

security investment (ROSI): *ROSI= (Risk exposure *% Risk mitigated)-Solution costs*, that leads to the conclusion that cyber risk oversight is a loss prevention approach. Another possible explanation for ROI and benefits is reported by Respondent [24]:

> "I wouldn't say investment; it's more [about] of revenue protection because the ROI we would look at from my perspective is (again they are all relevant) …but we would look at just pure business growth. If we are delivering what we've committed to, to our clients and our regulators, we automatically see that business growth, and that's the ROI measure, so [that's] when the business is making money.

Thus, the findings of this question address a controversial belief among practitioners that ROI should be quantifiable. The Researcher propounds the view of a speculative assumption of unquantifiable ROI, respectively benefits. The proposed 'unquantifiable' ROI is outlined below in Figure 6-16.

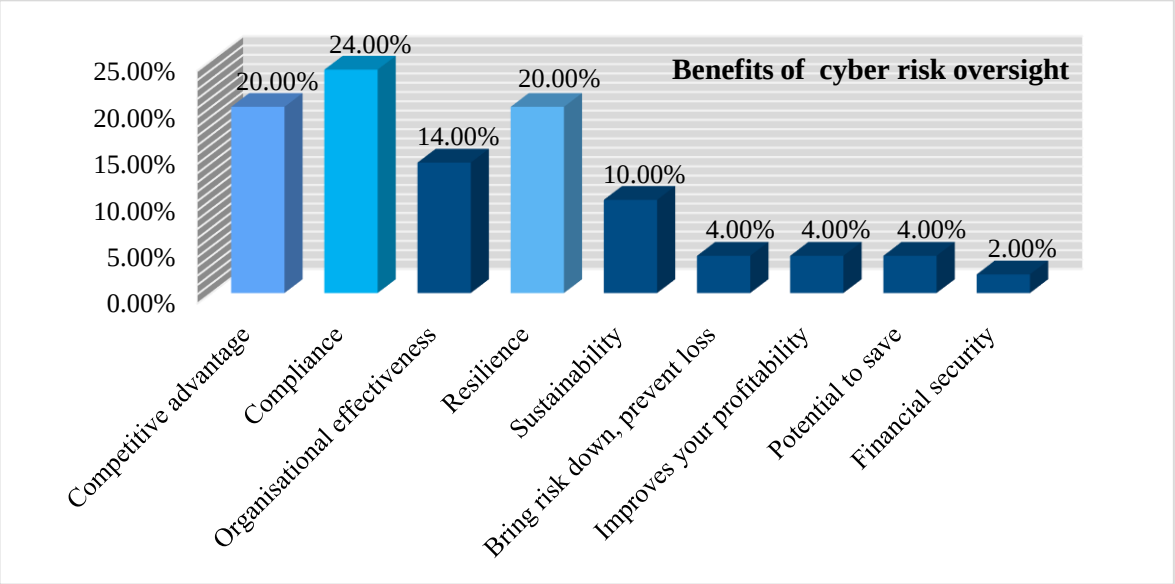


Figure 6-16 Benefits of cyber risk oversight

Five main benefits emerged as key drivers: compliance (24.00%), competitive advantage (20.00%), resilience (20.00%), organisational effectiveness (14.00%), and sustainability (10.00%). Among many others, *compliance* seems to be the principal justification of implementing cyber risk oversight/CsM; with small differences, *competitive advantage* (20%) and *resilience* (20%) being two other benefits of deploying security practices.

In this context, data shows that organisational effectiveness (14%) is another benefit to consider; as exemplified by Respondent [15]:

> "It's organisational effectiveness. I mean if you had asked this question a few years ago, it would have been answered differently. Probably [I] would have said compliance because obviously there's significant regulatory pressure, but you can't

> just be ticking the box and following laws. You have to do that, but ultimately you have to know how to use risk in a smart way. So, the whole purpose is to make the organisation more effective, more sustainable."

Respondent [15] puts forward the view that organisational effectiveness is well understood and ensuring effectiveness, in turn, leads to sustainability and compliance. This is in line with views of Armenia *et al*. (2018), hence mature cybersecurity implying proactive compliance. Respondent [24] considers that each aspect has an impact on the next one and vice-versa:

> "Competitive advantage is gleaned from the promise we make to our clients and customers that "we going to keep your stuff secure", that gives us a competitive edge, that also boosts our reputation. It has a cascade effect I think to all the other ones."

The aftermath of cyber risk oversight is considered by Respondent [18]:

> "The biggest benefit is to make sure that everything is maintained and the other biggest benefits are to avoid unnecessary costs, unnecessarily losses from poor Information Security over time because as a bank we are simply regulated. We have a lot of fines for not compiling with customer-related privacy protection or, maybe, not ending a proper report that shows our level of information security and overall enterprise risk posture [position]."

Likewise, Respondents [6] and [21] share a similar view, looking at the competitive advantage in terms of revenue and profits and ensuring that the organisation meets targets. Part of this pertains to its operational effectiveness — achieved targets with optimised costs. The causal link between *organisational effectiveness* and *competitive advantage* leads to sustainable practices. As Respondent [11] says: "…organisation effectiveness and competitive advantage, the two are inexplicable in joint." *Sustainability* was reported by 10% of respondents as being a result of implementing CsM. To clarify, organisational sustainability refers to more than business expansion and economic development and is therefore an interlink between strategic business and cultural dimensions. Either it refers to a group of actors and organisational structure, technology, or governance; sustainability in the context of ROI is efficient and effective financially, socially, environmentally, strategically, and culturally (Ilmaz and Flouris, 2010).

When discussing benefits with respondents, four additional subthemes emerged: (1) *bring risk down, prevent loss, (2*) improve your profitability of risk oversight, *(3*) *potential to save*, and *(4) financial security*. In short, these findings suggest that achieving organisational effectiveness leads to resilience, which in turn leads to a competitive advantage and

compliance. All of the options are interrelated and even though they serve as loss prevention, a potential to save and comply can be calculated for the remaining non-metric.

6.2.3.8 Executive board expectations regarding enterprise risks and cyber risk governance (Q24)

Championing good practices for risk oversights has been long employed as a practice that 'sets tone from the top' (Society of Actuaries, 2018). Direction from a company's Board matters because it is a governing body with the ultimate goal of overseeing risk and ensuring the alignment of objectives with its organisations' missions, visions, core values, and strategies (COSO, 2017). In other words, the board of directors represents the interest of shareholders and aims to ensure that sound risk conduct is applied in conformance with external pressures (e.g. shareholders, regulators, customers, competition, rating agencies). Due to increased external pressure to protect an organisation's value, the involvement of a board of directors becomes more dynamic (EY, 2015; COSO, 2017; AICPA, 2018; Society of Actuaries, 2018). The aftermath of such pressure is passed on to executive managers. Essentially, the role of the board becomes twofold: to respond to external pressure for transparent oversight and ensure internal applicability and measurement for both protection and value creation.

Thus, the board's expectations emphasise whether key elements are in place, whether departments are engaged with each other, and whether the organisation manages risk oversight appropriately (Beasley *et al.*, 2015). This prompts a hierarchy of responsibilities to ensure effectiveness and accountability of risk exposure (AICPA, 2018). Moreover, knowing the board's expectation helps to understand if there are any deviations. Figure 6-17 reveals the main expectations for risk oversight.

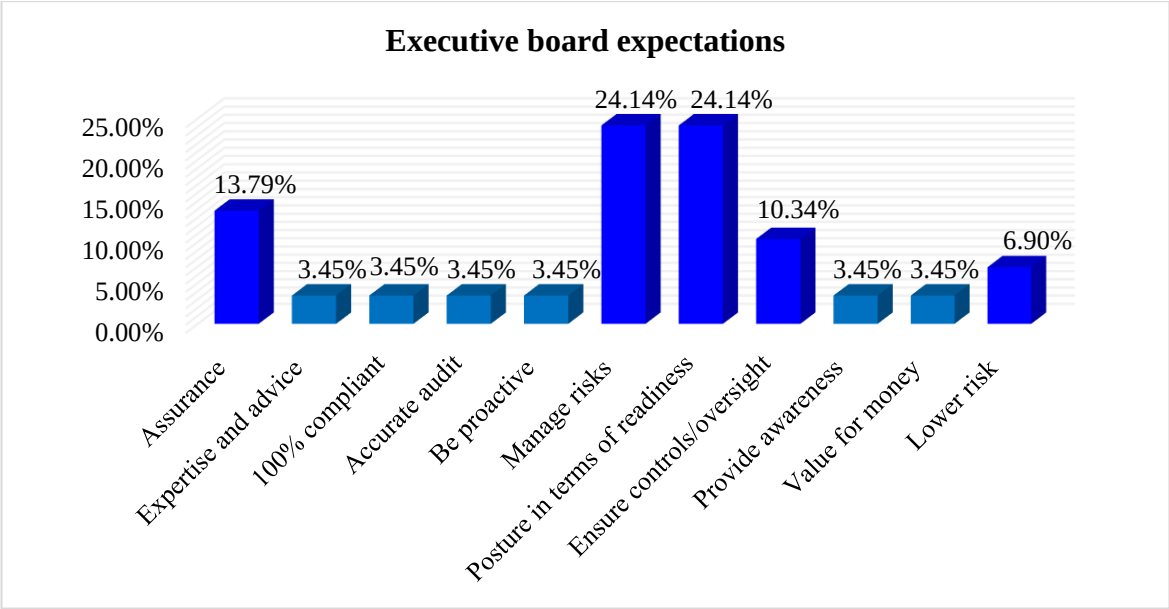


Figure 6-17 Executive board expectations regarding risk oversight

There is evidence that the board's expectations have a positive effect on risk oversight of both enterprise and cyber risk. Firstly, managing risk (24.14%) and stating the organisation's position regarding readiness (24.14%) are of the utmost importance for respondents. This interrelates with *assurance* (13.79%), which show that expected controls are in place. The overall response to other compounds was low value (expertise and advice, 3.45%; 100% compliant, 3.45%; accurate audit, 3.45%; proactive, encompass and capture all aspects of risk, 3.45%; provide awareness to employees, 3.45%; value for money, 3.45%). In this context, it should be considered that a board's expectation is related to a high-level approach: on how well the department is **managing** the risk within **risk appetite** and what the current position is (**risk profile and tolerance**) in terms of readiness. Lastly, it expects an assurance that everything is in place in order to lower risks. *Assurance*, (reasonable of taking care, handle risk) in the view of Respondent [18] is:

> "The main expectation of what needs to be done. Also, I make sure they are aware of what is happening in the risk industry in the region specific to, you know, financial institutions…what are the risks, what are the things we need to watch and specifically where are we as a bank, where is our status, how do we look inside, what is our posture in terms of readiness, how ready we are and what needs to be done? Also, what's the expectation from inside, what's the competition from outside? Those are the main concerns from it…, visibility, whether we have the right tool to monitor and control, if we have the preparedness inside and if we have identified critical business processes to help us and maintain the business."

These findings demonstrate the multifaceted responsibilities of risk oversight, which are expected to make the correlation between external variables and internal readiness. *Managing risks* effectively is among the main two expectations. Respondent [17] draws an interesting line saying that: "They would only want to know exceptions in risk that were in the range of being high." In spite of that, Respondent [23] believes that an executive board expects to provide ample support:

> "I think that they expect that the risks are properly managed, in the sense that risks are identified, and prepared actions are taken to manage risks, to manage or to assess them or to transfer them."

This asserts the view of Respondent [4]: "absolutely zero breaches". Respondent [24] echoes a much milder expectation:

> "Keep it under control. Keep risks as low as possible, we don't want risks that's the reality of things. It's no different to…they don't want incidents or risk exposure. We are no different to all the other risk types. So, keep it within tolerance, keep it within appetite, and that's it. What it translates to is a whole different ball game."

However, practitioners' literature asserts that such expectations in current market context are an 'illusion' and an unreasonable expectation to have given the increase of emerging risks (Oliver Wyman, 2018b). Further analysis shows that position regarding readiness (24.14%) is central. Respondent [20] offers a descriptive account of three paths: past incidents, current exposure, and solution in order to lower risks. While others such as Respondent [9] indicate expectations for proactively and consistently identify vulnerabilities to mitigate what those are, respectively to *ensure controls/oversight.*

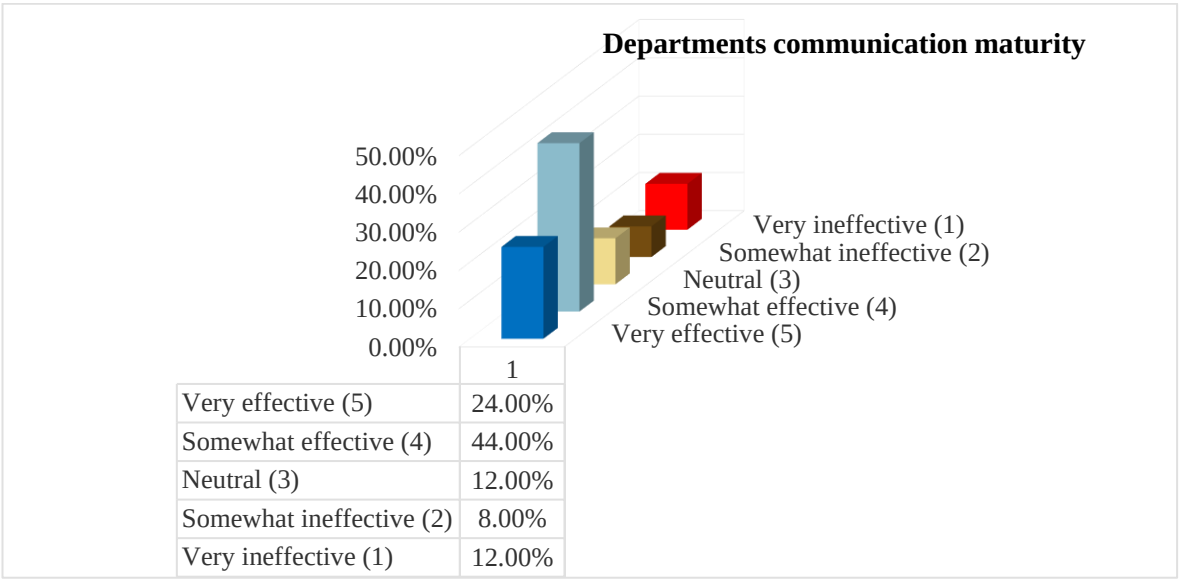
Another outcome was *value for money* (3.45%). Respondent [26] highlights that the executive board would want to make sure that there is value for money and what the department is providing is worth the money being spent (metrics). All captured data represents the view that validates interest for resilience and assurance of governing boards. In contrast with the literature that discussed the hard task of the board in assuring internal control (see Section, 2.4, Chapter 2 and Subsection 4.3.1.3, Chapter 4), the empirical findings show another side of the board, one that delegates and sets expectations by way of setting the roadmap for good practices.

6.2.4 Theme Four: Strategic Alignment

The objective of this section is to underline the value of variables in the context of strategic alignment that conditions the theoretical assertion of the need for a strategic alignment between CsM and ERM and key organisational dimensions.

6.2.4.1 Departments communication (Q25)

Communication between departments is identified by way of alignment measurement (Hosseinbeig *et al*., 2011). Communication results in being the link between strategy and implementation, and an enabling tool that connects silos (Althonayan, Keith and Killackey 2012; Volk and Zerfass, 2018). An excellent strategic communication creates departments' connection and engagement with organisational strategy, pertaining to common vocabulary and mutual understanding that provide knowledge sharing and alignment (Chen, 2010; FINRA, 2015). The results in Figure 6-18 show that communication is acknowledged by respondents segmented in five strands of maturity.



	1
Very effective (5)	24.00%
Somewhat effective (4)	44.00%
Neutral (3)	12.00%
Somewhat ineffective (2)	8.00%
Very ineffective (1)	12.00%

Figure 6-18 Departments communication maturity

When discussing departments' communication, respondents were required to describe current maturity. This involved a description of how risk is communicated and dealt with across the respondent's organisation. Determining effectiveness, nearly half of the respondents (44%) describe their practices to be *somewhat effective*. Analysing the options available, Respondent [11] ascertains that:

> "I would say that most [of the] time, it is very effective. I've seen a couple of incidents which've been somewhat effective. In my humble opinion, I thought that it could be faster. And perhaps more [communication] across the enterprise as opposed to segmented communication. But most times, [it's] very effective. Sometimes, not always…I would go to four, 'somewhat effective'."

With particular reference to long-term improvements, Respondents [14] and [15] enunciate the importance of making sure people understand policies and procedures as well as how to

escalate and what to escalate. Ascertaining that communication effectiveness varies, Respondent [18] evaluates ineffective communication:

> "It's on a basic level. There is some awareness, but as a culture, we need to improve our transparency, we need to open our open communication. There is no way to improve on its own; our challenge is on working on the culture at an enterprise level, being more transparent and openly, talk[ing] about it. It's very low. 'Two'."

Only 12% declared having very ineffective communication. Respondent [20] shares a negative view, asserting that:

> "They [departments] are [have] very different systems as well, so they wouldn't communicate unless they are crossing each other in some way."

Overall, these findings suggest that the maturity and effectiveness of strategic communication are other determinants of alignment. The existence of these effects implies that despite broader research, the relationship of communication and alignment has yet to reach maturity.

6.2.4.2 Risk ownership for managing cyber risks (Q26)

This issue of how cyber risks (cybersecurity risks) are dealt with by an organisation are explored with a twofold scope. Firstly, the purpose is to identify the respondent's opinion based on observation and experience, and whether it is appropriate to manage each cyber risk or incident at a departmental level rather than at an enterprise level. The second part of this issue is later addressed in Q27, which seeks confirmatory statements regarding how things actually happen. It is based upon an accepted responsibility among all parties. Risk ownership is a critical administrative aspect that enforces accountability within an organisation (COSO, 2016), and it is, therefore, difficult to address the question without understanding the grounds of responses (what resources and preventative controls are in place at all levels). Thus, ownership is a delegated responsibility, based upon an accepted responsibility among all parties. The risk owner is *accountable* for managing risk (Olson and Wu, 2007). In this particular case, the cyber risk owner is the organisation, respectively delegated managers. They can, therefore, decide whether to retain, mitigate, increase, or avoid a risk, or, lessen its exposure or lesser consequence (Olson and Wu, 2007). To this end, this question should determine if cascading accountability for risk is a common approach at the departmental level is (EY, 2015) or if it is dealt with at an enterprise level. Figure 6-19 summarises the identified risk flow ownership of sampled organisations.

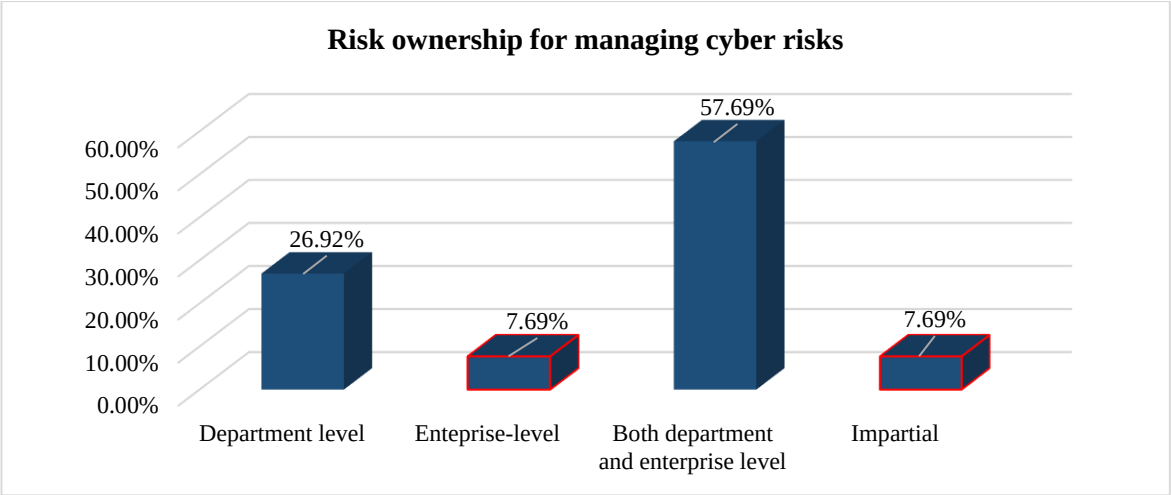


Figure 6-19 Accountability in managing cyber risks

Seeking to discover how risks are dealt with at an enterprise-level, four categories have been generated, some demonstrate interdependencies across risks while others demonstrate disconnection between parts of an organisation. The context of exploring the accountability and responsibility in managing risks was investigated mainly through an alignment paradigm lenses. From four themes that offer a potential option for dealing with risk oversight, two reach more significant values. A majority of respondents (57.69%) described the management of risk deployed at *both department and enterprise levels*. How an organisation implements risk governance, at both a departmental and enterprise-level, is exemplified by Respondent [1]:

> "I think it should be a system at the enterprise level, I mean you may find some stuff that needs to be also looked at a departmental level, but I think that encouraging things to be looked at the enterprise level. I think that yes that company stood view of how stuff fit together. Sometimes if things are looked at the department level, that angle it's kind of missed."

While Respondent [13] outlines an operational perspective:

> "I think it is. From our perspective, if there are specific HR issues, it should be managed at the HR level with a governance component around that.[It] ties enterprise risks and that's how we manage and think about our own audit functions We're identifying these risks, we're thinking about the management at the department level, but our audit and our governance level is coming in at an enterprise risk level."

Respondents [15] and [17] outline a dual-responsibility: one that is local with a low level and does not require senior management input, and a second that is a centralised approach for understanding the impact on the business.

As evidenced in the interview data, the second category of respondents describes risk ownership remaining *at department level* (26.92%). Respondent [10] identifies that the management of risks and mitigation usually takes place at a department level. According to Respondent [11], some risks are particular to departments and are usually managed and owned by that department, with automatic complications happening at an organisation level. The idea of escalating only significant risk is also acknowledged by Respondent [4]:

> "Quantitative is great but not all risk can be quantified, so you really want a low risk to manage an absolute department and never get communicated to senior level. Only your significant risks should be communicated to senior levels; the senior level do not want to see 300-500,000 risks, they want to see what the critical risk is. So, I think risk management has to be where your subject matter experts."

Respondent [7] believes that depends on the type of incident, impacts and lastly upwards triage of risk. Respondent [8] refrains from commenting on this issue by providing a cautious statement:

> "I'm going to give a risk person answer: 'it depends'. Because it depends on the situation. If a risk is identified and it is even at departmental level, it needs specific controls. However, that risk and how it was acted on must be communicated at enterprise-wide [level]."

The problem of how risks are managed also received impartial answers (7.69%). In some ways, despite having impartial statements, it describes an isolated approach; respectively, risk shall be dealt with by chance, and this thus shows dissonance with ERM principles (e.g. Respondent [20]).

6.2.4.3 Department cross-functional responsibilities for cyber risks (Q27)

Investigating how organisations deal with cyber risks, this question is a continuation of the previous question. Q26 delimitates the context, whereas Q27 generates a statement describing sampled organisations' maturity in dealing with risks. Concerns have been expressed about how organisations deal with risks internally, and how business objectives are strategically supported. Controlling risk strategically and holistically has been of interest for many scholars (aspects discussed in Section 2.7, Chapter Two and Section 3.1 and 3.5, Chapter Three). However, overcoming difficulties in successfully implementing strategic alignment remains a challenge (McShane, 2018). To comprehend in what way cyber risks are managed and controlled, the below Figure 6-20 presents the maturity of sampled organisations.

Figure 6-20 Department cross-functional cyber responsibilities categorised

These findings reflect previous research, which outlined immature alignment (objectives and strategies) and a lack of operational flow within organisational departments.

Risks are treated through both silo and enterprise-wide approach (57.69%)

Respondent [11] states:

> "In terms of the process where risk is identified, each department deals with that risk because the owner has a line of business. But, as it applies the ERM philosophy, I think that in that way, there is a holistic approach to it. However, [we] haft to have the enterprise-wide awareness of additional impact down [into] other lines of business. So, they own that risk. There is mandatory enterprise awareness."

Previous respondents emphasised how risks are delegated, while Respondent [23] describes a different approach of 'once a year assessment' that., it may be assumed, aligns annually:

> "We have a top-down and bottom-up approach and that it's more holistic [view] in the sense that every year we identify, we map all the risks within the organisation with the support of the business unit and the head of the business unit, so we have the complete mapping. So yes, departments are responsible of implementation of actions that are defined by the board. We normally do training once a year."

This approach of delegating risks through a top-down and bottom-up approach is also confirmed by Respondent [8], who describes the holistic alignment by the use of a central repository for all risk types, so it would be aligned across the enterprise.

Risks treated holistically received fewer considerations from respondents (23.08%). Respondent [10] argues that:

> "[It] depends on what risks are you talking about because manag[ing] risk dictates how you approach it. Because [of] that, for instance, we would need subject matter expertise rather than general expertise."

Each department deals with its own risks (15.38%) represents in plain senses that the risk owner is the department itself. As many others say (Respondents [2], [6], [12], and [18]):

> "There is a bit of miscommunication. That is one of the biggest challenges, if you ask maybe two/three departments, they will give you different information. So that's one of the reasons we are trying to have an enterprise level corporate-wide [approach] that is ultimately responsible for having single source of trust for all of us. That's the strategy, that's what we are working on."

This broadly explains that the organisation acknowledges the gaps and value of ERM in alignment risk oversight, creating a bridge between departments and leveraging the principles of wholeness, strengthening the governance of risks. If referring to how literature is categorised (Section 2.7, Chapter Two, the three-dimensional perspective of the alignment literature, *adoption-implementation-assessment*), these findings are asserting maturity assessment. In short, the antecedent of alignment is in line with empirical findings. Thus, it is not surprising that the empirical evidence points towards the idea that there is scarce consideration for the integration of CsM. A final finding illustrated in Table 6-10 supports the above.

Table 6-10 Organisation alignment maturity

Question 27		**Question 26**	
Organisation alignment maturity		**Respondents' view**	
Each department deals with its own risks	15.38%	Department level	26.92%
Risks are treated holistically	23.08%	Enterprise-level	7.69%
Risks are treated through both silo and enterprise-wide approach	57.69%	Both departmental and enterprise level	57.69%
Other	3.85%	Impartial	7.69%

Surprisingly, identical results were identified for both questions 27 and 28, echoing a double confirmation that risks are managed through a mix of approaches. This is in line with what was reported by so-called *level two – structured and implemented alignment, some form of risk approach is addressed through basic policies, processes, procedures but mainly on a silo basis* (see Subsection 4.4.2.4, Chapter 4). A slight contradiction has been identified regarding how departments deal with their own risks (15.38% versus 26.92%). This suggests that respondents lean towards silo views, meaning that the value of ERM in those specific organisations might be less in terms of value and benefits.

6.2.4.4 Credence for aligned strategies of CsM with ERM (Q28)

Literature that focused on CsM alignment with ERM is scarce, yet for the literature there is, it overlaps with antecedents of either IT/ IS alignment or RM (previously discussed in

Section 2.7, Chapter Two). Understanding the relationship of CsM and ERM is pinpointed through the lenses of both paradigms' advancement and assessment of the adequacy of current risk strategies in the view of respondents. To identify the effect of implementing aligned strategies, respondents were asked their opinions. The results of the analysis are shown below in Figure 6-21.

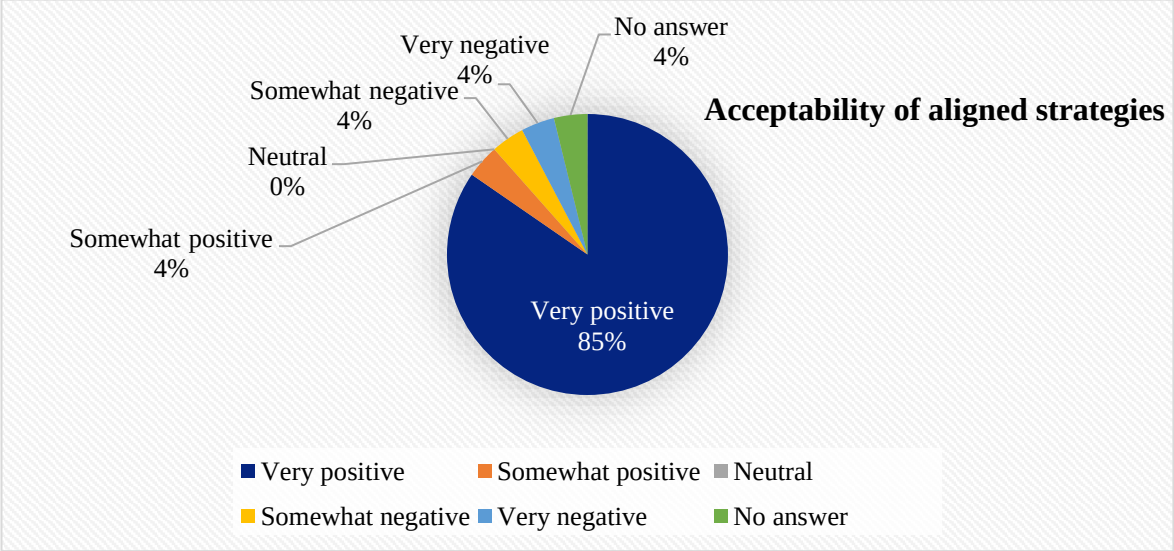


Figure 6-21 Acceptability of CsM and ERM

Figure 6-21 summarises the results of the analysis, which revealed significant acceptability of CsM and ERM alignment (85%). When looking at findings, there is a disparity between previous outcomes (maturity of alignment) and an acceptability of alignment.

Nevertheless, achieving holistic risk oversight and control is a well understood concept among respondents. The first concept refers to holistic management of risks and the latter refers to controlling/modifying specific risks (BSI, 2018). The remaining respondents share an identical result (3.85%). None of the respondents remain neutral. Under these conditions, the feedback about the proposed approach was perceived by Respondent [10] positively:

> "I think if people have got the resources, to have that kind of specialisation, I would say yes. The reason we have it in the same places is partly because of our resources."

Additionally, Respondent [11] explained:

> "I think that it would be very positive. We want cybersecurity risk to be baked in everything we do. We don't want to be overly preoccupied with."

Respondent [12] added:

> "I think that it is part of the ERM, it is a more interesting element and makes sense. Because ERM should have all types of risk."

Often overlooked, integration of all risks plays an essential role in holistically managed risks. Respondent [4] considers that:

> "The 'unified strategy' absolutely; one of the fundamental principles of risk management is to have a common approach to how you deal with it."

Respondent [6] expresses opinion by saying that:

> "Often you see IT risk and cyber risk as a subset of operational risks, if you know what I mean. At the enterprise level, risk and cyber form one of those. Because of the growth of cybersecurity nature of IT security, I think probably has a positive effect."

Indeed, there were several respondents who had very negative views (4%). For example, Respondent [25]:

> "I've kind of gone somewhat negative here. I guess I'm not…could be swayed but I guess the strategy at the moment of cyber is completely different to the strategy we have for risk management and governance. I think the two are very different but also share a lot of similarities. So, we'll use risk management as a framework in cyber, so we would want to make sure that whatever the businesses framework for risk management was, it was aligned to how we were doing things."

Despite such a negative view, Respondent [25] seems to understand that 'compartmentalised' strategies may lead to impairment of achieving organisation objectives. When things are in a state of mature alignment, it becomes a 'business enabler' (Mean, 2014).

6.2.4.5 Mechanisms in place for alignment (Q29)

A problem that emerged during the initial stages of the systematic literature was the lack of literature referring to a unified mechanism by which an organisation identifies, assesses and mitigates both cyber and enterprise risks across its organisation. Strategic alignment has been identified as a mechanism of performance. This cross-examination therefore evaluates practical views, respectively if/which mechanisms are in place and how they can be achieved.

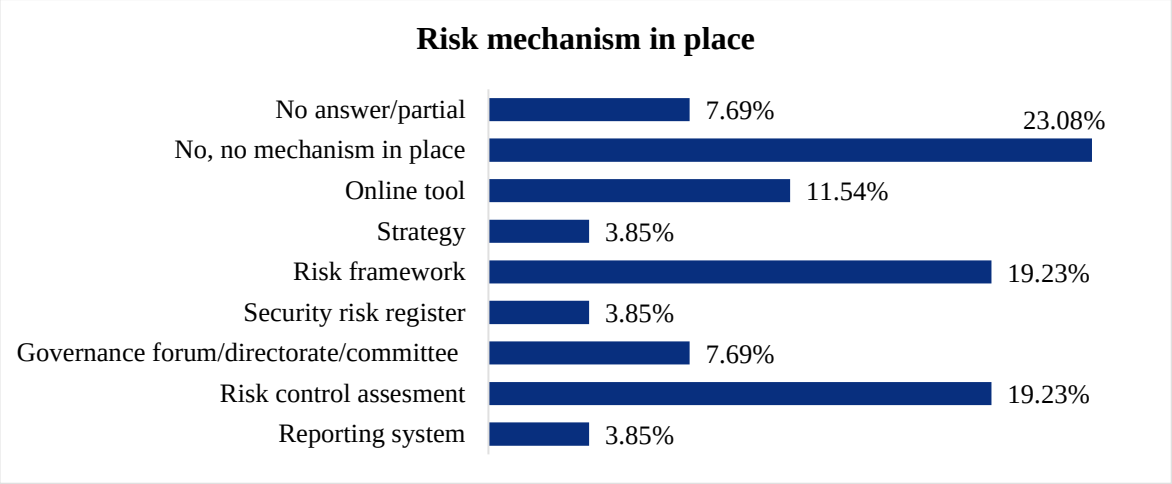


Figure 6-22 Mechanisms in place for alignment

23.08% stated that there are no mechanisms in place and 19.23% said that risk framework is supporting the process of alignment. Another 19.23% rely on risk control assessment to ensure alignment. A further category attributes alignment to the use of an online tool (11.54%). It is important to highlight that the highest percentage of respondents stated that no mechanism is in place. It was recognised by Respondent [23] that:

> "Structurally we are a bit behind in terms of cyber risk, the idea is to have a unified strategy, but we are not there … we are not still there. Actually, the implementing it is our goal, but we still have to work on it."

Likewise, Respondents [5] and [6] stated that their organisations are trying to build that, *however no unified mechanism is in place* at the moment. This is where departments manage their own risks, and they might escalate the risk that they have identified. Moreover, some others, for instance, Respondent [10], explain another type of approach:

> "We take Nike's approach: 'we just do it'. Don't get a picture of complex structure around that. We don't have complex services. That cuts a lot of the risks."

In light of the above statement, it can be recognised that alignment is still immature and, in some cases, misunderstood. Several respondents stated that alignment is considered, but drawbacks exist and delay implementation. Others, such as Respondents [12] and [15], describe the mechanism of alignment as being the mechanism influenced by *RM framework*, a top-down and a bottom-up approach where risk is identified concerning their business processes and pushed down to business areas. The role of the RM framework, according to Respondent [20], is to set out risk appetite for operational risk and cybersecurity, and additionally manage all risk from risk identification, risk escalation, and risk continuation (Respondent [21]). Another respondent (Respondent [25]) advocates:

> "All I've been focusing on is perhaps using the mechanisms (methodology) within enterprise risk management to help support cybersecurity management but not necessarily alignment because our enterprise risk management includes a number of different and varied operational risks as well as business risks to the firm. And if you're aligning one, there'd be questions to ask why you're not aligning others. I'm not aware of organisations that would have dealt with that."

Apart from using ERM principles to meet alignment, some other respondents endorsed risk control assessment (19.23%) while a few other respondents reported the use of online tools (11.54%). Respondent [19] justifies the approach by explaining:

> "It's easier just to outsource and go out in the internet and procure a tool because it's easier, it's more agile then you need to be and if you'll be running into risks, normally the [outsourced] IT organisation will take care of."

At this stage, it was not possible to investigate which tools Respondent [16] was referring to. The Researcher can only assume that they were referring to performance tools (e.g. strategy map, balanced scorecard, and/or strategy alignment matrix, applications). Likewise, the analysis of alignment literature, which referred to mechanisms and tools, was problematic. Furthermore, Respondent [24] explains that despite technology advancement, ERM has been around for a long time to ensure alignment, However, people are realising that it is valuable when organisations globalise. Such view is additionally articulated by Respondent [16], when explaining the role of a governance forum (*a mechanism*). The security risk is articulated, monitored, and tracked by technology and risk management for visibility regarding what the issues are and how they are being reported and escalated.

The above *risk control assessment* relates to the literature that links the main contributors of Strategic Alignment Maturity Model alignment (SAMM alignment—composed by Henderson and Venkatraman 1993 and discussed in Subsection 4.3.3.1, Chapter Four). *Per total alignment condition* refers to an organisation's willingness to achieve its strategic goals and objectives. Gregor *et al.* (2007) refer to the mechanism of alignment as being a strategic planning mechanism, a governance arrangement, and lastly a communication mechanism. Whilst Luftman's strategic alignment model (SAM) describes a mechanism through the lenses of value, governance, partnership, scope, and architecture, and skills, Wu *et al*. (2015) complement this with three primary governance mechanisms: decision-making structure, formal processes, and communication approaches. Moreover, more recently Jevtić *et al*. (2018) proposed a model that comprises seven elements known as (7S): strategy, structure, system, shared values, style, staff, and skills. Furthermore, Joshi *et al*. (2018) understand

governance by means of a mechanism that drives structures, processes, and relational mechanisms, either intellectual (strategic), operational, structural, or social (see Subsection 4.3.3, Chapter 4).

6.2.4.6 Defining strategic alignment purpose, responsible and how it can be achieved (Q30)

As one interviewee said: "Alignment is a process of creating a roadmap to achieve the organisational purpose" (Respondent [13]). Early discussion about how organisations achieve strategic alignment is a cadence about how risk is acceptable in respondents' views, and how different parts of an organisation coordinate/integrate. These results raise intriguing questions regarding the nature and extent of alignment purpose, responsibilities and duty of achievement.

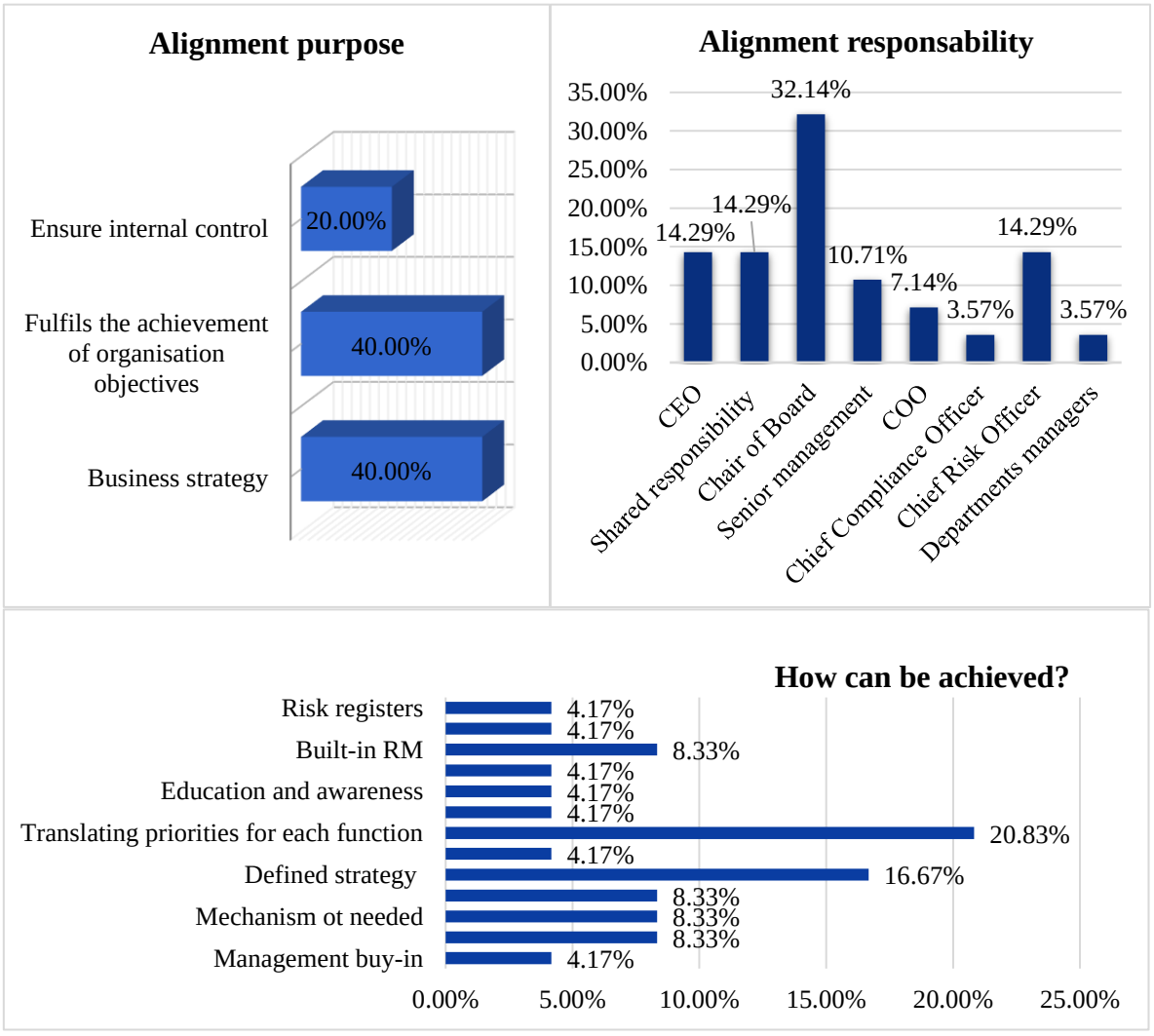


Figure 6-23 A three-dimensional view of alignment (purpose, responsibility and achievement)

Data is extracted from 24 respondents, and two respondents (7.69%) conclude that alignment does not apply to their organisation. Thus, this data is based on 92.31% frequency of answers. Respondents [20] and [22] preferred to be impartial/neutral in their answers.

Mentioning the alignment purpose, the themes identified in these responses were to ensure *internal control* (20%), to *fulfil the achievement of organisation objectives* (40%), and to attain *business strategy* (40%). Concerning the second part of the question (responsibility), it was found that the *Chair of the Board* (32.14%) was consistently indicated by respondents. Respondent [18] believes:

> "Ultimately the Board is responsible for making sure that all the business' initiatives are aligned with the business' objectives at the end of the day. At least it starts with the Board, at least it is championed by the Board or it will never make headway. So that's the biggest gap - getting the Board committed to making sure that all these initiatives are aligned with the business objectives."

A second view of Respondent [16] exemplifies the role of *senior management* responsibility (10.71%) for translating the strategy into priorities for each function (department or function). This is interpolated into key objectives for specific teams, tracked through performance reviews at the end of each year. Consequently, departments have specific deliverables and measures of deliverables. Such an approach would be typically aligned with the strategy of the firm. Moreover, Shao (2018) suggested that senior executives' backgrounds and behaviours influence alignment. Other responses to this question included *Chief Risk Officer* (14.29%), *Chief Operations Officer* (7.14%), *Chief Compliance Officer* (3.57%) and *Departments managers* (3.57%).

Consistent with the literature, Respondents [1] and [21] point towards the CEO's responsibility for transferring communication downwards, making everyone ultimately responsible. This pinpoint shared responsibility. *Shared responsibility* (14.29%) is evidenced by Respondents' [5] [11] and [24] responsibility for alignment, a joined exercise hence each team and business unit being responsible for their own programme.

Lastly, the third part of the question (alignment achievement) pertains to how alignment can actually be achieved. It has been suggested that *translating priorities for each function* (20.83%) and *defined strategy* (16.67%) are of utmost importance. Together these results provide valuable insight into the necessity of a holistic risk oversight function in order to proactively align all functions. Even so, prior research argues that function integration remains a challenge for most organisations (Majdalawieh and Gammack, 2017).

6.2.4.7 Benefits of alignment (Q31)

Systematic literature evaluation (Chapter Three) evinces the benefits of CsM alignment with ERM by extrapolating several research mainstreams of IT, IS, and RM, and by looking at their joint effects through lenses of alignments antecedents (e.g. neutral alignment, IT: Business alignment, IS: RM alignment, IS: ERM alignment) because of trends in the literature of alignment (discussed in Subsection 3.5.2, Chapter Three) and scarcity of literature on CsM and ERM alignment. Furthermore, data from Figure 6-24 (below) is thematically in line with systematic literature findings, which show typology trends of alignment (Subsection 3.5.2, Chapter Three) while Quadrant 1 (Adoption) refers to the motivation of alignment.

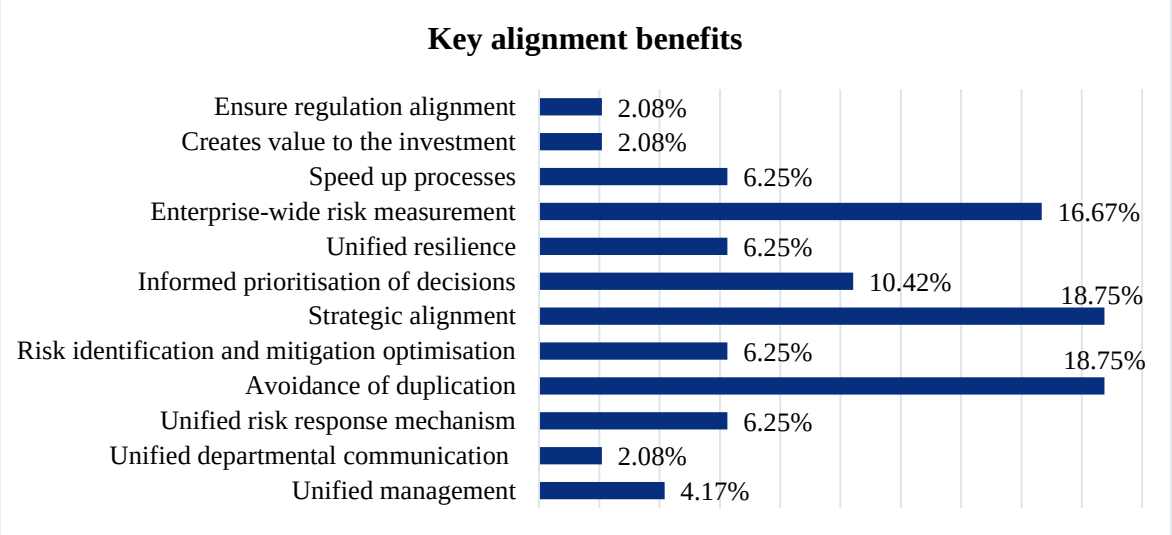


Figure 6-24 Key alignment benefits

Among the main key benefits identified are *avoidance of duplication* (18.75%), *strategic alignment* (18.75%), and *enterprise-wide risk measurement* (16.67%). Granting low values, three themes emerged: speed up processes (6.25%), give value to the investment (2.08%), and ensure regulation alignment (2.08%).

Respondent [11] argues value of alignment stating that:

> "I think that there're multiple benefits. It has to be an enterprise-wide accounting of risk, enterprise-wide measurement, I think is critical. I think that [the alignment] it does better; in terms of duplication, I think that the is mission is critical where it is a particular line of business mitigating a certain type of risk, and they then go in a fourth database. Then, resources can be combined, avoiding duplication. I think it is all these cascading benefits of having this alignment of risk governance and organisation objectives."

Respondent [8] adds more arguments, asserting that:

> "The biggest benefit I have seen it is the allocation of resources. And resources being people, as well as money, as well as technology and so on. So, if you don't align, the business is at highest risk (e.g. the 'crown jewels' of the organisation: data, the information). Then you will waste your resources. That is why it is important to align your cybersecurity strategy with the business strategy."

Respondent [18] supports the view that alignment gives value to the investment while others such as Respondent [21] believe that alignment, apart from meeting business objectives, also *ensures regulation alignment*. This is in line with literature findings, respectively Section 4.4, Chapter Four.

6.2.4.8 Consideration for CsM alignment with ERM (Q32)

Building on the idea that alignment of CsM with ERM literature is scarce, Q31 explores if respondents have considered the alignment or whether their organisation applies or is interested in applying the alignment paradigm principles. Figure 6-25 shows the distribution of answers per categories.

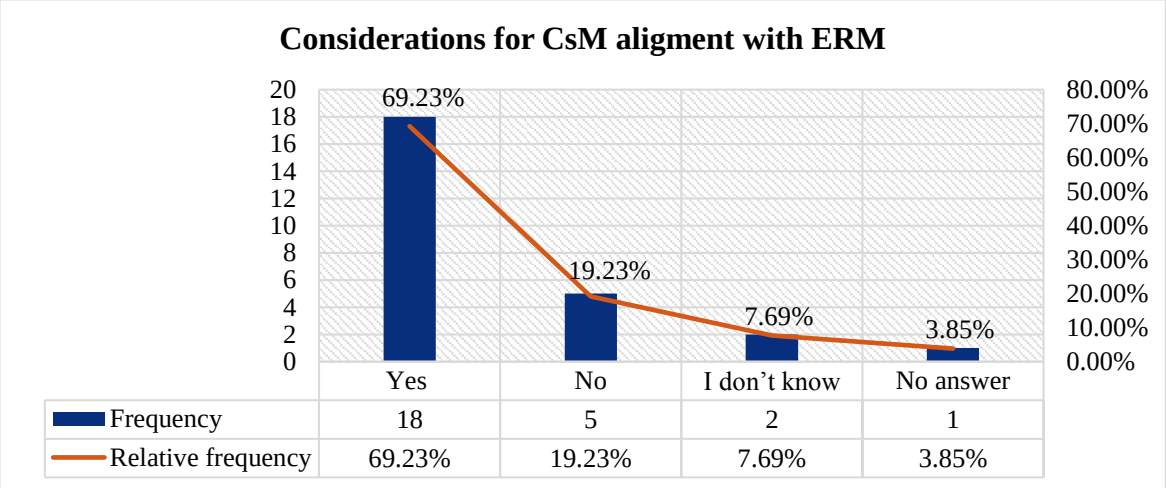


Figure 6-25 Considerations for CsM alignment with ERM

Figure 6-25 above shows that almost 70% of respondents considered CsM alignment with ERM. Respondents [6] and [21] believe that cybersecurity strategy is a subset of enterprise risk. It seems that there is a general agreement regarding CsM and ERM alignment benefits. Additionally, Respondent [18] supports this finding and justifies it:

> "Yes, we have considered that one we are working on it. We have underlined if we have a disconnection between the cyber risk and enterprise risk. Because cyber risk is everywhere it needs to be in every process it's every branch responsibility, it's not, obviously the cyber risk department or risk department … [that] might be the face of

> it but the Board is accountable, everybody is also responsible at a level to make sure that the realignment of cyber risk and enterprise risk."

Another line of thought on implementation is introduced by Respondent [1]:

> "[We're] currently in the process of aligning all the risk frameworks more internally together. Focus from current way of working to a new way of working, so that makes it a little bit difficult, but we see the benefits of it."

However, not all findings show that role of alignment is valuable. Some evidence agrees that CsM should not align with ERM (19.23%).

6.2.4.9 Sustainability of CsM and ERM alignment on long-term (Q33)

Question 33 is a double confirmatory statement. Initially, Q32 questioned if the alignment of CsM with ERM has been considered, while at this phase it explores a sustainable approach in terms of long-term organisational risk governance. Sustainable alignment is viewed as a mechanism that ensures a correlation between strategies and processes (Morrison *et al.*, 2011).

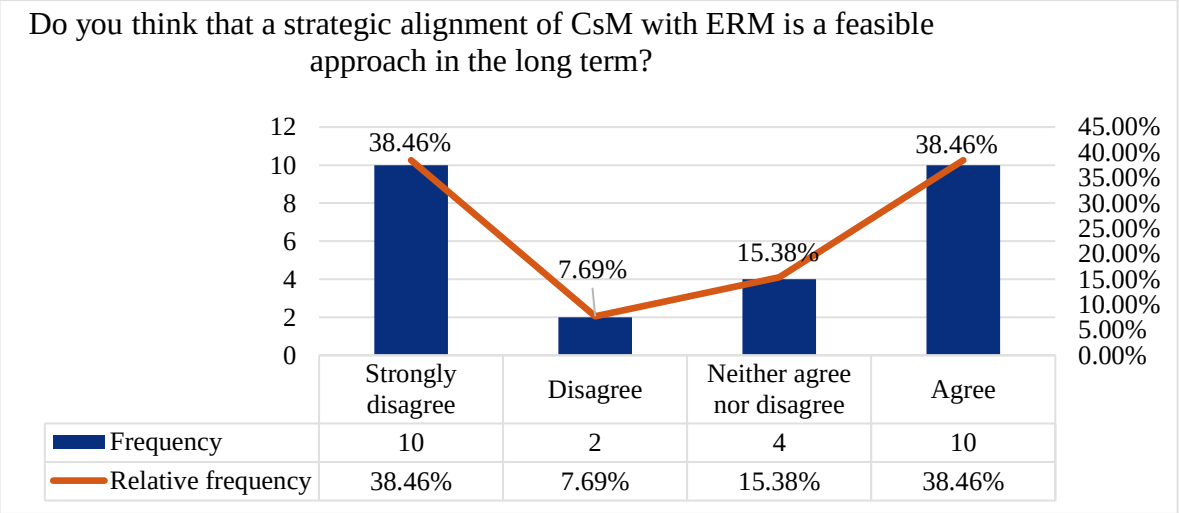


Figure 6-26 Respondents' view on CsM and ERM alignment sustainability

As reflected in Figure 6-26, a double contrasting agreement was identified; 38.46% of respondents strongly disagree with the alignment feasibility while another 38.46% agree with implementing alignment. A potential explanation of respondent's resistance to alignment might be explained by immature practices regarding ERM and CsM alignment, a lack of executive support (Papp *et al.*, 1996), a lack of mutual understanding (Johnson and Lederer, 2007) and/or a lack of understanding the alignments' benefits (Althonayan, Matin and Andronache, 2018). Factors thought to be influencing the decision to implement alignment have been explored in several studies. O'Reilly *et al.* (2010) assess the longer-

term impact of senior executives on strategic alignment, suggesting continuous enforcement and leadership guidance.

Furthermore, Respondent [25] asserts that they neither agree or disagree:

> "I'd agree with that in the long-term. But it will also be with the fact that there are other operational disciplines or legal disciplines of which risk management and enterprise risk management sort of strategy need to align as well. So, it's not just one and done. There needs to be other considerations, conduct risks, legal risks, operational risks etc."

In contrast, to be successful in alignment, Respondent [26] said:

> "Yes, I think from what I've seen in the way that various groups interact, there're a lot of positives [signs], there's a lot of. I suppose cross-fertilisation between groups making sure that at the end of the day, that the risk is addressed in the most efficient and best way for the organisation."

The arguments of Respondent [26] are in line with Respondent [9], who similarly emphasises agreement with CsM and ERM alignment.

6.2.4.10 Overall status of CsM alignment with ERM (Q34)

The maturity of alignment refers to the degree of implementation, as a result of the measurement and value of adoption. ERM is, therefore, objective-centric (Hopkin, 2014) as it considers aspects of fostering performance and alignment with an organisation's objectives, respectively their achievement (metric). Table 6-11 examines maturity concentration of the sampled organisations.

Table 6-11 CsM and ERM alignment maturity on sampled organisations

	Mature	Somewhat mature	Slightly mature	Immature	Considered but not yet applied	Not considered
Alignment maturity	*Relative frequency*					
	19.23%	34.62%	19.23%	11.54%	3.85%	11.54%
	Frequency					
	5	9	5	3	1	3

Table 6-11 provides an overview of sampled organisations. 34.62% of respondents score maturity as being *somewhat mature, optimised to organisational needs.* Interestingly, only 19.23% score maturity as reaching full *maturity* (fully optimised). In contrast 19.23% rate their organisations as being *slightly mature, implemented but not fully integrated*. Respondent [12] explains *maturity in more depth*:

> "Very mature in our case. Because any incident that happens on the cyber front or technology front gets reported to the ERM on a monthly basis."

Respondent [20] considers their organisation to be mature because risk appetite statement comprises cyber risk appetite statements as well as other areas of operational risk. Instead, Respondents [8] and [11] describe their organisations' alignment as being somewhat mature, optimised to organisational needs yet not completely optimised to the organisations' needs. In this manner, Respondent [24] states:

> "We are somewhat mature. We're on a journey because of trying to split that into two. It's the maturity in relation of integration of IS and ERM, yes. Holistically, given the domino effect, everyone's starting to change as this as IS comes into ERM and you start connecting the dots. So, everyone's needs to recalibrate."

Immature implementation initiation phase is admitted by Respondent [23]:

> "I would say it is still immature. We are in a transitional phase, but I'm not completely satisfied with our level of implementation."

Respondent [25] explains:

> "We are using some enterprise risk management methodology within our cybersecurity approach. I guess we haven't really considered it, it's not really been attainable yet so… Yes, we [are] neither here nor there."

Each of these respondent's positions make an essential contribution to the appreciation of current practices in financial institutions. By the same token, literature emphasises gaps in managing their exposure to risks in a more strategic manner (employing all efforts in one single scope).

6.2.4.11 Barriers in implementing CsM and ERM alignment (Q35)

Undoubtedly misalignment between strategic objectives and business alignment was researched by many scholars. The strategic alignment advanced to become a more challenging task due to increased impediments (Reynolds and Yetton, 2015). Prior studies have noted the importance of alignment through various research mainstreams but research regarding CsM and ERM alignment remains scarce. Concerns have been raised as outlined in the below Figure 6-27.

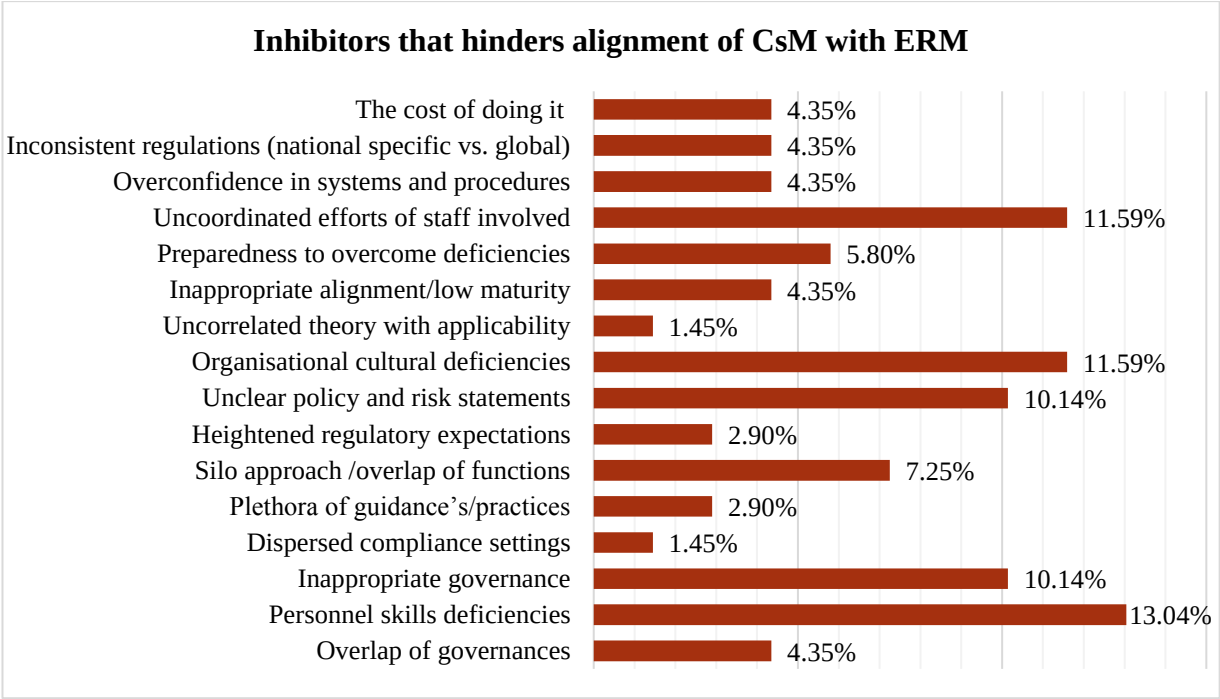


Figure 6-27 Inhibitors that hinders alignment of CsM with ERM

Regarding the question of what hinders alignment, this examination found a key limitation of people-centric association meaning that 24.63% of respondents reported concerns related to skills, culture or lack of coordination. A higher percentage, governance was mentioned by 31.87% of respondents, being the second thematic category to influence misalignment. From Figure 6-27 key themes were further extracted to confirm the association between the role of governance and employees.

Table 6-12 Key themes acknowledged

Theme	Inhibitors		
Governance	Organisation cultural deficiencies	11.59%	
	Inappropriate governance	10.14%	**31.87%**
	Unclear policy and risk statements	10.14%	
Employees	Employees skills deficiencies	13.04%	
	Uncoordinated efforts of staff involved	11.59%	**24.63%**

The main themes identified are related to governance and employees. In view of El-Telbanya and Elragalb (2014), any inhibitors can interrelate with each other and are expected to have a domino effect towards alignment (mentioned *previously as 'systemic'*) (El-Telbanya and Elragalb, 2014; Marotta and McShane, 2018). Thus, El-Telbanya and Elragalb stress caution in the identification of potential variables as a new type of risk.

Despite various research mainstreams (aligning business strategy, IT strategy, IS strategy, ERM strategies, operational alignment, infrastructure and process align), commonalities of inhibitors and drivers have been identified and are in line with literature.

For instance, *employees' skills deficiencies* (13.04%) is alluded for all workstreams (13.04%). Commenting on employees' skills deficiencies, Respondent [1] argues that:

> "I'll say lack of understanding the regulations and how it applies. Because it is often confusion around what is policy, procedure [and] what is the risk of those elements."

As specified in Subsection 4.4.2.2, Chapter Four, a policy is a written statement that illustrates how strategic planning is going to be implemented. It is a set of rules that states the alignment of purpose, objectives, and guidelines to organisational philosophy, strategy, and enabling controls (Chapman, 2011; CESG, 2012). Given the critical role of a policy, it is understandable why it can create confusion.

Another respondent shows consideration for capabilities and performance:

> "Skills, if they don't have the right people trying to implement and align both things then it will never grow. Silo's approach [is] when people work independently, and no one has seen the overall picture and haven't a clear risk appetite statement." (Respondent [21]).

The statement of Respondent [21] corresponds with the beliefs that risk appetite is difficult to be set (Viscelli, Hermanson and Beasley, 2017; PwC, 2018). In addition, Respondent [20] suggests that employees skills, capabilities, and lastly a shortage of employees all hinder alignment:

> "Our biggest challenge, [is] resources…finding the right resource to do the job. Personal skills deficiencies is a big thing."

These findings are in line with Chan and Reich (2007) and Gerow *et al*. (2016), among many others. Initially focused on reimbursements of benefits, the alignment paradigm advanced towards a need of understanding its weaknesses. Luftman (2000) and Henderson and Venkatraman (1990, 1993, 1999) were among a few researchers who proposed to identify factors of misalignment experienced by organisations. Section 3.5 in Chapter Three and Subsection 4.3.3, Chapter Four thoroughly discusses initial research and maturity. Despite extensive research in IT-business alignment, IS-business alignment authors such as El-Telbanya and Elragalb (2014) stress that alignment remains an "unsolved problem".

It should be noted that the vast majority of respondents highlighted various components (dependable of mainstreams) that may hinder proper alignment. Although in some cases alignment was referred to different research mainstreams (IT and RM Respondent [7], IS

and RM Respondent [10], or IS and ERM Respondent [2]), none of them addressed what misalignment means. Such various paths for alignment caused current solutions to be inconsistent and the empirical findings of this research confirm that executives acknowledge some of the inhibitors.

Additionally, *unclear policy and risk statements (disconnected policies)* is another factor that hinders alignment that applies to all workstreams. Respondent [15] illustrates just how vital clarity is:

> "We're fortunate we don't have that lack of clarity, but if we didn't have clarity and also strong management commitment to that, then nobody would want to do this [alignment]. You just see it as it's an overhead – 'I have to do' – and obviously together with that need the right culture. So if the organisational culture is deficient and does not have appreciation for risk, then that will not allow risk management activities to be effectively carried out."

Overall, Respondent [15] provides converging evidence for the relationship (i.e. *organisational cultural deficiencies* with *unclear policy and risk statements* and *strong management commitment*). Preparedness to overcome deficiencies in implementing CsM and ERM alignment depends on the organisation's vision, interpretation, governance engagement, sponsorship/leadership and prioritisation, and the people responsible for the alignment. Some participants express the belief that resistance to change or non-acceptance of ERM (parallel views with Prioteasa and Ciocoiu, 2017; Merhi and Ahluwalia, 2018), and the cost of doing so are among inhibiting factors, (Respondent [9], Respondent [11], and Respondent [14]).

6.2.4.12 Fulfilment of strategic alignment (Q36)

Deconstructing previous research findings that corroborate alignment purpose, cross-functional responsibilities, benefits, inhibitors, current maturity, credence, mechanisms in place, translation, and alignment theoretical antecedents support the conceptual premises that fulfilment of strategic alignment is achievable. Translating strategic objectives into practice and the avoidance of parallel activities (duplication) are among many factors that can help an organisation become more agile and aligned.

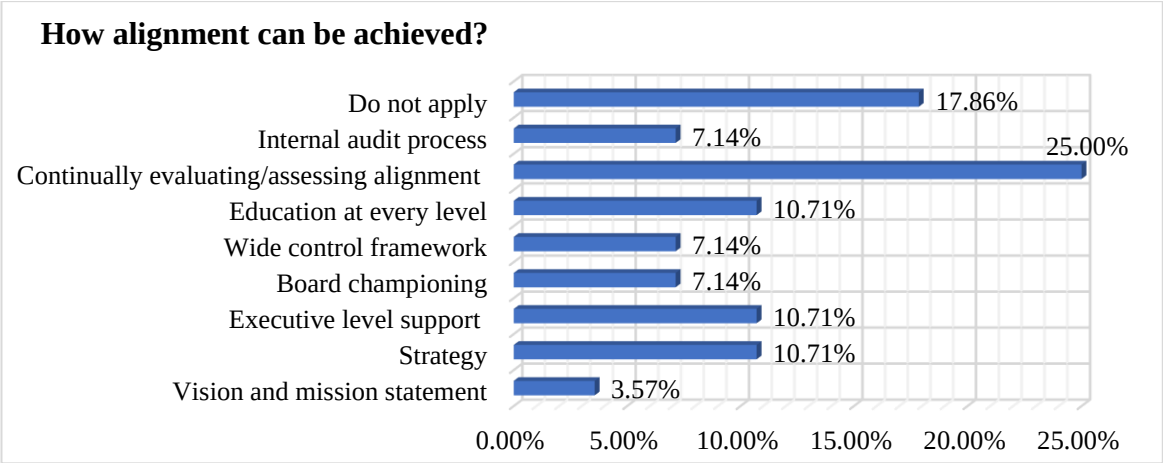


Figure 6-28 Key drivers for achieving alignment of CsM with ERM

Figure 6-28 above presents five main key drivers for achieving alignment. Findings suggest *continually evaluating/assessing alignment* (25.00%) is the main driver, followed by recognition for *strategy* contribution (10.71%), *education at every level* (10.71%), and *executive-level support* (10.71%). However, 17.86% of respondents' state that alignment *does not apply* (17.86%).

Continually evaluating/assessing alignment is recommended by Respondents [7] and [21], who encourage the use of policies as metrics and measurements accordingly. Audit challenge against objectives and baseline and strategic requirements, self-assessment, direct and control verification, and perhaps framework can all be used as a metrics. This view was echoed by Respondent [3], who suggested that:

> "I think you need to identify a quantifiable baseline to defined certain risks. I think you start with predefining the risk taxonomy and you work up to strategic risk from that between risk taxonomy and you work down the operational risks. That scale that measurable layer of risk."

Moving from assessment, strategy (10.71%) was another key factor mentioned by respondents. Respondent [23] thinks that effective alignment is tied by centralising strategy and communicating it at the level of the board of directors. In this view, Respondent [8] states:

> "Well…, we don't just write the strategy document and have a lovely cheese and wine reception. We actually follow up. We take our cybersecurity strategy that has been aligned and we would develop the programme that would deliver that strategy for us. And then we reassess every six months to verify if it is still aligned with the business strategy."

This needs *executive level support.* It was felt that executive level support is the only way strategic alignment can be achieved (believed by Respondent [4]), while Respondent [18] considered that:

> "The first and the most important thing is to work on need and try to show the value by having a very close engagement with the executives. The IT leaders have to work very closely with the business leaders for each critical business process functions and the board has to also champion it."

A variety of perspectives was expressed regarding what helps achieve alignment. Four broad themes emerged from the analysis: *strategy, executive-level support, assessment, and education.* The four dimensions of alignment are dependable, respectively intellectual (strategic), structural, operational, and social. These findings advocate a similar view discussed in Subsection 4.4.3, Chapter Four. The majority of prior research has advocated the use of one or two dimensions, or a mixture of them. Evidence shows that all four dimensions are interrelated, influencing effectiveness of alignment. In the light of reported linkage of alignment dimensions, it is conceivable that implementation prescribes the use of intellectual (strategic), structural, operational and social approaches, hence them all being interrelated. Thus, empirical findings shed new light on industry practices.

6.2.4.13 Assessment of alignment (Q37)

Notwithstanding, assessment of alignment comprises in measurement against risk appetite, policies, and risk and control assessment as comparable baselines between current capabilities, performance, and objectives (Salaheddine and Ilias, 2017). Looking at intrinsic risks across organisations and at-risk resiliency, the need to continuously optimise alignment is substantiated.

Table 6-13 Alignment assessment key elements

Response	Relative frequency	Frequency
RM methodology	7.69%	2
Framework	3.85%	1
Annual questionnaire	3.85%	1
Reduction in the number of incidents	3.85%	1
Capability maturity model	3.85%	1
Audit	19.23%	5
Metrics (KRI, KPI)	15.38%	4
Measured against risk appetite	3.85%	1
Risk and control assessment	11.54%	3
Not considered	11.54%	3
Do not apply	15.38%	4
Total	100%	26

Among key drivers reported to support alignment, *audit* was the highest value (19.23%). An emphasis on audit was further advocated by Respondent [9]:

> "I think that if you really want to get a clear picture [of] how well is your risk governance, your information security is mapped together, [then] and the only way to do that would be to hire an external auditor."

However, in contrast with empirical findings, the literature reflect mainly a research mainstream of IS and RM alignment. If referring to Deming's PDCA cycle method (plan-do-check-act) in assessing alignment, 'check' is a general characteristic of available theoretical maturity frameworks (Salaheddine and Ilias, 2017). The PDCA cycle is a continuous effort to re-align risk oversight. Respondent [11] indicates that:

> "Every time [there] is a re-alignment. There is always an ongoing monitoring and full assessment to make sure that it works. So, in that regard, they use performance as the base level and do the re-alignment and then remeasure the business efficiency, compares with the baseline of what we were doing at the beginning and then see if the alignment has optimised the effect of line to the business."

Thus, re-alignment depends on *metrics*. 15.38% indicated that metrics are a scoring performance mechanism against the various targets. For instance, Respondent [12] describes examples of the scoring mechanism on a scale of one to ten, with traffic light methods, or questionnaires. On the other hand, Respondent [24] suggests that a scoring mechanism/metric could be anything.

One unanticipated finding was an endorsement for a specific model for monitoring the effectiveness of internal control for the financial industry. Respondents [2], [19], [21], [22], and [24] endorsed the Three Lines of Defence Model (referred to as the 8th EU Company Law Directive). Similarly, within Section 3.2, Chapter Three, maturity assessment has been referred to as measuring maturity of both implementation performance and compliance. Conversely, 15.38% of respondents say that they do not apply, and other respondents do not even consider such a thing (11.54%); suggesting a lack of alignment enforcement and once again emphasising the research gap.

6.2.4.14 Experts recommendations in implementing CsM alignment with ERM (Q38)

Returning to the scope of this research, Question 38 is to formulate a link between the initial views of respondents and current research in order to facilitate a general reiteration of the respondents' views in this context. Table 6-14 illustrates 16 main themes identified.

Table 6-14 Overall recommendations for CsM alignment with ERM

Themes	Words relative frequency	Frequency
Set robust governance	2.63%	1
Clear strategy and objective	2.63%	1
Talking with stakeholders	2.63%	1
Risk assessment	7.89%	3
Risk ownership	2.63%	1
Communication	18.42%	7
Prioritisation of risks	18.42%	7
Organisational culture value	7.89%	3
Education and awareness	7.89%	3
Understand RM	7.89%	3
Having the right skills set	2.63%	1
Budget	2.63%	1
No company does well	2.63%	1
Reviewing frameworks	7.89%	3
Standardisation of risk management	2.63%	1
Incident scenario	2.63%	1
Themes=16	=100%	T=38

Among the main recommendations, communication (18.42%) and prioritisation of risks (18.42%) received the most consideration. To accomplish these objectives, education and awareness are understood to be significant factors for enhancing alignment. The additional views of Respondents [5] and [20] provide evidence that senior managers understand the implication of the human-element factor that eventually requires education and training. Moreover, the results confirm that this is a good choice when combined with clear strategic goals, as evoked by Respondent [17]:

> "Determine the framework and methodology to be used. Train the organisation in a way so that it will establish a common language. Set up a structure of risk management meetings. Risk manager to run/facilitate periodic meetings. Path to escalate risk."

Respondent [2] further recommends:

> "I would say to instil risk culture in everyone from their organisation, every single employee, everyone should be made a risk manager. Risk shouldn't be limited to RM functions, but we have to create these cultures of risk awareness across all staff."

Returning to RM applicability, reviewing frameworks was said to be essential by Respondents [3], [25] and [16]. Respondent [16] advocates that:

> "So, I would say framework is number one, appropriate standards and policies in place, ensuring that appropriate controls [are] in place to mitigate inherent risks that

> are identified for the businesses. Communication and appropriate governance [in place], and what I mean by that is adequately reporting and escalating issues, so they come up to appropriate levels for senior management attention."

Ensuring the support of board and executive management (Respondents [9] and [38]), having a strong tone from the top and having a mapping mechanism both support business resilience, championing communication and strategic prioritisation of risks.

6.2.4.15 Risk governance predictions/forecasts (Q39)

Lastly, Question 39 challenges respondents' views on risk governance forecasts within their organisation over the next five years. A few main themes have been identified, as illustrated below in Figure 6-29.

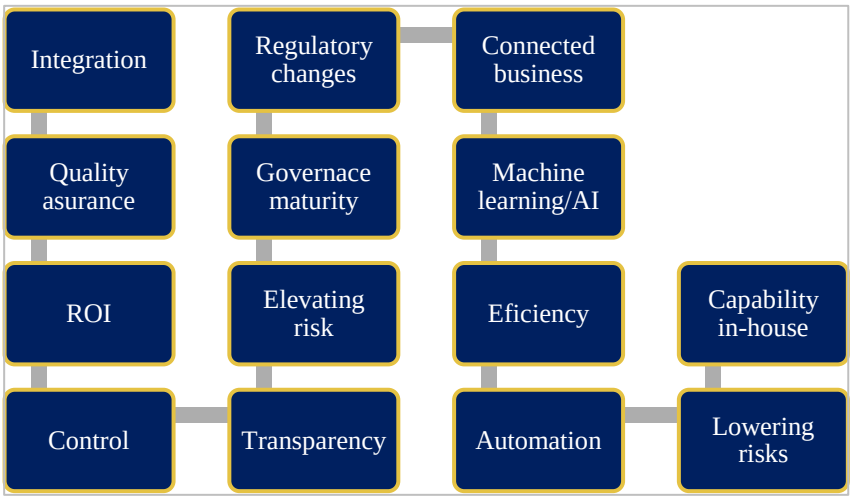


Figure 6-29 Risk governance predictions main themes

Some organisations have a much more mature programme, yet alignment is predicted as being mature, thus further helping organisations control and mitigate risks. Integration of CsM with ERM is predicted to become more integrated and efficient as stated by Respondents [11], [15], [19], and [2]. This entails the prediction of increasing awareness among both users and organisations, as advocated by Respondents [20] and [24]. Positive prediction in changing and improving risk oversight culture is emphasised by Respondent [7]:

> "Perhaps in terms of culture shift, we plan to make some changes to ensure enterprise-wide awareness and embed it at all levels. Also, automation of functions that quantifies the risks to ensure a faster deployment of resources to protect the organisation."

A further question is whether increased regulatory pressure will entail advancement in risk practices (Respondents [23] and [8]).

Another promising line was associated with standards/frameworks driven initiatives Respondent [4] believes that:

> "Within my organisation,I think we'll see more and more departments brought from the Board to the usual corporate risk management framework. So, we have this management risk function within the company that sets the direction for the whole company. Each department has its own local implementation of that corporate framework, but we haven't completed the role out for all departments. So what we would do over time is to have more departments for fixing that framework. And they will be adopting, hopefully, the same framework that has been set by the top."

Respondent [24] claims that more and more automation and machine learning will fill the gaps in security, making organisations more agile. In support, Respondent [5] states:

> "I think most companies will continue to invest more in security, in people, in infrastructure, in automation."

However, in contrast, Respondent [2] believes it will not be always possible to automate everything. In leveraging innovation through automation, Respondent [21] argues that:

> "Artificial intelligence (AI) - they are going to be able to do a lot of the basic jobs that a risk manager does right now. I see that the role of a risk manager as a human will be to collate [by] all those conclusions that the AI is getting. It will change the risk management industry I think."

No doubt proliferation of various technologies may lead to even more threats, which preside an advancement of adversarial sophistication that could trigger further risk oversight maturity, thus connecting business capabilities and fostering the development of in-house capabilities.

6.3 Conclusion

This chapter was designed to determine the rationale of CsM with ERM alignment within the financial industry in the context of empirical findings. Grounded in the research question "What are the key issues that impede the alignment process in the financial industry regarding CsM and ERM", this chapter collected and analysed empirical data to inquire about current maturity and likely solutions. A questionnaire was designed to unfold data of ERM, CsM and Alignment understandings from senior executives to ascertain research validation. Firstly, an analysis was conducted, focusing on respondents' and organisations' profiles and aiming to comprehend in much detail the nature of challenges faced by the financial industry in which the respondents operate. Secondly, this chapter delved into enterprise risk oversight, seeking to determine an organisation's maturity in order to

substantiate the research rationale. Thirdly, it researched the cyber risk oversight maturity. Lastly and above all, it analysed the strategic alignment of CsM with ERM.

Qualitative data analysed in this chapter indicates that CsM, ERM and strategic alignment have key determinants/drivers as well as inhibitors specific to the financial industry. The format of the questions explores positions regarding preparation against risks, the velocity of risks, accountability for risk oversight, governance maturity, and willingness to accept alignment. Research findings determine that each mainstream (ERM, CsM and Alignment) encounters various types of challenges and stages of in implementation.

In this regard, systematic steps were taken to explore the three paradigms to ensure appropriate valuation. Initially, from a total of 39 questions, the first nine appraised respondents and organisation profiles, while further themes explored ERM (7 questions), CsM (8 questions), and strategic alignment of CsM and ERM (15 questions). Through the content of the chapter, respondents report an interest in CsM and ERM alignment. Furthermore, an essential finding of the chapter was that respondent's responses voiced clear views that support implementation of alignment for CsM and ERM. Nevertheless, respondents seemed concerned that organisations lack a unified mechanism by which they can identify, assess, and mitigate both cyber and enterprise risks. On the other hand, the overall status of CsM alignment with ERM has been identified as being immature; hence existing practices relying on antecedents of alignment (business strategy, IT, IS, RM).

Findings of this chapter evidence agreement between the interviews' findings and existing research identified in Chapters Two and Three. Overall, it can be concluded, based on empirical evidence, that the results of this chapter support the aims of this research. Furthermore, findings actively support the research aim of developing a Strategic ERM Alignment Framework for addressing key shortcomings. Heightening the arguments of literature with empirical evidence, it has been found that the role of RM can no longer act as a separate and reactive function. Besides, due to the value proposition, respondents reported an interest in CsM and ERM alignment; a fact which reinforces the *CsM—ERM Strategic Alignment Framework* value proposition of effective and holistic risk control.

Returning to the question posed at the beginning of this chapter, "What are the key issues that impede the alignment process in the financial industry regarding CsM and ERM", it is now possible to attain the relationship between variables: dependables and derivations condition the theoretical assertion of the need for a strategic alignment between CsM and

ERM and key organisational dimensions. Drawing on these findings, this chapter streamlines a base for the next two chapters and an extension for the research framework. Furthermore, the next chapter offers foresight into research value and the findings implication in terms of the research framework. This will be followed by an additional chapter (Conclusions) that concur with main the findings, the research proposal, and the research's position in current theoretical context.

7. Chapter Seven: Discussion

7.1 Introduction

While the previous chapter reported findings by using the content analysis technique, this chapter thematically explores how the perceptions of industry practitioners revolve around aggregating answers to the research questions. The research findings identified in Chapter Six are further analysed using thematic analysis. Additionally, the findings are compared to the existing bodies of literature. Accordingly, the focus of discussion moves from 'description' to 'interpretation' of the research findings (Vaismoradi *et al.,* 2013). The chapter explores the phenomenon antecedents, determinants, barriers, readiness and capacity to sustain risk governance as a core competency for sustainability and efficiency and avoiding ripple effects. It uses thematic analysis to explore patterns, themes, uncertainties and discrepancies and is focussed on the research questions:

- Research Question 1: Why does a strategic alignment of CsM and ERM sustain a financial business in the long term?
- Research Question 2: What are the key issues that impede the alignment process in the financial industry regarding CsM and ERM?
- Research Question 3: How are theory, practice and regulation direction applied regarding the current alignment of CsM and ERM within the financial industry?
- Research Question 4: What effects have the implementation of the new framework?

Following the research questions, this chapter discusses the empirical findings and is structured as follows. The first section offers a brief review of thematic analysis implications (Section 7.1). Section 7.2, analyses themes that identify main threads across the whole set of interviews (Vaismoradi *et al*., 2013). Section 7.3 presents the research findings' implications and Section 7.4 outlines a revised version of the conceptual framework, distilled to leverage a new governance framework (both risk control and oversight) that aligns CsM with ERM. Lastly, limitations (Subsection 7.4.2) and conclusion (Section 7.5) provide a synthesis of findings, demonstrating how the questions of this research were fulfilled.

7.2 Thematic analysis of research findings

Relying on the initial findings of content analysis from Chapter Six (descriptive), further, the thematic approach develops by systematically and methodologically expanding the interpretation of results that entail common codes (Nowell *et al*., 2017). Nonetheless, a

thematic analysis implies careful consideration for identification of words frequency, themes, trends, ideas (Guest, MacQueen and Namey, 2011). Moving to an interpretative phase, such analysis looks beyond word counting, and it aims to understand the focus of groups ideas (codes) in themes (Guest, MacQueen and Namey, 2011). Nevertheless, the initial codes that emerged from the interview questions (39 questions = 39 codes) were grouped into four main themes. However, a reconsideration for reframing the initially identified themes was undertaken and so the first theme, respondent and organisation profile, was deemed irrelevant at this phase and therefore remains to be used as an indication. As a result, the remaining three themes were decompounded in other sub-themes, apprehended in a level two thematic analysis. Henceforth content analysis represented Level One of coding research findings, the initial synthesises was undertaken with NVivo, a qualitative software. NVivo provided support in the first phase to organise systematic views, shown in a mind-map (Guest, MacQueen and Namey, 2011; Ciesielska and Jemielniak, 2017). Accordingly, the Researcher conveyed core patterns and identifying patterns, similarities, differences, and connections in the context of the research questions (Maguire and Delahunt, 2017). However as indicated by Clarke and Brown (2013), as thematic analysis means more than coding, and thus extracting themes from previous interview questions seemed insufficient. The format may only lead to summarised data (descriptive coding) instead of synthesised and examined data. Therefore, the Researcher also applied her own judgement in organising the themes while considering any significance outlined by respondents. For clarity, thematic analysis is a general and abstract concept while a code is specific and related to a specific issue (Williamson and Whittaker, 2017); thus, a theme contains at least two codes. Therefore, initial coding themes (Level One) were distinguished and revised accordingly. Table 7-1 captures synthesised interview findings corroborated in codes respectively and a codebook from which further sub-themes are extracted (Level Two). Such an approach is defined by Guest, MacQueen and Namey (2011) as an 'applied thematic analysis' technique.

Table 7-1 Level One (content analysis) versus Level Two (thematic analysis)

	Level One (Chapter Six) Initial codes encoded from interview questions (Codebook)	**Level Two** (Chapter Seven) Sub-themes and categories generated
Theme 1	**Enterprise Risk Oversight Maturity**	
Q10	Preparation against risks	**Sub-theme 1: ERM Baseline expectations** Category One: ERM determinants • Strategic governance • Differentiation-centric • Risk resiliency
Q11	Velocity of risks	
Q12	Department responsible	
Q13	Risk governance maturity	
Q14	Risk governance role	
Q15	Main determinants/drivers	

Q16	Main inhibitors	Category Two: ERM reimbursement • Internally • Externally Category Two: ERM inhibitors • Resources • Direction • Capability • Pressure Category Three: ERM readiness • Risk Oversight
Theme 2	**Cyber Risk Oversight Maturity**	
Q17 Q18 Q19 Q20 Q21 Q22 Q23 Q24	Department responsible Main determinants Main inhibitors Cyber incident handling Unwanted effects Industry framework ROI Board expectations	**Sub-theme 2: CsM Baseline expectations** Category One: CsM determinants • Internal • External Category Two: CsM Reimbursement • Performance Category Three: CsM Inhibitors • People-centric • Strategic-centric Category Four: CsM Readiness
Theme 3	**Strategic Alignment**	
Q25 Q26 Q27 Q28 Q29 Q30 Q31 Q32 Q33 Q34 Q35 Q36 Q37 Q38 Q39	Department communication Risk handling Practical alignment Aligned strategies Unified strategy mechanism Strategic alignment Alignment benefits Alignment applicability Alignment feasibility Alignment maturity Alignment inhibitors Alignment achievement Alignment assessment Implementation recommendations Practice forecast	**Sub-theme 3: Establishment of strategic directions** Category One: Strategic Alignment Reimbursement • Determination • Benefits • Potential reimbursements Category Two: Inhibitors • Governance • Employees Category Three: Alignment Readiness • Maturity Category Four: Prospect • Potential • Alignment fulfilment

Table 7-1 depicts a thematic map of research findings with main themes initially identified in Chapter Six, respectively Enterprise Risk Oversight Maturity (1), Cyber Risk Oversight Maturity (2), and Strategic Alignment (3). An emphasis of sub-themes and categories are further delved into in order to establish implications. Consequently, the sections below discuss the research findings in context of additional theoretical contribution of literature.

7.2.1 Theme 1: Enterprise risk oversight maturity

This theme partially addresses the research question of why ERM sustains a financial business in the long-term (Research Question 1). The sub-themes underpin determinants, inhibitors, benefits and consequences of implementing ERM principles and helps to further

explore the importance of enterprise risk oversight maturity further. An overview of each sub-theme is described below.

7.2.1.1 Sub-theme 1: ERM baseline expectations

This sub-theme emphasises what the baseline expectations are, so ERM strengthens the value of strategy and objectives across an organisation (Fraser and Simkins, 2016). The relevance of each sub-theme is conceived accordingly with the empirical results.

Category One: ERM determinants

Research findings conceive that the main determinant factors to implement ERM are strategic governance, differentiation-centric, and risk resiliency. Most often, literature refers to determinants as the benefits of adopting ERM principles (Zéghal and El Aoun, 2016). However, for the purpose of this research, the term 'determinants' is used interchangeably with 'benefits'.

Table 7-2 ERM determinants

Category One: ERM determinants	
a) Strategic governance	Governance Strategy Prioritisation
b) Differentiation-centric	Competitive advantage Value
c) Risk resiliency	Control Compliance Knowledge

a) <u>Strategic governance</u> (45.16%)

i. **Governance** was reported by 17.74% of respondents as being a determinant of ERM. These results support the view that the role of governance is essential for achieving organisational goals and strategy (Gheorghe, 2011). It has been noted that the relevance of governance is supported by current findings and in line with both academics' and practitioners' views. Evidence of literature argues that the role of governance became even more critical after regulator's intervention post-effects of GFC of 2008 and corporate scandals. Organisational failures evidenced weakness in the risk governance of certain organisations (Cohen, Krishnamoorthy and Wright, 2017; McShane, 2018; Rubino, 2018). Failures in implementing adequate and sustainable solutions to address risk have demanded organisations to change their attitude and behaviour to risks and incorporate RM into overall organisational governance planning and thus strengthen their

capability to identify and mitigate risks (McShane, 2018; Viscelli, Hermanson and Beasley, 2018). As a result, risk control function became insufficient and shifted to governance principle so as to ensure that ERM addresses all portfolios of risk, ensuring accountability, delegated responsibility, and well-defined structure regarding how decisions are taken (Dabari, Kwaji and Ghazali, 2017; McShane, 2018). Likewise, PwC (2018a) brings into focus the role of governance as a core concept to link ERM with organisational strategy, governing both risk oversight and in-depth management/control of risk, and harnessing governance. Another line of thought on governance demonstrates that it incorporates values, beliefs, rules, and practices, which represent constructs of Institutional Theory (see Subsection 4.2.2, Chapter 4) (Aguilera, Judge and Terjesen, 2018). Moreover, Aguilera, Judge, and Terjesen (2018) emphasise that prevailing literature focuses more on successful risk governance and less on deviance from governance.

Consequently, governance is a strategic approach that controls and directs an organisation towards achieving its strategic goals (Gheorghe, 2011) as well as ensuring that the right mechanism is in place (Nason and Fleming, 2018). Literature highlights that risk governance is applied through policies and procedures that delegate accountability, define overall structure, and allocate resources for addressing risks (Gheorghe, 2011). Thus, the strength of such an approach is that it sets the 'tone'; it dictates direction and ensures that risk control and oversight are understood and continuously reinforced (COSO, 2017). Therefore, governance defines, incorporates, and delegates risk control, risk oversight, and strategic risk planning (strategies, objectives, appetite, planning, structure, processes, capabilities, competencies, and risk culture) to serve organisational mission and vision in a unified manner (Althonayan, Matin and Andronache, 2018). This view is also emphasised by Respondents [24] and [25] in the initial research findings; and thus, governance is an archway that bridges departmental silos into a central risk governance tool (Frigo and Anderson, 2011). In short, the strength of risk governance is that it translates strategy into actions and orchestrate its holistic applicability to cross-functional structures, rules, processes, culture, accountability, and necessary control to govern organisational objective achievement (Frigo and Anderson, 2011).

ii. **Prioritisation** of risks refers to effective strategic prioritisation that is driven by organisational strategy that states the risk appetite and compiles risk assessment of top priorities (Lam, 2017; Iswajuni, Manasikana and Soetedjo, 2018). With reference to the research findings identified, prioritisation was highlighted to be a determinant of ERM in the proportion of 22.58%. Likewise, previous studies often suggested that for strategic and operational efficiency, prioritisation of risks is expected to be undertaken out of departments' self-interest. This means that prioritisation is expected to be made based on severity in an enterprise-wide context and in accordance with the organisation's overall risk appetite, rather than in the siloed perception of each department (COSO, 2017). In short, effective ERM sustains and oversees the management of priorities in managing risks (EY, 2017). However, the low levels observed in this investigation (22.58%) may be explained by the fact that ERM determinants are multiple (previously delineated in Table 2-1, Section 2.4, Chapter Two).

b) Differentiation-centric (11.28%)

Overseeing performance constitutes in view of COSO (2017) integration of ERM with business strategy. ISO 19011:2018 (BSI, 2018b) presents the view that performance is a 'measurable result'. However, the differentiation-centric category comprises of two elements, competitive advantage and value creation that demonstrate ERM differentiation through performance effects.

i. **Competitive advantage** was identified to be a differentiation factor brought about by ERM implementation in percentage of 4.84%. This finding is in line with Yang, Ishtiaq and Anwar (2018), which confirms that ERM competitive advantage is associated with performance. This also agrees with earlier findings of literature review (see Section 2.8, Chapter 2), which demonstrate ERM's influence over the long-term. This is consistent with the industry's view that outlines the capabilities of an organisation as being the differentiation factor for gaining the competitive advantage (KPMG, 2017b; PwC, 2018). Consistent with prior literature, research findings confirm that ERM positively influences the achievement of organisational objectives (Roslan *et al.*, 2017; Shad *et al.*, 2018; Farrel and Gallagher, 2019). Furthermore, the effect of performance determines a competitive advantage that produces value (Farrel and Gallagher, 2019). Additionally, a competitive advantage can represent a 'measurement technique' of valuating the impact effectiveness of ERM implementation (Roslan *et al*., 2017; Shad *et al*., 2018).

ii. **Value** was identified to be the second factor of ERM differentiation. The empirical findings highlight that ERM performance leads to **value creation** (6.44%). This finding broadly supports the view of prior literature which calls into question value as one of the roles of ERM, anticipating that impact of ERM performance leads to value creation/proposition for an organisation (Lechner and Gatzert, 2017; Shad *et al*., 2018; Silva, da Silva and Chan, 2019; Iswajuni, Manasikana and Soetedjo, 2018; Li, 2018). In the recent years, the valuation implications of ERM have been recognised as an approach that helps create, preserve, and maximise shareholder value (KPMG, 2017b; Majdalawieh and Gammack, 2017; Bohnert *et al*., 2019; Shad *et al*., 2018; Slagmulder and Devoldere, 2018). Moreover, it provides capabilities of strategic planning to examine, measure, and deter risks continuously (Bohnert *et al*., 2019). ERM's goal is to unify siloed functions into holistic risk governance (Lundqvist and Vilhelmsson, 2016; Farrel and Gallagher, 2019). Hence, governance guides organisational behaviour, both internally and externally and maintains organisational direction when achieving its objectives (BSI, 2018a). Thus, ERM facilitates value creation for an organisation by duplication avoidance, coordination of silos, reduced risks, holistic risk portfolio management, creation of risk transparency for boards supporting decision-making, risk insight insurance, and stronger risk culture and optimisation, and return on investment (ROI), among many others (COSO, 2017; Lechner and Gatzert, 2017; Farrel and Gallagher, 2019). Even so, organisations struggle to extract the entire value that ERM can deliver (PwC, 2018). To ensure that potential risks are limited in affecting the strategy execution and objectives achievement, ERM manages risk under the setting of strategy (PwC, 2018; Viscelli, Hermanson and Beasley, 2017). Thus, the **value** element is contingent with the **strategy** element.

To conclude, the research findings assert two main strands: competitive advantage and value creation. A possible explanation for these results may be because effective ERM aligns with organisational strategy and thus enables performance (COSO, 2017). Likewise, BSI (2018a) emphasises value creation and protection. Consequently, it leads to a competitive advantage which in the end brings value to the organisation as well as maturity. It can, therefore, be assumed that once performance is achieved through ERM, competitive advantage and value creation are the projected outcome, determining an effective and sustainable ERM. Therefore, the Researcher assumes that a **performance risk chain** has positive ripple

effects: *effectiveness ─ resiliency ─ value creation ─ competitive advantage ─ compliance ─ risk strategy sustainability ─ risk foresight ─ organisational objectives achievement.*

Resiliency (43.56%)

In addition to benefits as a performance enhancement and strategic governance, ERM is also implemented for resiliency achievement. Research findings indicated that resiliency is among ERM's determinants. In addition to the provision of resiliency, literature associates the strategic approach with agility (Slagmulder and Devoldere, 2018). This means that organisations which integrate ERM principles in their overall strategy become more agile in dealing with risk. To follow, the category of resilience was identified as having three main elements: control, compliance, and knowledge.

i. **Control** is the first category of resiliency sub-theme. Risk control function was identified as having a frequency of 14.52%. Additionally, the evidence confirmed that ERM as a risk control function is expected to be a function with shared responsibility. This finding demonstrates that ERM is perceived through the lenses of traditional RM, hence ERM comprising of both control and strategic risk oversight function.

ii. **Compliance** requirement relates to mandatory regulatory guidelines, and industry-specific refers to voluntary actions that advocate the adoption of ERM. Compliance reimbursement was indicated in percentage of 14.52%. Therefore, the GFC of 2008 determines reconsideration of the siloed practice of the traditional RM approach. Financial institutions in the USA were required to demonstrate higher due diligence (Whitman, 2015; Althonayan, Matin and Andronache, 2018). Either regulators, rating agencies, public authorities, or industry norms and compliance for implementing ERM pointed towards an increased expectation for integrated management of risks (Boromiley *et al.*, 2015; Viscelli, Hermanson and Beasley, 2017; Anton, 2018). Due to increased expectations for risk governance, ERM is perceived by some as an assurance function (Viscelli, Hermanson and Beasley, 2017) (for further details see Section 2.4, Chapter Two).

iii. **Knowledge** refers to cross-domain risk knowledge within an organisation, respectively departments. Similar to the control and compliance category, it registered an identical percentage of 14.52%. These findings validate those of

earlier studies, which articulated the importance of cross-domain risk knowledge as a shared knowledge for risk functions/business units (Majdalawieh and Gammack, 2017). Additionally, Kerstin, Simone, and Nicole (2014) understand that cross-domain knowledge can be open to interpretation, and thus it is expected that for an effective ERM, a knowledge should be agreed; things such as risk glossary, definitions, risk assessment, RM methodology, and the significance of organisational risk shall be under a holistic guideline (Kerstin, Simone and Nicole, 2014).

In short, the control, compliance, and knowledge categories demonstrate that in practice there is a tendency towards strategy governance, performance, differentiation centric, and risk resiliency hardening. Likewise, COSO's definition is confirmatory to some degree with research findings and compounds many elements altogether:

> "The culture, capabilities, and practices, integrated with strategy-setting and performance, that organisations rely on to manage risk in creating, preserving, and realising value" (COSO, 2017).

Furthermore, the next category looks at ERM inhibitors that impede either adoption and/or implementation.

Category Two: ERM reimbursement

This category compounds the rationale of implementing ERM, respectively the positive reimbursement as an effect of implementation.

Table 7-3 ERM Reimbursement

Category Two: ERM reimbursement		
a)	*Internally*	Culture Shareholders' requirements
b)	*Externally*	Regulatory requirements Competition

a) **Internally** (42.87%)

i. **Culture** (8.57%) was found to be a direct effect on execution of ERM due to potential positive effect in shaping the organisational risk behaviours as well as positively impacting decisions (Selamat and Ibrahim, 2018). In the same vein, COSO 2016 defines ERM as being dependent on "culture, capabilities, and practices" (COSO, 2016; Bohnert *et al*., 2019). Additionally, the risk awareness

was found as an additional indirect component of culture being influential on organisational effectiveness (Braumann, 2018).

ii. **Shareholders' requirements** is indicated by 7.14% o respondents as being an ERM effect that fulfils shareholders requirements, ensuring capture and enhancement of shareholder value (Majdalawieh and Gammack, 2017; Saedi *et al*., 2018).

b) **Externally** (57.15%)

i. Regulatory requirements were found to be a significant reimbursement (30.00%) when organisations discern proper practice for risk oversight. Moreover, thus, this finding is in line with prior research that articulate that ERM seems 'induced' by regulations because it is assumed that governance failures can have ripple effects on other industries (Kauspadiene *et al*., 2017; Sax and Andersen, 2018).

ii. Competition (10.00%) was identified to be a second external reimbursement for organisations. Apart from driving good practices, the financial landscape complexity dynamic drives implementing ERM which creates assurance for due diligence.

Category Three: ERM inhibitors

This category implies factors that inhibit or undermine the achievement of organisational strategy, organisational robustness, and the sustainability of ERM (EY, 2017). The main categories identified are referring to internal inhibitors (resources, direction, capability) and external pressure. Internal and external inhibitors can determine alterations in how an organisation manages risks.

Table 7-4 ERM inhibitors

Category Two: ERM inhibitors		
Internal	**c) *Resources***	Cost Data and Information People Skills
	d) *Direction*	Strategy Leadership
	e) ***Capability***	Maturity Culture
External	**f) *Pressure***	Risks and Threats Standardised Practice Regulations

Internal pressure (42.87%)

a) **Recourses**

In the expectation of resiliency, performance, and competitive advantage, most organisations are driven to invest tangible and intangible resources (Yang, Ishtiaq and Anwar, 2018). However, a limitation or lack of resources is an inhibitor of ERM.

i. **Cost** was evidenced by findings and relates to the implied costs of implementing and maintaining ERM. Respondents have stated that cost can inhibit risk practices. Underpinning a cost-effective investment for security was a general agreement among respondents, even though some respondents argued that receiving the expected investment was not always in balance with organisational needs. Comparing with prior research, literature has referred to additional aspects of cost, for example, an interest in gaining more return by lowering compliance costs and an opportunity to have the right risk oversight strategy in place (Mensah and Gottwald, 2016). Hereafter ERM plays an important role in business decisions, because it aims to avoid loss as well as optimise and even reduce cost. Protiviti's (2018) survey has similar findings when referring to the cost of implementing risk control, and it additionally referred to cost regarding compliance, marginal cost, and maintenance cost. In contrast, this research found limited evidence for compliance costs, converging mainly to the cost of implementation.

ii. **Data and Information** refers to the quality of data as well as communicating information are challenging when department lack of collaboration and sharing information (Kerstin, Simone and Nicole, 2014). The impact of data/information quality is an outcome enunciated by research findings (7.04%). Commenting on poor, incorrect, or incomplete data as inhibitors of ERM, several authors (Viscelli, Hermanson and Beasley, 2017) articulate that such drawback can affect decision-making. Even so, the role of ERM is to deliver enhanced and improved information for strategic decisions due to its capability to view risks holistically (Hopkins, 2018). Another finding that emerged from the research findings is reporting. Likewise, the guide of ISO 31000: 2018 emphasises the importance of quality in reporting as a pillar in placing oversight and controls (BSI, 2018a). For instance, lack of some principles as integrated, continual, customised, or

inclusive communication may suggest that value creation of information is unreachable and is incompletely addressed (BSI, 2018a).

iii. **People** represent another key element in deploying decisions related to risks (Craig, 2018) and have been reported by respondents as being an inhibitor in deploying ERM. Regardless of preparation, training, or background, it has been reported that often failures are dependable on people. These findings are in line with literature, which specifies that people-related risks are intentionally or intentionally related to people's actions (Craig, 2018). Accordingly, people-related risk covers lines of responsibility, accountability, and risk knowledge; all of which are required for synchronising various elements such as people with processes and processes and tools (Majdalawieh and Gammack, 2017). People-related risks are a common challenge for organisations. Firstly, a risk is when allocating people as a resource (ISO 31000: 2018) and secondly, when the risk of loss is due to the way individuals perceive severity of risks as well as how decisions or non-decisions are made by individuals (Blacker and McConnell, 2015). Therefore, people as a factor can inhibit the effectiveness of ERM, either by an unlawful, unscrupulous, inappropriate, or unsuitable line of actions in their daily activities. This makes reference again to well-known cases of GFC of 2008 when decisions were influenced by cognitive biases, over-confidence, or negligence, and lead to substantial losses (Blacker and McConnell, 2015). Given this example, risk perception is demonstrated to be different for most individuals; and thus, decisions related to risks are often based on individual's judgement and understanding of risks, respectively perceived level of risk (World Business Council for Sustainable Development, 2017).

iv. **Skills** refer to a lack of in-house skills or limited skills sufficient for fulfilling requirements of risk functions. The evidence demonstrated that 23.94% of inhibitors are people-centric in terms of capabilities (skills set, lack of education, communication, culture). Briefly, the respondents outlined that a lack of skills set affects the ability to understand what risks are and their consequences, thus affecting the deployment of a suitable solution. Given this orientation, a lack of skilled employees adds additional difficulties for organisations in deploying appropriate security risk control and risk oversight and consequently leads to difficulties in reaching ERM effectiveness and maturity (Zhao, Hwang and Low, 2015).

b) Direction

i. **Strategy** was reported by respondents as being another inhibitor (4.23%). Evidence shows that a lack of appropriate strategy influences the overall direction of an organisation. Strategy is a concept that refers to a business strategy, and it delimitates the purpose and intent of what an organisation intends to reach (Hopkin, 2018). It is a written statement of intent and how that intention shall be reached through planning (Kaplan and Norton, 2003). ERM plays an essential role in strategy achievement hence its principles being governed by enterprise-wide alignment ensuring achievement of objectives in pursuit of strategy, thus being strategy-execution focused (COSO, 2017; Viscelli, Hermanson and Beasley, 2018; Slagmulder and Devoldere, 2018).

ii. **Leadership** refers to senior management support for coordinating and integrating arrangements to manage risks (BSI, 2018a). To accomplish leadership, levels of direction, control, and guidance for managing risks are deployed through authority, responsibility, and accountability (BSI, 2018a). By this means leadership also emphasises the commitment of executives in supporting ERM (Selamat and Ibrahim, 2018). Consequently, a lack of leadership is seen as a mismanagement and was reported by respondents as being an inhibitor in achieving ERM. There is still a lot to learn about why traditional RM is characterised by its lack of leadership, minimal oversight, and thus isolated silos practices (Slagmulder and Devoldere, 2018). The answer is that leadership support is identified as being a performance driver. In this respect, findings are in agreement with literature, which shows that the top-down approach supports ERM. The **leadership** element is interrelated with the **communication** element being communicated through a top-down approach.

c) Capability

i. **Maturity** concerns were raised by Respondents when referred to RM/ERM maturity function. A closer look at research findings indicated that handling and implementing risk controls is more challenging when an organisation's functions are immature and decentralised. Respondents also emphasised an understanding of alignment in the context of business strategy. A similar view was also emphasised by literature, indicating ERM immaturity (Kerstin, Simone and Nicole, 2014; Mensah and Gottwald, 2016). However, there is still a need for

maturing ERM practice, thus considered a developmental phase (Agarwal and Ansell, 2016).

ii. **Culture**

ERM culture is a category related to both organisational governance capability, an element that can be influenced by leadership and commitment of executives and also ethical values, rules behaviour, and understanding (COSO, 2017; BSI, 2018a). In addition to external risk, internal issues are another aspect of uncertainty (Firsova and Vaghely, 2018). A lot of the current literature refers to culture as being a risk that implies cultural issues related to formal and informal constraints in an organisational context (Firsova and Vaghely, 2018) defined by some as institutional (see Subsection 4.2.2, Chapter 4). In fact, tackling risk culture was found to be a significant barrier because it implies a cultural change brought by ERM and in context of organisational culture (Kimbrough and Componation, 2009; Viscelli, Hermanson and Beasley, 2017; Prioteasa. and Ciocoiu; 2017) The human aspect and cultural elements (e.g. language, beliefs, behaviour, values, communication, informal norms, and ethics) can inhibit effective implementation of ERM if resilience to change exists (Kimbrough and Componation, 2009). On the other hand, some authors outline that risk culture should be part of the overall strategic planning (Firsova and Vaghely, 2018; Selamat and Ibrahim, 2018). Another point to consider is that respondents indicated that one aspect of internal culture is when employees speak the language of the business unit and make critical decisions and are successful in managing risk.

Lack of education and awareness is another issue part of *ERM culture* that influences the effectiveness of ERM implementation. Evidence outlines that the role of education is interlinked with the risk culture and thus goes beyond a descriptive meaning because it interrelates with other factors that influence the effectiveness of ERM. In particular, skills and knowledge are seen by practitioners as a way of embedding ERM (Tower Watson, 2010; PwC, 2015). Education is therefore considered essential for implementing and instilling ERM. Youngberg (2010) explains that education starts from the top, so both management executives and employees must be knowledgeable.

d) **Pressure** (16.90%)

i. **Risks and Threats** refers to emerging risks and their velocity that concern respondents. The notion of risks and threats are described as increased in complexity and type. Practitioners also mention this, with the perception that managing risks is becoming more challenging (AICPA, 2018). To this end, organisations encounter various indeterminate conditions which relate to volatility, uncertainty, complexity, and ambiguity (VUCA) (Deloitte, 2017; Iswajuni, Manasikana and Soetedjo, 2018). As evidenced in the interview data, 61.54% self-diagnosticated velocity of risk as medium—within an acceptable tolerance. Much has been written about the vital importance of managing risk with acceptable risk appetite and tolerance. In contrast, prior findings states that the rise in emerging risks means that risk continually changes and organisations struggle (see Practitioners' viewpoint, Section 2.4, Chapter 2).

ii. **Standardised practice** was suggested as a benchmark for being a pressure for following good risk practice. Either in the form of standards or frameworks, respondents indicated that bureaucratic implications represent an additional burden (5.63%).

iii. **Regulations** category refers to mandatory compliance (pressure) on organisations. While industry requirements are voluntary to some degree, regulations in their nature are mandatory demands/expectations of conformity. Evidence found by empirical data shows that for some organisations it is difficult to attain complete compliance. Evidence has demonstrated that it is becoming difficult to reach compliance, and thus, some respondents even indicated regulatory fatigue in reaching compliance. Likewise, a lot of academic literature expresses concern that ERM is being seen as merely demonstrating compliance (Youngberg, 2010). Nevertheless, global expansion has brought a higher necessity to both international regulations and local regulation (Khan, Hussain and Mehmood, 2016). Noticeably, this finding relates to Institutional Theory, respectively with the coercive isomorphism that outlines the effects of regulatory pressure on organisations (see Subsection 4.2.2, Chapter 4).

Category Four: ERM readiness (maturity)

On the whole, this category refers to the level of ERM risk oversight maturity.

a) <u>Risk Oversight</u>

i. Security maturity curve (55.65%)

Evidence shows that most respondents ponder whether security maturity is proactive. The findings shed an optimistic light regarding proactive risk oversight. However, RM (Interview question 12) remains one of the most significant names among managerial components/departments (declared by 34.62% of respondents), while ERM is preferred by 15.38%, and Operational Risk Management by 7.69%. In contrast to evidence which presents the view that the security maturity curve is high, an alternative perspective of prior research illustrates that despite many efforts, ERM remains immature (see Section 3.6, Chapter 3). Drawing on a strategic perspective, the findings demonstrate maturity implementation regarding sampled organisations (38.46%). As predicted, consideration for risk governance evolved but is partially implemented across units/departments. The findings prompt a re-thinking of the status quo of risk governance maturity. The findings show that siloed practices of RM remain embedded in security practices.

7.2.2 Theme 2: Cyber risk oversight maturity

Theme 2 is structured in a sub-theme and four additional categories: determinants, reimbursement, inhibitors, and readiness.

7.2.2.1 Sub-theme 2: CsM baseline expectations

Category One: CsM determinants

This section presents main determining factors to implement CsM, with reference to internal and, external implications.

Table 7-5 CsM determinants

Category One: CsM determinants	
a) ***Internal***	Initiative Culture
b) External	Cyber threats Regulatory Standards/framework

a) <u>Internal</u> pressure (40.81%)

i. **Initiative** refers to organisations' own initiative to proactively initiate CsM adoption. Evidence shows that initiative taken by the organisation's board is a determinant (14.29%).

ii. **Culture** in the context of internal culture was indicated as being the second determinant for CsM adoption (10.20%) because of various security human-related failures. It is believed that cultivation of risk culture is a way of influencing behaviour and attitudes among individuals within an organisation (Nasir *et al.*, 2019). Thus, cybersecurity culture aims to change the mindset towards awareness of risks among employees as well as adherence to internal policies (ENISA, 2017). In addition to the generic research findings, the literature emphasises different dimensions of culture that overlap, either behaviour, perception, assumptions, knowledge, commitment, accountability, awareness, attitude, communication, norms, responsibilities, or values (Korovessis *et al.*, 2017; ENISA, 2017; Nasir *et al.*, 2019). All of the aforementioned are believed to be influenced by artefacts (procedures) and exposed values (guidelines) (von Solms and van Niekerk, 2013). Previous studies have based their criteria on selecting a few elements and have articulated either a top-down approach or mid-level approach (operational) while some other studies focused more on awareness and emphasised a bottom-up approach. Specifically, for this research, culture determinants refer to overall, strategically driven cybersecurity culture. To keep pace with cybersecurity challenges some authors contend a need for an institutionalised cybersecurity culture that standardises everything (von Solms and van Niekerk (2013). This relates to Subsection 4.2.3, Chapter Four, which considers the implications of Institutional Theory.

b) **External** pressure (59.18%)

i. **Cyber threats' velocity and complexity** are one of the main reasons stipulated by respondents. The relative frequency for this determinant was 16.33%. Over the past two decades, major advances in cyber threats were reported by the industry as being a designated effect. Moreover, it is believed that cyber risk poses significant challenges for most organisations (World Economic Forum, 2017).

ii. **Regulatory pressure** is a second external determinant identified with a relative frequency of 14.29%. Regulation as a driver is described by literature as influencing investments for internal control as well as influencing the risk oversight transparency and the disclosure of practices (Gordon *et al*., 2018). This finding overlaps with the literature emphasised in *Regulators' viewpoint*, Section 2.6, Chapter Two and Subsection 3.4.3, Chapter Three.

iii. **Standards** were referred by research findings as being a blended approach (31%). The sampled organisations preferred either a customised approach to the use of a mix

of standards and frameworks and/or create their own frameworks. Most prevalent were ISO 27000 series, COBIT and NIST cybersecurity frameworks. As some respondents stated (e.g. Respondent [18]) it uses standards as a point of reference and refers to them as main guidance, even though is being 'customised'. Little literature refers to mixed/custom approaches that sustained a tailored oversight for organisational needs and capabilities even though it is believed that a customised approach is easy to implement (Talabis and Martin, 2012).

Category Two: CsM reimbursement

While the previous category referred to what determines CsM, this category refers to the benefits of implementation. Thus, reimbursement category is performance-centric and refers to key benefits of implementing CsM. Among reimbursements, evidence articulates five main benefits, as set below.

Table 7-6 CsM Reimbursement

Category Two: CsM Reimbursement	
a) ***Performance***	compliance competitive advantage resilience organisational effectiveness

a) **Performance** (100%)

i. **Compliance** (24.00%) is again indicated, however in this case it is reported as a benefit/reimbursement.

ii. **Competitive advantage** (20.00%) is indicated as being an effect of implementing CsM. Competitive advantage is found to be a cascade effect of all the other categories (e.g. performance, resilience, compliance). Competitive advantage was seen in terms of revenue and profits, the achievement of organisational targets.

iii. **Resilience** (20.00%) has an equal value with competitive advantage. In establishing resilience, it is well known that leadership plays an important role hence both strategy and culture are dependable as well as tactic oriented (World Economic Forum, 2017). The findings of this research identified that resilience is among the expected reimbursement of implementing CsM. Hence resiliency is driven from the top, aligning strategy of cybersecurity with organisational strategy, and is a recommended approach that proactively acknowledges of responsibilities, integration, risk appetite, resilience planning, or assessment of effectiveness in order

to ensure the long-term sustainability of organisational strategy. Within literature, it is recognised that apart from being led from the top, resiliency is also a shared responsibility within an organisation (World Economic Forum, 2017). The empirical findings demonstrate that the benefits of applying effective risk oversight are recognised among respondents as being valuable.

iv. **Organisational effectiveness** (14.00%) implies mapping results of security measures against the overall organisational strategy and objectives achievement (Hagen, Albrechtsen and Hovden, 2008). A significant trait of effectiveness is that it defines the effectiveness of the relationship between two or more variables. In this regard, Contingency Theory identifies prerequisites of effectiveness (see Subsection 4.2.1, Chapter 4). Additionally, evidence shows that measuring the reimbursement of CsM respective effectiveness has a positive effect as it endorses results and recommends security needs (e.g. IASME framework, Subsection 4.3.2.2.1, Chapter 4).

Category Three: CsM inhibitors

The below category emphasises main CsM inhibitors in order to understand what issues should be addressed in an organisation environment.

Table 7-7 CsM Inhibitors

Category Three: CsM Inhibitors	
a) ***People-centric***	culture
b) ***Strategic centric***	cost silos

a) **People-centric** (35.82%)

i. **Culture** is a CsM inhibitor that is people-centric. Considering that the culture of an organisation emphasises different dimensions that overlap (previously discussed in CsM reimbursement Subsection 7.2.2.1), it is clear that it encompasses a multitude of components. For instance, the research findings identified that only 7.46% appreciated as effecting CsM. However, if based on previously discussed dimensions of culture, awareness and skills (knowledge) are recognised to be part of cybersecurity culture. Thus, a **lack of awareness** was agreed by 17.91% of respondents. Additionally, 10.45% of respondents believe that a **lack of employees' competencies** (skills and knowledge) affect

implementation. To understand the role of culture, this category encompasses both a lack of awareness and a lack of skills, and thus it represents subcategories, respectively dimensions of cybersecurity culture (Korovessis *et al*., 2017; ENISA, 2017; Nasir *et al*., 2019), and not disparate concepts as had previously been understood by respondents.

b) **Strategic centric** (22.39%)

i. **Cost**, 11.94% agreed that the cost of implementation inhibits CsM. Literature emphasises that there is a tendency for organisations to underinvest due to the latency of results about uncertainty of the likelihood of a cost being associated with a breach of security (Gordon *et al.,* 2018). One possible explanation for mistrust is because cybersecurity investments generate cost avoidance instead of revenue (Gordon *et al*., 2018).

ii. **Silos**, 10.45% of respondents mention silo approaches and silo strategies as impeding CsM. Similar findings were signalled by literature in Subsection 3.5.1, Chapter Three.

Category Four: CsM Readiness

The corresponding results of CsM readiness refers to how well a department is **managing** the risk within **risk appetite,** and what the current position (**risk profile and tolerance**) is in terms of readiness. A lack of maturity was reported by respondents to have three main side effects have been identified: reputational loss (24%), regulatory consequences (17.33%), and financial loss (16%). Given the fragmented management related to cybersecurity, this category is unable to provide specific data of respondents' estimations. Instead, this aspect is discussed and evaluated further in Subsection 6.2.4, through alignment lenses.

7.2.3 Theme 3: Strategic alignment

This section describes the main categories identified for strategic alignment. Understanding the root of strategic risks and how they can affect business objectives is a key scope of this section. Research findings articulate how key risks are being managed and where these key controls are located across an organisation. A re-frame/realignment for an effective and integrated assurance plan for both risk control and risk oversight was suggested by some authors in a bid to reach holistic risk governance (Althonayan, Matin and Andronache, 2018). Similar to the other two themes (CsM and ERM), the research findings determined a

strategic alignment sub-theme and five categories deconstructed in reimbursement, inhibitors, readiness, potential and alignment fulfilment.

7.2.3.1 Sub-theme 3: Establishment of strategic directions of alignment

To tackle establishment of strategic alignment, the research findings of this section are aligned with two research objectives (*Research Objective 2 and Research Objective 4).*

Category One: Alignment Determinants

This category underpins main reasons for implementing the strategic alignment.

Table 7-8 Alignment determinants

Category One:	**Alignment determinants**	
a)	***Determination***	objectives business strategy

a) **Determination** was revealed as being grounded in two main elements ranked as being the highest: strategy and objectives.

   i. **Objectives** were evidenced by 40% to be a determinant in establishing strategic directions. Similar to ERM and CsM the common goal is sustenance of ensuring achievement of organisational objectives. Since it confers a clarity and sense of expectations, objectives also defines the risk tolerance (Lam, 2017).

   ii. **Business strategy** attainment was reported to be another determinant factor (40%). This determinant is in close relation with effective alignment accomplishment and dependant on many elements.

Category Two: Reimbursement

Research evidence indicates that establishment of effective alignment reimburses positive effects, respectively remuneration of control deployed. This is in the line with much of the available literature on alignment (discussed in Section 2.8, Chapter Two). However, the literature refrains from specifically referring to CsM and ERM as a compound that aligns their strategies.

Table 7-9 Alignment Reimbursements

Category One:	**Alignment Reimbursements**	
a)	***Benefits***	avoidance of duplication strategic alignment enterprise-wide risk measurement

b)	***Potential reimbursements***	communication prioritisation of risks

a) Benefits of alignment

i. **Avoidance of duplication** (18.75%) means that alignment of CsM with ERM supports the elimination of risk siloed approaches and reduces organisational exposure owing to a single, unified mechanism of risk governance that supports business strategy and objectives (Deloitte, 2014b). This reimbursement was among three main benefits indicated by respondents.

ii. **Strategic alignment** was reported by 18.75% of respondents as being an effect of alignment. Likewise a extant literature indicated similar benefit (see Section 2.7, Chapter 2 and Section 3.5, Chapter 3).

iii. **Enterprise-wide risk measurement** is the third benefit indicated (16.67%) that articulate the need for understanding the long-term effects of ERM once implemented.

b) Potential reimbursements

Among the main recommendation was communication and prioritisation of risk.

i. **Communication** (18.42%) is acknowledged as a potential benefit if effective alignment occurs. Communication requires a specific mechanism to sustain inter-departmental communication and uniform reporting structure among all departments within an organisation in order to avoid inadequacy when tackling specific problems. Such communication and structure would undeniably lead to a more co-operative approach (fusing the departments of an organisation and disseminating information) should a formalised process be applied (Rubino, 2018).

ii. **Prioritisation of risks** (18.42%) is an essential requirement for adopting alignment. Even though competing priorities between business units are among the obstacles of efficient ERM (Gates, 2006), a strategic alignment reimburses this capability.

Category Three: Alignment inhibitors

This category refers to inhibitors and limitations of CsM with ERM alignment by focusing on understanding weaknesses and barriers. Research findings identified two main strands: governance and employees centric.

Table 7-10 Alignment Inhibitors

Category Two: Alignment Inhibitors	
Governance	cultural deficiencies
	inappropriate governance
Employees	skills deficiencies

a) Governance

Governance was mentioned by 31.87% of respondents, being the second thematic category to influence misalignment. Additional elements of cultural implications and inappropriate governance were identified.

i. **Cultural deficiencies** (11.59%) in this context refers to risk culture. Bearing in mind that risk culture is one of many components of organisational culture (Carretta, Farina and Schwizer, 2017), the findings indicated concerns in this regard. Traditionally, it has been argued that risk culture implies organisation values, past experiences, philosophy, and behaviour prevailed in management style along with operational deployment in the form of a pattern of conduct (Carretta, Farina and Schwizer, 2017; Chartered Institute of Internal Auditors, 2018). Additionally, risk culture has been defined as a predictable and repeatable behaviour or else desired level of ethical values influenced by internal values, beliefs, knowledge, and understanding (IRM, 2012). Therefore, most scholars define risk culture through various strands. Previous studies have shown that risk culture implies two main strands: (1) organisational attitude, and (2) people's behaviour under risk pressure (IRM, 2012; Chartered Institute of Internal Auditors, 2018). Accordingly, risk culture has been associated with various key elements of organisational culture as leadership, strategy, adaptability, coordination, and relationship (Smit, 2010; Silvius, Smit and Driessen, 2010). For instance, COSO 2017 framework (COSO, 2017) refers to both sides, the organisation and individuals (the latter is favoured instead of group/collective). COSO's framework refers to integrity, ethical values, organisational philosophy, organisational structure, roles, and responsibilities as well as employees' competencies and human resource practices (COSO, 2017). Likewise, Power, Ashby and Palermo (2013) provide an account of organisational risk culture emphasising culture as being driven by leadership, performance, ideology, and even control. When reviewing prior research, there was evidence regarding the challenges

of risk, often in terms of leadership support ('tone from the top'), management of risk culture, overconfidence in risk controls, pressing ideologies, lack of consistency, blame culture, and lack of rewarding ethical behaviour or acceptance of same attitude and behaviour across an organisation (Power, Ashby and Palermo, 2013). This suggests that culture is a collective ability to manage risk which can affect overall organisational culture and a lack of consistent risk culture inadvertently exposes organisations to vulnerabilities and predisposes them to risks (IRM, 2012). Risk culture is a cornerstone for risk governance and a confirmed inhibitor (both by prior literature and current research) for alignment and strategic changes (Power, Ashby and Palermo, 2013). In short, the same logic underlies the cultural dimension of alignment, which determines the degree of fit between organisational culture and strategic alignment strategy.

ii. **Inappropriate governance** was pinpointed by 10.14% of respondents as being an inhibitor in achieving alignment. As previously discussed in Subsection 6.2.4.11, Chapter Six, governance can be hindered by unclear policy, disconnected policies among business units, or disconnected risk statements (siloed). Readiness to overcome deficiencies of governance depends on the organisation's acceptance to change, the cost involved, and the availability of resources (Prioteasa and Ciocoiu, 2017; Merhi and Ahluwalia, 2018). Moreover, a lack of management commitment for translating strategy and a lack of aligned risk appetite make it challenging to prioritise risk. The evidence articulates that inappropriate governance also triggers uncoordinated efforts of staff involved (11.59%). Inadvertently, it implies resistance to change and/or non-acceptance.

b) Employees

The second category that inhibits implementation relates to people-centric rapport, meaning that 24.63% of respondents reported concerns related to skills, culture, or a lack of coordination.

i. **Skills deficiencies** (13.04%) was reported to be another core element that affects the effectiveness of alignment. This finding relates to Henderson and Venkatraman's model (main contributor of alignment paradigm, see Subsection 4.3.3.1, Chapter Four) and from the early 1990s has underlined the value of correlation between skills, process, and business scope (Henderson and Venkatraman, 1993). Similar considerations were evidenced by Luftman's model, which pointed to employees' skills as a prerequisite in preparing a sustainable and effective alignment, expecting

an understanding of concepts and drivers, and lastly a consistent language across the organisation (Luftman, 2000). One criticism of respondents is it related to the diversity of terminologies that varies between business units. In addition, the shortage of employees and unclear accountability (responsibility) sustain deficiencies.

Category Four: Readiness (maturity)

This section provides an overview of Alignment maturity curve extracted from empirical data.

Table 7-11 Alignment Readiness

Category Three: Alignment Readiness (maturity)	
a) Maturity	departmental communication risk ownership risk appetite maturity

a) <u>Maturity</u>

i. **Departmental communication** was found to be considered a descriptor element of maturity, particularly concerning how risks are communicated and dealt with across an organisation to illustrate coordination and coordination among teams. Even so, 44% of respondents categorised their practices as being somewhat useful. Only 24% stated that communication is very effective, declaring it as mature. Consistent with theoretical findings (see Section 3.6, Chapter 3), strategic communication has been identified as a determinant of alignment, a measure of maturity (demonstrated by empirical findings), an inhibitor, and/or enabler factor. The existence of these effects implies that despite broader research, the relationship between communication and alignment has yet to reach maturity. Attributes revealed by empirical findings are readiness, effectiveness, understanding of policies and procedures, culture, transparency, support, and common language. Consequently, communication is associated with effective decision making, hence it represents support clauses in many industry standards (e.g. Clause 7.4, ISO 31000:2018; Clause 7.4, ISO 27001: 2017).

ii. **Risk ownership** in this context refers to the organisation departments, respectively those delegated responsibilities for managing risks. It has been found by empirical findings that 57.69% of respondents stated that risk control is deployed at both

department and enterprise levels, like a dual-responsibility. However, findings showed that referring to them at both a department and enterprise level might lead to periodical reporting, and in some other cases reporting may occur only if a certain level of complexity is reached (Respondent [4], [7] and [8]). Departmental cross-functional responsibilities for risks (ownership) is a critical issue that refers to accountability (COSO, 2016). Having both types of approach, being both siloed and enterprise-wide is a paradox and an unanticipated finding. The fact that risks are managed through a mix of approaches shows that departments deal with their own risk and report further enterprise-wide (some sort of alignment) risks.

iii. **Maturity**

Overall status of CsM alignment with ERM denotes the identified maturity of alignment governance. With only 34.62% of respondents indicating maturity as being somewhat mature and optimised to organisational needs, the lower score of 19.23% state full maturity (fully optimised) and captures ineffective practices. Immature practices are difficult to manage when inconstancies in activities of business units appear. Perhaps of more concern, decentralised functions, as well as various geographies of business units, arise.

Category Four: Prospect

This category focuses on emphasising the prospect of instilling strategic alignment.

Table 7-12 Alignment Potential

Category Four: Alignment Potential	
a) Potential	Credence Acceptability
b) Alignment fulfilment	Responsibility Alignment deliverables Alignment drivers Assessment of alignment

a) Potential

i. **Credence** refers to some respondents' referrals for aligning strategies of CsM and ERM. Consideration for CsM alignment with ERM was found by 69.23% of respondents who considered alignment an enabler and were thus interested in applying the alignment paradigm principle. However, despite a significant credence for alignment others mention, despite understanding its principles, that in reality, a

lack of resources and specialisation impede deployment of alignment (Respondent [10]). Part of ERM and an aligned CsM are understood to play an essential role in holistically managing and controlling risks.

ii. **Acceptability**

The analysis revealed a significant acceptability among respondents for value proposition of CsM and ERM alignment (75%). It shows that value of alignment is understood, in detriment of 'compartmentalised' approaches.

Sustainability explores if an approach is sustainable in terms of organisational risk governance in the long-term. Evidence showed a paradox of findings and 38.46% of respondents *strongly disagree* with the alignment feasibility, while another 38.46% *agree* with implementing alignment. A potential explanation of respondent's resistance to alignment might be explained by immature practices regarding ERM and CsM alignment.

b) Alignment fulfilment

i. **Responsibility**

Alignment responsibility/accountability was indicated by respondents to be one of four recommendations. Support of senior managers is emphasised by respondents. Thus, understanding the implication of the human element in deploying security practice is another component to consider. The highest responsibility was indicated to be the Chair of Board (32.14%), followed by CEO (14.29%), Chief Risk Officer (14.29%), and lastly, 14.29% indicated that it is a shared responsibility.

ii. **Alignment deliverables** implies **translating priorities** for each function (20.83%), stating deliverable of alignment to create interconnectivity and partnership. Additionally, **defined strategy** (16.67%) is another deliverable expected post-implementation.

iii. **Alignment drivers** refer to elements that motivate implementation. Research findings articulate that **evaluating/assessing performance** of alignment is identified by 25.00%. Additionally, **recognition** of due care for strategy contribution (10.71%), followed by education at every level of implementation (10.71%) were identified. In addition**, executive-level support** (10.71%) is indicated to count in implementing the strategic alignment. Moreover, within the literature, it is believed that leadership behaviour influences alignment practices (Shao, 2018).

iv. **Assessment of alignment** is key when understanding alignment fulfilment. Consistent with literature, this research found that alignment is measured against risk appetite, policies, risk and control assessment, and comparable baseline between current capabilities, performance, objectives, and desired alignment (Salaheddine and Ilias, 2017). Commenting on alignment assessment, respondents indicated that alignment assessment is made through three primary methods: **metrics** (15.38%), **audit** (19.23%), and **risk and control assessment** (11.54%). Another angle on this is that respondents indicated that assessment of alignment can be made against objectives, policies, contracts, compliance (regulations), framework, and lessons learnt. This result provides further support in understanding implications and the pre-requisite of alignment assessment.

Previous studies evaluating assessment observed that a lack of suitable metrics creates difficulties in understanding effectiveness (Kerstin, Simone and Nicole, 2014). In particular, a metric is an indicator of performance, outlining progress towards achieving organisational strategy (COSO, 2010; Scarlat, Chirita and Bradea, 2012). Either as a risk indicator or performance indicator, it represents a form of feedback on actions undertaken, and thus the benefit is that it helps to optimise actions and resource allocation (Scarlat, Chirita and Bradea, 2012).

7.3 Key research findings of interviews

Despite various efforts of securing organisations, the research findings show that managing risk holistically remains a challenge for most organisations. In particular, organisations struggle in aligning the function of control and risk oversight to tie together all risk functions. Variations among the three disciplines (CsM, ERM and Alignment) explain why practices remain fragmented.

In this regard, Table 7-13 thematically synthesises the main findings of the research interviews.

Table 7-13 Key research findings of interviews

ERM Enterprise Risk Oversight Maturity	**CsM** Cyber Risk Oversight Maturity	**Alignment** Strategic Alignment
Sub-theme 1: ERM Baseline expectations	CsM Baseline expectations	Sub-theme 3: Establishment of strategic directions
Category One: ERM determinants	**Category One: CsM determinants**	**Category One: Strategic Alignment determinants**
Strategic governance (45.16%) • governance (17.74%) • strategy (4.84%) • prioritisation (22.58%) Differentiation-centric (11.28%) • competitive advantage (4.84%) • value (6.44%) Risk resiliency (43.56%) • control (14.52%) • compliance (14.52%) • knowledge (14.52%)	Internal (40.81%) • initiative (14.29%) • culture (10.20%) External (59.18%) • cyber threats velocity and complexity (16.33%) • regulatory pressure (14.29%) • standards (blended approach, 31%).	Determination • objectives (40%) • business strategy (40%)
Category Two: ERM reimbursement	**Category Two: CsM reimbursement**	**Category Two: Alignment reimbursement**
Internally (42.87%) • culture (8.57%) • shareholders' requirements (7.14%) Externally (57.15%) • regulatory requirements (30.00%) • competition (10.00%)	Performance (100%) • compliance (24.00%) • competitive advantage (20.00%) • resilience (20.00%) • organisational effectiveness (14.00%)	Benefits • avoidance of duplication (18.75%) • strategic alignment (18.75%) • enterprise-wide risk measurement (16.67%) Potential reimbursements • communication (18.42%) • prioritisation of risks (18.42%)
Category Three: ERM inhibitors	**Category Three: CsM inhibitors**	**Category Three: Alignment inhibitors**
Resources (32.39%) • cost (7.04%) • data and information (7.04%) • people (5.63%) • skills (5.63%) Direction (9.86%) • strategy (4.23%) • leadership (5.63%) Capability (43.66%) • maturity (9.86%) • culture (8.45%) • lack of education and awareness (7.04%) Pressure (16.90%) • risks and Threats (7.04%) • standardised practice (5.63%) • regulations (2.82%)	People-centric (35.82%) • culture (7.46%) (e.g. lack of awareness, 17.91%; lack of employees' competencies, 10.45%) Strategic-centric (22.39%) • silos (10.45%0 • cost (11.94%)	Governance (31.87%) • cultural deficiencies (11.59%) • inappropriate governance (10.14%) Employees (24.63%) • skills deficiencies (13.04%)
Category Four: ERM readiness	**Category Four: CsM readiness**	**Category Four: alignment readiness**
Risk Oversight • implementation maturity (38.46%)	Side effects • reputational loss (24%) • regulatory consequences (17.33%) • financial loss (16%).	Maturity • departments communication (44% of respondents categorise their practices somewhat effectively) • risk ownership (57.69, by both department and enterprise level, no mechanism) • maturity (only 19.23% stated to have full maturity; 34.62% of respondents indicating maturity as being somewhat mature)
Category Five: Alignment Prospect Enterprise-wide Risk Governance Alignment credence (69.23%) ─ agreed with alignment Alignment fulfilment, acceptability (75%)		

Source: The Researcher

Through the research questions, the empirical results have revealed **determinants** of ERM associated with strategic governance (45.16%) and determined by external pressure for risk resiliency (43.56%) whilst CsM is due to be implemented because of another type of external pressure (59.18%) related to the nature of cyber threats velocity and complexity (16.33%). Additionally, the regulatory pressure (14.29%) and industry standards influence good practices even though organisations prefer blended approaches of standards (31%). On the other hand, alignment seems to be a business decision being more lead by an organisation's own initiative, respectively being strong-minded by objectives (40%) and business strategy (40%). Given these findings of determinants, it was found that **reimbursement** is another dependable of the end goal. On this basis, ERM was found to be encouraged by external recognition (57.15%) of regulatory requirements fulfilment (30.00%) and by keeping pace with competition (10.00%). This aspect of reimbursement is, for CsM, a performance-centric orientation, focused on compliance (24.00%) as a way of achieving a competitive advantage (20.00%) and resilience (20.00%). More generally, alignment was benefits-driven by ROI, capable of duplication avoidance (18.75%), strategic alignment achievement (18.75%), enterprise-wide communication (18.42%), and prioritisation of risks (18.42%). Nevertheless, present findings also confirm that **inhibitors** are being consistent with the findings of prior research. ERM is indicated to be inhibited by capability (43.66%) and lack of resources (32.39%) while CsM indicates similar impediments, emphasising people-centric inhibitors (35.82%) and related strategic consequences (22.39%). Likewise, the alignment indicates enterprise-wide issues related to governance (31.87%), either in terms of inappropriate governance or being culturally related. Accordingly, outline people-centric issues registered 24.63%.

Broadly translated the findings indicate that **readiness** of alignment maturity of CsM and ERM is yet to be achieved. Despite significant consideration of ERM, it was indicated to be implemented in the proportion of 38.46%. In the case of CsM, an estimation of maturity was unachievable because of various types of departments and fragmented management controls in dealing with cyber risks (i.e. some of the sampled organisations have IT-related functions). Data gathered it suggests that security functions are in place to ensure avoidance of security flaws' side effects such as reputational loss (24%), regulatory consequences (17.33%), and/or financial loss (16%). Readiness, in cases of alignment, registers low values, with only 19.23% stated to have full maturity.

Moreover, communication in the process of alignment was indicated by 44% of respondents to be somewhat effective. Of more concern, risk ownership (57.69%) was indicated to be segregated in both department and enterprise level (no mechanism in place). On the whole, these results demonstrate what effects implementation has in the context of various determinants, reimbursement, inhibitors, and readiness among all three domains. Somewhat surprisingly, the alignment acceptability (75%) and credence (69.23%) for *CsM - ERM Strategic Alignment Framework* confirm the strength of the proposed solution. On these grounds, the empirical findings were organised thematically to sum up the results of interviews.

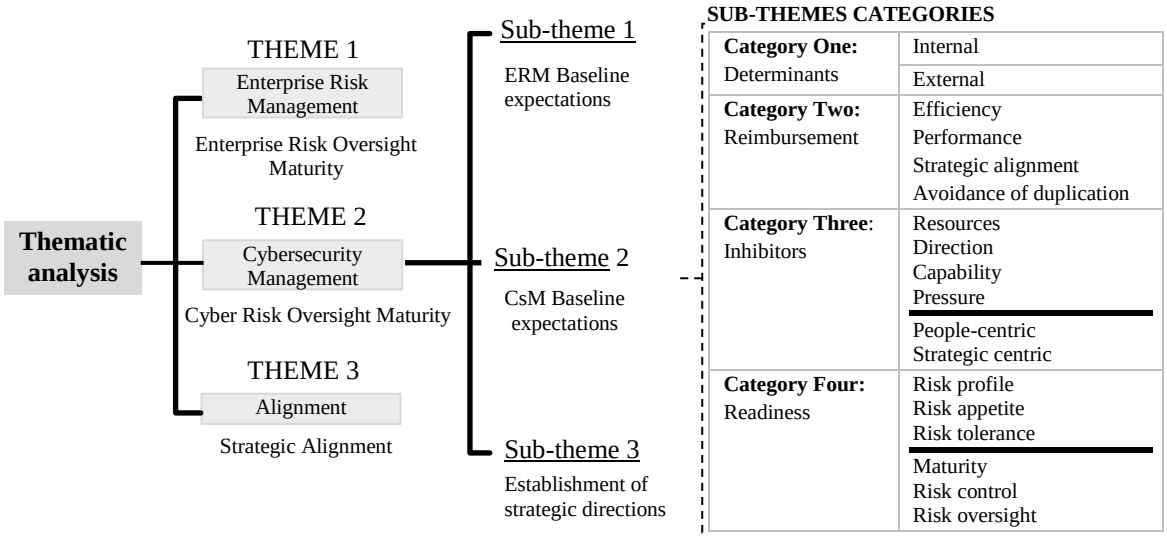


Figure 7-1 Thematic map of empirical findings (interviews)

Source: The Researcher

Evidence demonstrates that four dimensions of overlapping alignment exist: respectively intellectual (strategic), structural, cultural, and operational. It is conceivable that implementation prescribes the use of all dimensions because all interrelate. One of the aspects that emerges from these findings is related to the alignment paradigm. With reference to initial discussion from Section 4.2.3, Chapter Four, the research findings advocate that contingency and institutional alignment are both related to alignment (cultural and institutional dimensions).

For instance, the culture may act under specific context as a rule of law (i.e. some behaviours and practice can be standardised later on as official rules, bare expectation). In addition, moral and social norms can act as standards of behaviour of certain groups of people. Contingency Theory correlates with findings of RM, performance, and value delivery. On

the other hand, Institutional Theory correlates with empirical findings regarding aspects of cultural alignment, communication, and awareness. Institutional Theory relates to the purpose of employing good practices (e.g. standards, frameworks); respectively, external legitimacy (Cavusoglu *et al.*, 2015).

Furthermore, Institutional Theory provides support for exploring the external pressure of *mimetic pressure* that refers to imitating practices (Cavusoglu *et al*., 2015) as well as understanding the coercive pressure that refers to external pressure as a conformity influencer driver (Cavusoglu *et al*., 2015). Moreover, normative pressure refers to norms of security practice driven by the industry (Cavusoglu *et al*., 2015). Henceforth, an organisation strategy should calibrate with internal and external pressures (Kaplan and Norton, 2003; KPMG, 2017b) as it is essential to understand both institutional (e.g. strategy, structure, culture, organisational design, processes, leadership, technology, and structural alignment) and Contingency Theory implications (value, normative rules, legitimacy, beliefs, principles, behaviour, ethics, social systems).

What emerged from the empirical research findings is that all dimensions of alignment need to be included because they interrelate (cultural, intellectual, structural, operational). Even though literature defined the cultural dimension of alignment as 'social alignment' (see Section 4.3.3, Chapter 4). The empirical finding demonstrated that when theory refers to social dimension it refers to interdepartmental communication and social interaction. Which in fact relate to institutional theory and cultural dimension. Henceforth, cultural dimension of alignment incorporates communication, education, awareness and much more (Braumann, 2018). Thus, the social dimension emphasised by literature (e.g. Reich and Benbasat, 2000; Kay and Avison, 2005; Volk and Zerfass, 2018) submerge to the theory of cultural alignment; thus, this research emphasise that social dimension is in fact part of cultural dimension and was erroneously defined by prior literature.

It is clear that each domain contributes to risk governance and thus, when aligned together, they affect higher results. In short, findings suggest that despite separate efforts of each domain to maintain performance, addressing them individually remains a challenge. Therefore, the research findings point towards the potential value of pursuing integrated efforts that sustain enterprise-wide holistic governance. Once again reconfirm that the advantages of adopting the research *Framework* is that it ensures conformance, performance, sustainability, and effective strategic alignment between CsM and ERM.

7.4 Revised research framework

This section incorporates empirical findings that contribute to the research framework. Accordingly, the research framework is revised based on compiled evidence. To date, the first version of the *Framework* proposes five derivates (constructs):

- Literature review (derivate one);
- Systematic literature evaluation (derivate two);
- Research gap (derivate three);
- Supporting theories (derivate four);
- Supporting frameworks (derivate five).

Having incorporated the five derivates and a three-dimensional view (academics, practitioners and regulators), the first version of the framework represents a baseline for the validation phase. Overall, framework elaboration has been driven by Research Aim two, the quintessence of which is to determine *the development of a framework that assists CsM with ERM alignment within the financial industry, supported by practical guidance for the implementation of the proposed framework.* Consequently, the empirical results extend views on the validity of the conceptual framework that was initially presented in Subsection 4.4.2, Chapter Four. In this phase, empirical results are challenged against the research questions in order to validate necessity and validity. Then, the input of empirical findings completes the research with a practical view (**derivate six**); as a result, gives rise to an additional pillar for the framework.

The practitioner's view provides further evidence in articulating the issues within the financial business context. Accordingly, in view of empirical findings, the *CsM - ERM Strategic Alignment Framework* is revised.

In this regard, Research Question 1 explored *why strategic alignment of CsM and ERM sustains a financial business in long-term.* It was identified that an alignment of both paradigms holistically sustains risk resiliency. Both literature and empirical findings enunciate the importance of tying together all risk and oversight functions to ensure increased resiliency, and effectiveness. Given the nature of the financial industry, this aspect of securing strategically financial organisations has received more impetuous due to the increased constraints of the external environment (e.g. compliance, velocity of threats, client demand, etc.); something that is of concern when determining good practices. Evidence showed that strategic alignment sustains risk governance by utilising resources, reducing

cost, creating visibility of risks (e.g. risk register; risk mapping), prioritising, ensuring enterprise-wide risk measurement, compliance and thus effectiveness, and strengthening an organisation's security posture.

Moreover, the strategic alignment of CsM and ERM represents a risk performance function that encourages interconnectivity, communication, and partnership between business functions. This portrays the determinants revealed by the empirical findings previously reported in Table 7-13.

Furthermore, Research Question 2 investigated *what are the key issues that impede the alignment process in the financial industry regarding CsM and ERM*. It was found that each domain encounters similar challenges yet differs in type. For instance, both ERM and CsM were reported to encounter issues related to external pressure (e.g. risk and threats, standardised practice, regulations). Resource allocation, lack of direction, and a lack of capabilities were also similar to a certain extent. The alignment domain focus, however, indicates an inappropriate governance (e.g. cultural inefficiencies; inappropriate governance) and employees skills deficiencies as some of the main barriers.

To understand the research problem further, Research Question 3 assessed: *how are theory, practice, and regulation direction applied regarding the current alignment of CsM and ERM within the financial industry?* Although the question was addressed in the literature review, when applied to empirical findings it was discovered that the alignment of CsM with ERM is scarce (19.23%). However, implementation of ERM was reported to reach 38.46%, whilst CsM maturity was difficult to identify due to fragmented practices.

Lastly, Research Question 4 calls into question: *what effects have the implementation of the new framework*? It was concluded that strategic alignment supports enterprise-wide risk governance (75%), and the unified capabilities of strategic governance is beneficial for gaining value, resiliency, performance, compliance, sustainability, and competitive advantage. Figure 7-2 outline changes determined by the empirical findings' indications. Such changes are reflected in blue below.

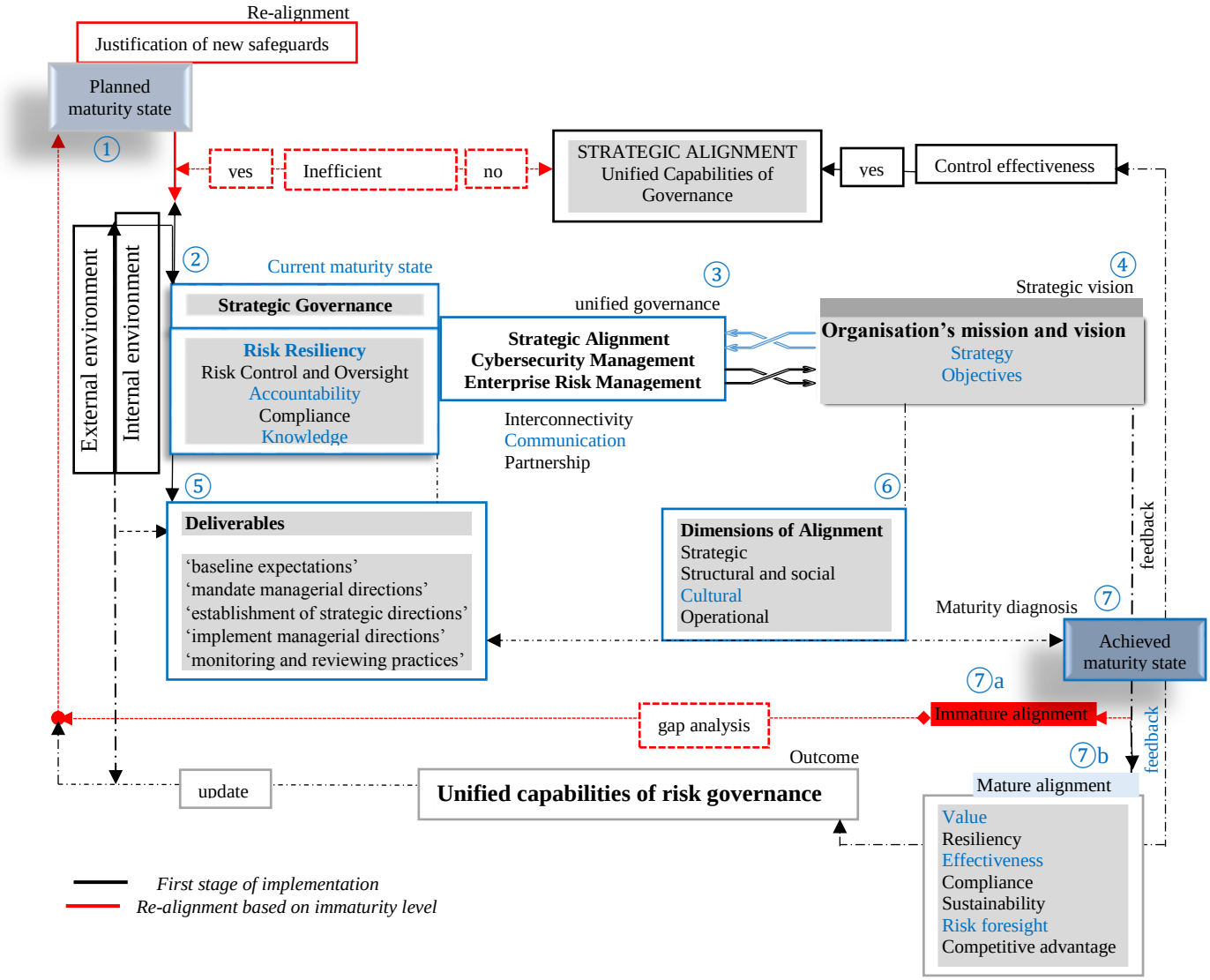


Figure 7-2 Revised *CsM - ERM Strategic Alignment Framework*

Consistent with the empirical findings, Figure 7-2 outlines changes identified in contrast with Figure 4-13 from Chapter Four. Figure 7-2 shows that integration of additional elements has influenced the transformation of the initial framework, leading to a more interrelated and cyclical framework. The changes appear in the first phase of the deployment of risk control, risk oversight, and compliance function. For instance, each domain has specific internal and external factors that were considered independently. In addition, to align all towards the goal of achieving the overall organisational strategy and objectives, it was deemed that each domain has its own determinants and inhibitors that are less applicable than those of the other two domains. Ultimately, the empirical findings showed that each domain has its own expectations, risk silos, and approaches. A first change is strategic related. Findings recommend re-assigning and accepting each domain's determinants and inhibitors, bridging and aligning all of them altogether. However, keeping in mind the specifics of each, instead

of putting them all together and prioritising, this task is delegated and tracked in a unified process of enterprise-wide alignment. This means that it deploys strategic governance of all three domains ─ thriving to address risks systemically while assigning risk ownership and roles accountability. A second change is culturally related. Cultural element implications in alignment were identified to be a predominant sub-theme in all three domains. Compared to the initial framework, the contribution of empirical findings demonstrates that elements such as education, awareness, skills set, and communication are interrelated elements of culture. For instance, communication was found to be an essential element for achieving unified governance. Much more, the research findings reflect the implications of culture in strategy, structural alignment, and operational alignment; all impacting performance, resiliency, compliance, sustainability, and competitive advantage. Consequently, labelled by the Researcher, the **performance risk chain** has positive ripple effects: *effectiveness ─ resiliency ─ value creation ─ competitive advantage ─ compliance ─ risk strategy sustainability ─ risk foresight ─ organisational objectives achievement.* In addition to strategic, structural, and operational alignment, the cultural dimension is the fourth dimension incorporated in the *Framework.* A third change is structural and related to risk control and oversight. Consideration for structural alignment of risk control and risk oversight were made. A fourth change relates to operational and strategic alignment. The risk resiliency function was included because it is one of the main drivers of the alignment. Respondents identified that risk resiliency underpins risk control and oversight, accountability, compliance, and also knowledge. A fifth change was related to the starting and ending point of implementation, thus changes were made. It was understood that a planned maturity state represents the starting point, followed by identification of current maturity state, and lastly after all are implemented, the achievement of a certain maturity state shall define further tasks.

Overall, refinement of the framework evidences a regrouping of few layers of control and provides direction to connect all components to organisational mission and vision. It facilitated an identification of continuous process, meaning that organisational strategy and objectives are used as a main point of reference. However, it is understood that at certain points not only ERM and CsM shall align but the strategy itself. As such, the organisation itself shall adopt and incorporate principles of holistic risk governance; being a continued realignment mechanism to sustain effectiveness, sustainability and resiliency. The *Framework* incorporates four lenses of alignment (strategic, structural, operational, cultural) meaning that it creates an equilibrium among potential inhibitors, implementing both

horizontal and vertical approaches (‘top-down and bottom-up’). Having outlined changes and answers to the research questions, the *CsM - ERM Strategic Alignment Framework* bridges the following deliverables:

- ✓ Deliverable 1: Advocates an understanding of organisational goals, objectives, strategy, risk appetite, risk tolerance, acceptable residual risk, and alignment expectations across the whole organisation. It fosters an effective alignment in accordance with organisation goals and objective.
- ✓ Deliverable 2: Defines strategic baseline expectations of external environment from which principles and context are derives with the determination to establish the drivers (purpose, limitation and constraints) and how alignment should be achieved.
- ✓ Deliverable 3: Emphasises the internal strategy in alignment, paying consideration to external requirements. Sets of internal directions are in balance with identified external directions, defining how the appetite, structure, processes, responsibilities, and commitment work in a unified manner in order to cope with external environment.
- ✓ Deliverable 4: Establishes processes and structure for strategic alignment implementation between CsM and ERM. It supports considerations of strategic and structural alignment enhanced with internal and external factors.
- ✓ Deliverable 5: Employs identification of risk owners, measurement (performance), improvement (development), transparency, and compliance. It establishes the context, identifying current situations (assets, threats, vulnerabilities, and control). Recognising the risk owners, location, or source of threats are all prerequisites in assuring flexibility of implementation.
- ✓ Deliverable 6: Transfers the strategic guidance into an operational and cultural dimension that aligns with operations to deploy enterprise-wide alignment.
- ✓ Deliverable 7: Includes documentation for further use of the reviewing processes that depend on comparisons of practices with the predetermined baselines, prior learned lessons, experiences, organisational cultural dimension, observations, and research.
- ✓ Deliverable 8: Compares maturity level against industry baselines to determine the degree of control function effectiveness.
- ✓ Deliverable 9: Entails systematic re-alignment as an enabler for reaching a higher level of maturity.

Overall, CsM-ERM Alignment Framework concentrated on siloed approaches of CsM and ERM and aimed to provide an alternative way for managing all types of risks holistically

and comprehensively, and thus contextualised them. Among top findings from empirical results are the benefits of implementing the frameworks as value creation, value capture, value enhancement, organisational effectiveness ─ instead of performance (initial version of framework), and risk foresight. Unified, the framework combines risk control capabilities with risk oversight capabilities in order to reach an enterprise-wide risk governance capability that enhances overall risk foresight capabilities of financial organisations.

[(CsM \ ERM) + rc] + [(CsM \ ERM) + ro] = \E-wRG (rr + oe + orf)

*\=aligned
*CsM=Cybersecurity Management
*ERM =Enterprise Risk Management
*rc =risk controls
*ro =risk oversight
*rr =risk resiliency
*oe =organisational effectiveness
*orf =organisational risk foresight
*E-wRG =Enterprise-wide risk governance

This propounds the idea of "catalyst for foresight" (Lauder, 2016, p. 3). The essence of this concept is being prepared to anticipate an event (known as 'black swans') and avoid failure (Lauder, 2016). Having foresight rests on the assumption that an organisation is able to foresee signals of risks and their impact. Moreover, it can create scenarios on how to manage, how to be risk resilient to emerging threat by having the right knowledge, accountability and communication, and how to recover successfully if avoidance is not possible; respectively adjusting the negative effects (Raban and Hauptman, 2018).

7.5 Conclusion

This section concludes the Discussion Chapter by highlighting some of the key implications, contributions, and limitations. Overall this chapter has advanced from 'description' in Chapter Six to 'interpretation' to investigate the alignment of CsM with ERM within the financial industry. The main aim of this chapter was to explore thematically how industry's views (practitioners) revolve around aggregating answers for attaining answers for research questions. Various contributions have been made via prior literature, however sustainable and enterprise-wide governance remains a challenge in practice. This renders the most obvious contribution of fulfilling the research questions.

Another significant contribution that has emerged from this chapter is that it has conveyed a revised research framework that fulfils the requirements of the second research aim: *to develop a framework that assists CsM with ERM alignment within the financial industry, supported by practical guidance for the implementation of the proposed framework.* Overall,

the contribution of the empirical findings is that indicated determinants, barriers, readiness (maturity), and capacity sustain risk governance. Moreover, it determines the regrouping of a few layers of control that provide clearer direction for connecting all components of organisational mission and vision. It has facilitated an identification of continuous process. This means that organisational strategy and objectives are used as a main point of reference in order to sustain effectiveness, sustainability, and risk resiliency.

From the outcome of this investigation, it is possible to finish with final conclusions, contributions, and limitations of this research; all of which will follow in the next chapter, Chapter 8.

8. Chapter Eight: Conclusions and Recommendations

8.1 Introduction

This chapter presents a synthesis of the research findings to provide evidence of how the aims of this research have been fulfilled. Linking each chapter's contribution, this final chapter restates the implications, contribution, potential impact and limitations of the findings. It explores how the research aims were achieved, how the research objectives were investigated and how the research questions were answered. Section 8.2 begins by justifying the research scope, followed by an explanation of how the research aims were achieved in Section 8.3. Sections 8.4 and 8.5 provide a brief overview of how the research objectives and research questions were addressed. Section 8.6 outlines limitations while Sections 8.7 and 8.8 discuss the theoretical and practical contribution of this research. Finally, Section 8.9 explains the emergent themes influencing risk governance practices and how they might be tackled in the future.

8.2 Research justification

Interest in organisational risk resiliency has registered significant consideration, but there are still unanswered questions as to why organisations are unsuccessful in applying effective risk security practices across all levels. Having a robust mechanism to deal with a variety of risks efficiently and in alignment with organisational strategy has always been something that organisations strive to accomplish. Changes in internal and external pressure have required organisations to turn their consideration from silo operational and managerial risk control to strategic approaches to ensure optimal achievement of the organisation's mission, strategy and objectives.

This research was intended to investigate possible approaches for enabling a more enhanced strategic approach to respond to the extended exposure to all types of risks; to move towards a proactive approach that ensures enterprise-wide risk governance with anticipation. The two types of organisational risks cannot be carried out in isolation, and so this research explored whether realignment of risk control and risk oversight of CsM and ERM support the establishment of enterprise-wide risk governance. This research responds to the need for harmonised risk handling, reporting, analysis, mitigation and resiliency across the whole organisation. Alignment (interconnectivity and partnership) can place the entire organisation in a more enhanced state of security through a unified perspective of control, accountability and decision making. Debates in this subject area have been centred on separate disciplines

of ERM, CsM and strategic alignment as an effective alternative to sustain organisational risk strategy as together they convey all capabilities in an integrated manner as opposed to siloed controls.

Weighing up the evidence, the research findings suggest that *CsM-ERM Strategic Alignment Framework* supports establishment of enterprise-wide risk governance. To reflect on the extent to which this was achieved, the sections below outline how the research results were identified.

8.3 Results determined by the research aims

The aims of a research project broadly state the main goal, scope and intent of the research, as well as defining the contribution and limitations of investigation (Thomas and Hodges, 2010; Stokes and Wall, 2014; Saunders and Lewis, 2018). In order to understand if the research aims have been achieved, the following section presents an overview of results.

Research Aim 1 was to investigate the alignment of CsM with ERM within the financial industry. The research proposition was guided by Research Aim 1 in all chapters. The thesis conceptually and empirically investigated the alignment of CsM with ERM within the financial industry. More specifically, the research aims were achieved through the tactical use of research objectives and research questions. As prior literature on the research problem was scarce, the investigation considered ERM, CsM and strategic alignment paradigms individually. It was found that alignment of CsM with ERM within the financial industry is feasible, yet is not common practice amongst the organisations sampled, being applied in most cases only partially. Second, it was identified that the empirical results are similar to previous studies with slight differences. Respondents confirmed that risk controls and risk oversight are immature and fragmented. This suggests that Research Aim 1 was validated by both theoretical and practical insights.

Research Aim 2 was to develop a framework that assists CsM with ERM alignment within the financial industry, supported by practical guidance for the implementation of the proposed framework. To achieve this the research brought together the literature review (derivate one), the systematic literature evaluation (derivate two), the research gap (derivate three), supporting theories (derivate four), supporting frameworks (derivate five) and empirical findings (derivate six) to generate a framework that supports an integrated approach that yields enhanced preparedness. By concentrating ERM capabilities and CsM capabilities in the same scope and not separating them as done in the past, the potential for

achieving strategic objectives, strategic planning and optimised processes balances the alignment of risk appetite with exposure, encourages tolerance, aids communication and enables risk prioritisation. All of this can enhance an organisation's overalls risk resiliency, preparedness and effectiveness to respond to risk events.

8.4 Results determined by the research objectives

Unlike research aims, research objectives are more specific in explaining the processes of how the aims are achieved (Thomas and Hodges, 2010; Stokes and Wall, 2014; Saunders and Lewis, 2018).

Research Objective 1: The first objective of this research was to identify, analyse and critically evaluate academic, industry-based and regulatory literature regarding ERM, CsM and their alignment, to explore the current state of the subject. Chapter One defined debates amongst academics, practitioners and regulators on how the financial industry's risk resiliency depends upon its ability to handle risk holistically. It highlighted the gap and necessity of alignment between CsM and ERM to deploy holistic risk governance. Chapter Two determined that alignment of CsM with ERM encounters numerous challenges in theory and practice.

The scarceness of literature focusing specifically on the topic led to confusion at some points. Exploration of a phenomenon uses key literature to recognise the literature legacy related to the research topic and a three-fold analysis based on academics', practitioners' and regulators' viewpoints. The second chapter reconfirmed that the organisational risk oversight is under-researched and the alignment of CsM with ERM is a joint effort that contributes to a holistic internal control of risks. The top eight challenges identified in prior research were: (1) the scarceness of strategic alignment literature that focused on CsM and ERM; (2) partial understanding of implementation benefits by stakeholders; (3) low level of alignment maturity within organisations; (4) lack of bottom-up consideration for alignment; (5) lack of coherent terminology and theory, and thus fragmented practices; (6) lack of common guidance for implementation; (7) low level of cyber risk awareness inside organisations; and (8) resiliency challenges due to siloed approaches.

Chapter Three further evaluated academic, industry-based and regulatory framework models to explore the typology of contributors, categorising prior research into four typologies: adoption, implementation, maturity assessment and compliance. This approach further supported an understanding of the literature. It moved beyond the descriptive exploration

and systematically evaluated the literature to explore why alignment is necessary, how it is sustained, what the key debates regarding the three domains are, and how theory, practice and regulatory framework interrelate. CsM and ERM have been only partially addressed in prior studies, with diverse topics, diverse approaches and varied viewpoints. These findings demonstrate that recent developments of risk practice are fragmented and focus significantly on silo approaches. The analysis of the literature also revealed that alignment of CsM with ERM can enhance a superior risk assessment, mitigation and resilience in an organisation and thus help towards reducing risk profile. Of much more concern is that transferring the whole organisation into an enhanced state of cybersecurity has proved to be a challenging task. A lack of integrated approaches amplified the efforts required and the required allocation of resources, strategic planning and implied allocation of costs.

The different types of evidence identified prove that further work needs to be done to manage risk strategically and sustain organisations effectively and in the long term.

Research Objective 2: The second objective of this research was to analyse the financial industry's environment and current practices regarding alignment. To fulfil this objective, this research had two approaches: revising prior literature and addressing questions to respondents during the semi-structured interviews.

The first approach showed that trends in literature regarding alignment were segregated in layers of neutral alignment, alignment of IT with business alignment, IS with RM alignment and IS with ERM alignment. There was little material on the integration of CsM with ERM. A lack of literature on alignment that guides implementation was also identified, and a significant body of literature remains conceptual, focusing mainly on adoption aspects. It has various paths of alignment (e.g. structural, cultural), lacking a multi-dimensional approach. Structural alignment shows inadequate structural collaboration and restrained organisational change behaviour. Cultural alignment was also immature. Research has tended to have been carried by academics rather than practitioners or regulators. Although in the case of CsM and ERM some contributors have addressed this problem and over recent years' alignment has received attention, it has unfortunately been applied in isolation (e.g. IT-centric, RM business-centric).

The empirical findings identified similar problems. Much empirical evidence shows that organisations struggle to align risk functions. The findings also indicate that alignment maturity of CsM and ERM is yet to be achieved. These results further support the idea that

alignment is immature, hence a small percentage of respondents claimed to have reached full maturity. The evidence demonstrated that siloed practices exist and remain constrained by determinants, reimbursement, inhibitors and readiness among all three domains. Whilst evidence determined the status of alignment in current practice as being immature, the surprising result was that alignment acceptability was recognised as being valuable (75%). Four dimensions of alignment were identified: strategic, structural, cultural and operational. The basic premise for this argument is that previous literature partially addressed the alignment dimensions and that empirical evidence suggests beneficial implications of alignment.

Research Objective 3: The third objective of this research was to review and evaluate the effectiveness of current CsM and ERM frameworks. Following the assessment of frameworks, the result pertaining to this objective were presented in Chapter Four. An in-depth overview of related CsM and ERM frameworks showed that there is a lack of supporting frameworks for CsM and ERM alignment. The available evidence consists of models or frameworks that consider the alignment through the perspective of IT alignment with business alignment. Additionally, the scope of most frameworks is generic and does not address financial industry-specific needs. Even though an array of approaches was identified, ERM, CsM and alignment have specific frameworks granulated to each domain. It was concluded that prior contributors have tended to adopt a disjointed approach to CsM so it addresses the research problem in isolation, stranded in fractional types of alignment: IT, IS, IA, with a later influence of RM. Scarce consideration for practised alignment was identified because the alignment paradigm was mainly developed by scholars. As an example, the assessment of literature on alignment shows that the main influencers are Henderson and Venkatraman (1993) and Luftman (2000).

Consequently, alignment fails to address the current needs of organisations. However, despite the drawbacks of previous frameworks of CsM, ERM and alignment, taken together as a compound they can form examples of good practice, especially as on their own they are limited to offering a partial insight into the research problem. Therefore, the implications of CsM, ERM and alignment frameworks evaluation provides support for the Research Framework (third derivation). Overall, it can be concluded that Research Objective 3 was addressed, helping to support the achievement of Research Aim 2.

Research Objective 4: The fourth objective of this research was to evaluate the potential and the limitations of strategic alignment between CsM and ERM within the financial industry, supported by practical guidance. This analysis compounds both theoretical and empirical findings. Many current frameworks revolve around IT, IS or RM alignment. The literature showed that strategic alignment supports the effects and interdependencies of an internal environment within today's business context. It delegates departmental communication to identify wider vulnerabilities in terms of structure and processes alignment, and supports acknowledgement of management directions with the driving principles of philosophy, appetite and direction. It ensures that implementation is in accordance with organisation objectives, capabilities and limitations, identifying current situations (assets, threats, vulnerabilities and control) and risk owners, and is accountable across business units, the source of threats and leveraging enterprise-wide security. Strategic alignment offers beneficial accountability, transparency, self-preservation and response preparedness to ensure that negligence is avoided and fewer disruptive actions exist in terms of achieving organisational value creation and strategy preservation. Objective 4 is similar to the categorisation of research made in Quadrant 1 Adoption (see Chapter 3), which referred to adoption.

Consequently, the value proposition of strategic alignment between CsM and ERM incorporates the modern CsM that adopts wider asset protection (not only partially as in IS or IT) and the broader principles of ERM. This practice has been found to be scarcely considered (see Chapter 4). Thus, the potential of strategic alignment between CsM and ERM is that it provides an understanding of how organisational appetite, culture, governance, risk oversight, risk profile, maturity, compliance, structure, performance and leadership in strategic risk governance. Previously, these aspects have often been investigated in isolation.

Consistent with the literature, the empirical results found that a formalised security procedure demonstrates due care for risk oversight. The potential of alignment would expect to address the collaborative efforts to support effectiveness of control. Among the top benefits considered by respondents were avoidance of duplication, strategic alignment, enterprise-wide risk measurement, communication and prioritisation of risks (see Chapters 6 and 7). To develop a full picture of the strategic alignment components, additional effects of ERM and CsM were examined. It was found that CsM performance is due to compliance, competitive advantage, resilience and organisational effectiveness. Likewise, ERM benefits

(see Table 2-1) trigger other benefits of culture enhancement, fulfilment of shareholders' requirements or fulfilment of regulatory requirements. These results further support the idea that reframing enterprise-wide risk governance is needed. Research Objective 4 identified both benefits and barriers for strategic alignment.

8.5 Results determined by the research questions

The research questions address the research gap and what exactly is missing, thus ensuring that the research is consistent with the research aims. Therefore, research questions are most often seen as a continuation of aims and objectives (Thomas and Hodges, 2010; Stokes and Wall, 2014; Saunders and Lewis, 2018). The research questions re-address the objectives to emphasise aims.

Research Question 1: *Why does a strategic alignment of CsM and ERM sustain a financial business in the long term?*

It was identified that an alignment of both paradigms sustains risk resiliency holistically. Both literature and empirical findings indicate the importance of tying together all risk controls and oversight functions to ensure increased resiliency and effectiveness. Given the nature of the financial industry, this aspect of strategically securing financial organisations has been given more impetuous due to the increased constraints of the external environment. Evidence shows that strategic alignment sustains risk governance by utilising resources, reducing cost, creating visibility of risks, demanding risk prioritisation, ensuring enterprise-wide risk measurement, and providing compliance and thus effectiveness, to strengthen an organisation security posture.

Research Question 2: *What are the key issues that impede the alignment process in the financial industry regarding CsM and ERM?*

This question re-addresses Research Objective 4. It was found that the role of RM can no longer act as a separate and reactive function. Chapter Six collected and analysed empirical data to examine current maturity and likely solutions. It was identified that each domain encounters similar challenges, yet slightly different in type. For instance, both ERM and CsM were reported to encounter issues related to external pressure (e.g. risk and threats, standardised practice, regulations). Additionally, resource allocation and a lack of direction and capabilities were similar to a certain level, whilst the alignment paradigm's main focus

indicated inappropriate governance (e.g. cultural inefficiencies resulting in inappropriate governance) and employees skills deficiencies.

The findings confirm inhibitors as being consistent with the findings of prior research. ERM is indicated to be inhibited by capability and a lack of research guidance, while CsM shows similar impediments, with inhibitors being people-centric and strategic-centric, the alignment indicates enterprise-wide issues related to governance, either culturally or in terms of inappropriate governance. Similarly, the other two domains outline people-centric issues.

Research Question 3: *How are theory, practice and regulation direction applied regarding the current alignment of CsM and ERM within the financial industry?*

Like the literature findings, when applied to industry practice it was discovered that alignment of CsM with ERM is scarce and only partially applied. Sections 6.2.4 and 7.2.3 support this view and show the identified alignment of CsM and ERM alignment. Research Objective 2 addressed this matter and was identified an immature approach.

Research Question 4: *What effects have the implementation of the new framework?*

This question links with Objective 4 of this research and the results of Chapter Six. It was concluded by empirical findings that strategic alignment supports enterprise-wide risk governance.

8.6 Research limitations

This research aimed to fill the gap in strategic risk governance in financial organisations. It had some limitations that are highlighted in this section. A limitation of research embodies the factors that can hinder an investigation under specific rules and methods unsettled by a researcher. Such limitation can restrict the investigation and the methodology or results (Molina, 2015; Mertler, 2015). Therefore, some possible limitations of the current research are related to the literature fieldwork, research design, researcher's biases and time framework.

8.6.1 Literature research limitations

Referring to the literature fieldwork, the content of the research is limited to the theories, practices and regulations applied to various industries. Thus, the initial data gathering is focused on a general perspective due to the lack of literature that addresses the financial

industry. To counteract this limitation, the phenomenon is later analysed within its context via the empirical data collected.

Researcher bias is another possible limitation due to any interpretive analysis bias that might appear in the interview process with practitioners.

Another limitation is time, which is a confined by the cross-sectional analysis due to the time constraint of the research timeline. This restriction is acknowledged by the researcher and research phenomenology evolution has been evaluated since the early 1990s, even if longitudinal research might enhance the results.

Additionally, to integrate the practitioners' view, the papers selected were limited to reports, white papers and industry standards. The reports selected were the production of consultancy organisations well-recognised for their due diligence practices. The standards selected were only the ones that focused on strategic approach of RM, ERM, IS and CsM. Despite focusing on the financial industry, some standards and literature are generic and thus can be generally applied to all industries. Standards with specific reference to alignment are non-existent and therefore analysis comprised theoretical models and frameworks.

8.6.2 Research design limitations

The research used qualitative methods, which are open to possible subjectivity. A lack of quantitative data is a limitation specific to qualitative studies and perhaps the use of mixed methods would add additional views on the research problem even if quantitative in their nature. Analysis of Chapters Three and Four aimed to address this limitation.

With regards to primary data collection, another limitation was related to the respondents' profiles. Selection of respondents was made based on a predefined set of expectations related to their professional experience and credentials, and thus they were selected based on their expertise in the strategic side of risk governance. Conceivably, future research would include views of the technical and operational side to be more inclusive. For the purpose of this research, no technical views were considered. Instead, operational, structural and cultural alignment was considered while the main focus remained strategic.

Other aspects such as age or gender were intentionally avoided due to the complexity of possible results. In this case, perhaps a future comparison of gender and age of respondents would create a better understanding of all professional changes.

Another limitation is the number of respondents. The 26 respondents were from 25 organisations, with only two respondents from the same company. It was not possible to select only companies that had both mechanisms in place. Contrasting CsM and ERM within the same organisation would also be valuable in widening the understanding of practices. Perhaps a higher number of sampled organisations would add an additional contribution.

Research that applies a questionnaire to subordinates from lower levels of implementation may generate a larger number of respondents and reveal differences. Of more interest would be longitudinal research to explore the performance of organisations in deploying alignment of CsM and ERM or related fields. Another research limitation refers to geographical dispersion of respondents. This research was restricted to seven countries and possibly global research would add an expanded view across a larger sample of organisations. This research was also limited to respondents who spoke English either as a first or second language. The problem with this approach was that it limited the pool of respondents and thus the number of interviews.

Another limitation is that the usability of *CsM-ERM Strategic Alignment Framework* has not been empirically tested to comprehend the whole effects of pre- and post-implementation in a real-life context. Instead, it has been validated by empirical findings and the other five derivates (literature review; systematic literature evaluation; research gap; supporting theories; supporting frameworks).

8.7 Theoretical contribution

This research has shed light on prior research, adding a contemporary light on the literature while suggesting an update to the body of knowledge through a paradigm shift of holistic risk governance driven by the alignment theory. By exploring the effects of CsM and ERM alignment, it aimed to endorse performance, value enhancement and risk resilience for financial organisations. The research findings found a granular theoretical legacy, most often stranded on the siloed technical and/or operational side.

Accordingly, this research contributes to theory with key contributions:

(1) **substantiated prior literature** by offering a broader understanding of the extant literature with a three-dimensional perspective of academics, practitioners and regulators determinants, instead of a mono view. It incorporates what the current theory, best practices and industry standards, laws and regulations prescribe.

(2) **explored a theoretical reframing of the problem in the context of strategic alignment** which highlights the potential usefulness of a holistic approach. While previous literature yielded limited empirical studies, addressing only two elements for alignment (e.g. IT security with either and/or business strategy or RM), the current research recommends the integration of two types of strategies (CsM and ERM), with an additional third element co-aligned towards the organisational strategy. To overcome the negative effects of siloed approaches, this research contributes to the theory by underpinning the homogeneity of the ERM, CsM and Alignment discipline. Thus, it contributes altogether and extends the understanding of enterprise-wide governance and bridging the theoretical gaps–to ensure the maximisation of the overall organisational strategy. The strength of the proposed approach is that it identifies the cause and consequences and influences towards an approach that recommends holistic and rapid adaptation to evolving risks and challenges to ensure the achievement of an organisation strategy. The research does not dismiss previous research and instead uses the findings to acquire a thoughtful view of the phenomenon legacy to provide evidence on how all three paradigms can have a positive contribution to the research topic.

(3) **contributed by demonstrating knowledge gaps ─** extensively examining how prior research adopted disjointed risk governance, thus addressing the research problem in isolation. While much attention has been centred on the separate disciplines of ERM, CSM and Alignment, the Researcher was constrained to deploy the investigation by examining the ERM, CsM and strategic alignment paradigms separately. It was found that the alignment of CsM with ERM within the financial industry is scarce and yet viable and sustainable. A key aspect of this contribution is that it validates the progress/maturity of each paradigm. For instance, it was found that CsM is grounded in prior IT, IS, IA literature, with a later influence of RM. Accordingly, the findings concluded that CsM theory was found fragmented and most often still perceived as an IT problem and most often researched in isolations.

(4) **extended the understanding of the phenomenon through the lenses of alignment** which revealed useful extension and enhancement within the contingency and institutional theory. The Researcher advocates that the contingency and institutional theories are two facets of the alignment itself. For example, the institutional theory implies coercive pressure (regulations), mimetic pressure (internal pressure) and normative pressure (skillset, education, awareness) for achieving an organisation's objectives. Each of the theories has specific philosophical perspectives and their

association illustrates two different insights (institutional norms and variations of contingencies) with a commonality based on alignment enhancement. Altogether, Contingency and Institutional theories reflect on the contingencies and dependent factors that need to align within an internal and external environment along with their causal relationship (Sutton and Staw, 1995) and institutional norms. The difference lies in the fact that each of them focuses on a distinct perspective or 'fit' and offers a different outcome. For example, the Contingency Theory concentrates on achieving an internal fit with an external environment, whereas the Institutional Theory focuses on making an external fit (e.g. recognition of conformity, external support) by adapting its internal environment.

The Institutional Theory refers to the institutional constraints that shape organisations' behaviour. Whilst the Contingency Theory focuses on how organisations can be managed and coordinated as a whole, marrying organisational structures, systems, and external environments; the association of the two theories is valuable hence both of them have roots in the Organisational Theory and are related to organisation design/structure.

(5) **re-contextualised contingency and institutional theory in the risk context** and compared any intercorrelations in order to determine its suitability within a CsM and ERM alignment. Institutional theory addresses what sets the condition of an action to understand how and why institutions interact under internal and external environmental pressures.

The merger of both theories helps to explain how mimetic, coercive, and normative pressures affect the interdepartmental linkage compliance on daily work practices. As organisations are unique, a combination of both Contingency and Institutional Theories is advocated by the Researcher with the purpose to explore and explain how a correlation between the two can ensure performance, sustainability and effective strategic alignment between CsM with ERM and business strategy. It outlines how each element can complement the other when striving towards a common goal, extracting the value of each and understanding potential inhibitors in implementation. It recommends a paradigm shift of risk governance contextualised in the strategic approach that correlates the two theories and the research problem grounded on the premises of concepts and principles of governance, alignment, communication and coordination of the interdepartmental control functions. Henceforth, it is centric for an organisation to fit its organisational characteristics with external pressure. Alignment is firstly about marrying CsM and

ERM with organisation strategy and objectives. Secondly, it seeks to respond to external pressure and risks.

The Contingency Theory strategically provides consensus to align the CsM with ERM management functions such as strategy alignment, objectives alignment, planning alignment, structural and operational organisation with social systems, and leading and control—all intended to better cope with external pressure and risks. Thus, this research has rejected a prescribed universal approach and in turn, recommended an optimised and unique response corresponding to the situation as determined by events and circumstance. Contingency shifts to a security perspective, whereas prevention and detection help organisations to react and respond.

Nevertheless, the terminology of alignment registers various similarities in strategic management (i.e. both the Contingency Theory and Institutional Theory use the term 'fit'). Moreover, contingency and institutional fit approaches are both co-alignment approaches that focus on different types of synergy between the organisation and its environment (Vorberda *et al*., 2011, p. 1044). This is relevant when proving the theories' commonality and appropriateness. On this ground, this research positions the theoretical dimension of alignment in the context of Contingency Theory and Institutional Theory and organisational goals; it combines the fit/integration theoretical lenses along with achieving legitimacy and sustainability (Semler, 1997). For example, the Contingency Theory has consideration for an organisation's strategy, structure, culture, organisational design, processes, leadership, technology, and structural alignment. Whilst, the Institutional Theory considers the value, normative rules, legitimacy, beliefs, principles, practices, structures, processes, obligations, behaviour, ethics, and social systems establishing command and assigning responsibilities.

Overall, the re-contextualisation of theories brings together internal variables, external variables, strategy and management. The Contingency Theory states that every organisation and every organisation's situation/context is unique, and thus needs to be adapted and tailored. Both theories strive to identify and solve organisation issues in an optimised manner, ensuring organisational efficiency (i.e. objectives achievement with limited resources) rather than general efficiency (merely objectives achievement), and with the intention of yielding profitability, competitive advantage (Hatch and Cunliffe, 2013), and sustainability.

(6) **determined the main success criteria and interdependencies across prior ERM literature**. Identified that it varies between value, performance, appetite, culture, and governance, most often addressed in isolation. Therefore, this research makes a contribution to the ERM criteria of success and compiles them in the context of the research problem.

(7) **demonstrated that the literature related to alignment is scarce** and thus lacks coherent theory when researching the CsM alignment to ERM. Accordingly, this research validated that prior research was IT-centric. Henceforth, the alignment literature transitioned from a strategic alignment in general, towards IT alignment with business strategy. Moreover, the findings demonstrate that there is a scarce industry-specific focus – namely the financial industry (ERM has a more significant consideration, while CsM and alignment is addressed generically). The literature review outlines that the strategic alignment of CsM with ERM is scarce in academic literature.

(8) **identified a multi-dimensional array of alignment approaches** in the literature and concluded that there are inconsistencies hence prior approaches failed to understand the interdependencies between the social, strategic, operational, cultural, social, and intellectual dimensions. Identified granular theoretical frameworks ─ prior frameworks revealed shortcomings in terms of the completeness of the implementation stages. A pattern was identified in the theoretical framework grounded in various phases such as planning, implementing, controlling, and assessing risk (also known as by Deming's PDCA cycle method). Accordingly, the systematic analysis identified a pattern in adoption, implementation, maturity assessment and compliance. Some of the frameworks focused on adoption and implementation whereas a significant number of the frameworks analysed predominantly focused on the maturity assessment. In addition, it discovered patterns and similarities in both CsM and ERM earlier theoretical frameworks. Most often, there are mirroring approaches regarding the framework stages. For instance, there is considerable similarity on the number and order of phases. For instance, it was found that ERM and CsM are seen as minimum compliance (reactive measure rather than proactive controls). On the other hand, previous CsM frameworks have incorporated different sub-domains of CsM and have shown variations in perspective. Overall, the research has shown that all three domains failed to address the alignment of CsM and ERM holistically. The identified evidence supports the key argument that prior alignment frameworks have not addressed a complete approach and remained centred around IT alignment. The proposed solution of alignment considers all

phases (Phase One: ‘baseline expectations’, Phase Two: ‘mandate managerial directions’, Phase Three: ‘establishment of strategic directions’, Phase Four: ‘implement managerial directions’, Phase Five ‘Monitoring and reviewing practices’) and requires an interrelated alignment of CsM and ERM management, strategies, planning, structure, processes, skills, competencies, and culture acknowledged at all levels, in order to instil communication and mitigation on a common ground throughout business units. These theoretical premises can help to reduce over-investment, effort, and overlaps, as well as develop organisational awareness and enterprise-wide effectiveness.

(9) **demonstrated the existence of siloed approaches** – it compiled evidence from six derivates (literature review, systematic literature evaluation, theoretical frameworks evaluation, research gap, supporting theories, prior frameworks derivations) to prove that prioritisation in security decision is still seen from a silo perspective, resulting in the mismanagement of risks and misalignment. Also, the research supplied empirical arguments on the challenges of alignment and thus, enriched the growing conceptual literature by extending an understanding into how it impacts an organisation. And, so the theoretical CsM - ERM Strategic Alignment Framework justifies why a common governance creates a ‘common mechanism’ that would prioritise, enable and support initiatives, unify the overall risk planning, and prioritise risk investments based on current organisational needs (i.e. not on subjective departmental needs - IT department might have different investment security priorities than organisation security); thus alignment shall support the identification of overall necessity on a multi-layered security basis. Moreover, the theoretical premises evidenced that the alignment improves the risk governance transparency and risk oversight across the whole organisation.

(10) **developed a conceptual framework** able to support the alignment of strategies through the inclusion of ERM principles and theoretical premises of institutional and contingency concepts in order to yield enhanced preparedness in forthcoming risk events. By concentrating ERM capabilities and CsM capabilities in the same scope and not separating them as done in the past it proposes a shift from the traditional silo approach. Potentially, the conceptual framework provides a guide to new studies when considering a potential area of improvement with the alignment tenets and organisational components.

To support the validity of the above mentioned, a set of publications were authored as a supplementary piece of evidence which confirms that this research has contributed to the theory.

8.8 Practical contribution

This research is relevant to financial organisations since it proposes an alternative way of managing risks holistically and comprehensively, and accordingly recommends co-alignment in various layers of protection. It contributes by extending the view on how an organisation can achieve enterprise-wide resiliency, conformance, performance, sustainability, and efficiency utilising the alignment of CsM with ERM.

The practical research contribution includes:

- **portraying how managing risk holistically has become a factor** that influences and/or leverage risk control performance. Empirical findings confirmed that misalignment has become a growing problem for financial organisations, and it was thus acknowledged that both ERM and CsM received heightened demands. Thereby, the findings advance an understanding that ERM implementation remains under increased external pressure, such as meeting regulatory requirements, recognition of compliance, and organisations' strategic governance. Whilst, for CsM it was validated that is being implemented due to increasing threats velocity and complexity, industry standards influence, performance-centric goals, compliance, competitive advantage and ultimately, resiliency; besides it presents the various perceptions of industry practitioners showing that emphasis is placed on aggregating answers on how to respond to exposure' ramifications towards enterprise-wide risks and cyber risks altogether and what is needed to sustain a financial business in the long term;
- **identifying gaps in how risks are managed.** It was found that within many organisations, managing cyber risk remained grounded on Information Security departments or IT security, whereas ERM is most often applied through traditional RM. The empirical findings prove a gap within the practice, showing that overcoming this problem remains driven by a silo perspective, across departments units, resulting in internal mismanagement. The results also echo positive approaches within the industry that recommends the use of modern CsM to ensure wider protection;
- **reporting patterns for effective risk foresight** (benchmark) across various financial organisations and to which an organisation shall abide in order to ensure proper resiliency and efficiency. A closer look at the results indicates that value in

aligning planning, control, measurement, and mitigation is measured in one compound mechanism;

- **providing evidence of current ERM immaturity** among various financial organisations and finding it immature, with an implementation maturity rate of 38.46%; whilst also providing insights into the main ERM implementation drawbacks and showing that despite strong development, the financial organisations still struggle with undeveloped practice (immature ERM), lack of capability and lack of resources;
- **acknowledging dependency on key determinants for achieving effective ERM** implementation. Found evidence of the key determinants specific for the financial industry: strategic governance, differentiation capabilities and enhanced risk resiliency. All of which focus on control, compliance and knowledge; likewise identified patterns in barriers, readiness (maturity), and the capacity of organisations to sustain holistic risk governance;
- **finding the main ERM inhibitors specific for the financial industry**: (1) *resources-related*: - cost, data and information, people and skills; (2) *direction-related*: strategy and leadership; (3) *capability-related*: maturity, culture, lack of education and awareness; (4) *pressure-related*: risks and threats, standardised practice and regulations;
- **obtaining important insights into the main factors that impact alignment** readiness within an organisation's departments; the results show a positive effect among the top three factors: communication, joint risk ownership and maturity;
- **revealing that within practice CsM depends on certain key determinants** for successfully implementing: (1) internal - initiative and culture; and (2) external - cyber threats velocity and complexity; regulatory pressure and standards; on the other hand, identified that for CsM, the main inhibitors are people-centric (culture) and strategic-centric (silos and cost) factors; the findings offer insights into the fact that financial organisations most often fail due to people-centric and strategic-centric issues (e.g. lack of resources, direction, capability, and pressure); and so ascertain that these factors are essential for achieving successful CsM implementation, instead of technology reliance.

- **concluding that within the practice the alignment inhibitors** are related to (1) governance: (e.g. cultural deficiencies, inappropriate governance) and (2) employee's skills deficiencies;
- **determining the main side effects of misalignment feared by the financial organisation**. The findings highlight that organisations are concerned with three top concerns: reputational loss, regulatory consequences and financial loss.
- **outlining immature risk governance** within the financial industry, pointing towards challenges and barriers in achieving value and holistic risk resiliency; thus, showing that managing risk holistically remains a challenge for most organisations despite awareness, considerations and investments; empirical findings indicate that readiness of alignment maturity of CsM and ERM is yet to be achieved henceforth implementation was reported to be in proportion of 38.46%. The data obtained demonstrate that practices remain fragmented in all three domains - CsM, ERM and Alignment. Such results highlight the importance of an organisation to understand its current risk profile, exposure and capabilities when setting strategic directions as well as implementing corrective measures.
- **obtaining empirical evidence which shows an overlap of four dimensions of alignment**. It is conceivable that implementation prescribes the use of the intellectual (strategic), structural, cultural, and operational dimensions of alignment because all interrelate and are dependable on each other; it maps the principles of strategic alignment and reflects onto the value of multi-dimensional alignment that increases risk governance effectiveness;
- **determining the essential factors needed in achieving maturity, risk control and risk oversight;** provided empirical evidence which reiterates how organisational appetite, strategy, culture, governance, risk oversight, risk profile, maturity, compliance, structure, performance, leadership and alignment expectations may impact a whole organisation. Above all, it was demonstrated that organisational strategy and objectives remain the main point of reference when implementing alignment;
- **contributed to clarifying the usefulness of alignment,** stressing that practitioners agree with the alignment's benefits in a proportion of 69.23% ─ and identifying a potential of 75% interest/acceptability to adopt the alignment paradigm. Therefore, the research provided empirical evidence that alignment can create a common

mechanism that would prioritise risk, support initiatives, unify strategic planning, support informed decisions and prioritise investments as a security enabler based on current organisational needs rather than on subjective departmental needs. By doing so, it explored the overall necessity for multi-layered security driven by the purpose of serving the organisational mission and vision in a unified manner; along with the preservation of resiliency that advocates the idea of rejecting the 'organisational dissociation';

- **leveraging a reconsideration of traditional risk governance** when aligning CsM with ERM and business strategy. It enabled insights into how practitioners employ risk governance to optimise the use of resources, lower costs and reduce effort. Determined that alignment influences ROI, avoids duplication and strategic alignment, reaches enterprise-wide communication and the prioritisation of risks; emphasised that misalignment can be mitigated with the collaborative effort of CsM and ERM, thus shedding light on a common governance across all three domains ─ emphasising the benefits of implementing the frameworks ─ value creation, value capture, value enhancement, organisational effectiveness, performance and risk foresight; the unified framework combines risk control capabilities with risk oversight capabilities in order to reach an enterprise-wide risk governance capability. The presented evidence that alignment creates collaboration between departments, points towards the view that the cost of risk awareness can be decreased when ERM and cybersecurity risks are compiled altogether;
- **proposing a framework capable of acting as an inside service**, risk function and guideline for an organisation. The framework shows the importance of considering all risk controls (physical, technical and procedural) and oversight functions pertaining to the main organisational goal. The framework embodies a representation of how a strategic organisational statement can achieve its main objective. Therefore, through the implementation of the framework, an organisation can reduce over-investment and the duplication of efforts when adapting to internal and external changes (Miles *et al.*, 1978), avoiding the overlapping of functions and the duplication of resource allocation. This implies that the framework proposes to support organisations' risk governance strategies and procedures by emphasising strategic responsibility, leadership, accountability and enterprise-wide risk governance with the intention to seize opportunities, make risk-informed decisions and contribute to the achievement of resilience against enterprise risks and cyber

risks; respectively reaching risk governance effectiveness and overall risk foresight (see Chapter 4, Sections 4.2 and Subsection 4.4.4); emphasises the impact of internal strategy in alignment, paying consideration to external requirements. Sets of internal directions are in balance with the identified external directions in order to cope with the external environment;

- **shedding new light on the ERM contribution** when aligning with CsM, helping to avoid bias in decisions related to investments or budget allocation. The findings highlighted that little is known about the implication of correlating the capabilities of CsM with ERM while risk appetite and tolerance is aligned with the organisational risk appetite, risk tolerance and acceptable residual risk. The research presented the effects and benefits of creating common risk governance for risk control and risk oversight to support the achievement of the overall business strategy and enterprise-wide risk governance capability to enhance overall risk foresight capabilities for financial organisations. The insights identified the support considerations of internal and external factors that entails systematic re-alignment as an enabler for reaching a higher level of maturity;
- **evidencing gaps in existing practitioners' methodologies,** demonstrating that compliance is not merely about meeting regulatory expectation/rules. It can help to have a unified mechanism to ensure the efficiency of risk oversight and provide insight into how due care leads, in turn, to competitive advantages, increasing business performance and risk resiliency;
- **expanding an understanding into the implications of the multi-spectrum of variables** when implementing the strategic alignment (e.g. governance, strategy, risk appetite, risk tolerance, structure, culture, organisational design, processes, leadership, technology, structural alignment, communication, competence, partnerships) that can impact the return on investment and performance;
- **recommending a mindset change**, switching from reactive to proactive risk strategies to ensure a continuous identification for internal and external challenges; accordingly offer insights into the critical importance to integrate shared risk oversight (unified capabilities of reporting, analysis and mitigation). Thus, action prioritisation is made in alignment with all three components and ensures that it leads to an optimised response, based on organisational needs and the risk profile, whereas a silo valuation presumably leads to incorrect responses and misalignment;

- **incorporating the review of industry best practices** for both CsM and ERM, elaborating how most are often generic and granular instead of specifically addressing the financial industry-specific needs (e.g. regulatory compliance). In particular, the summarised insights of industry best practices focus attention to compare and predetermine a baseline for control function effectiveness;
- **finding evidence to justify the value of a multi-dimensional strategic alignment** correlated with cultural, operational and structural alignment; for example, providing a deeper insight into cultural dimensions as a significant determinant in implementation, hence the human aspect is a variable (informal procedures, norms, beliefs, behaviour, ethics);
- **demonstrating an insufficient understanding of holistic risk governance** within financial organisations and drawing attention to the management of financial organisations towards the negative effects of the siloed approach and to the importance of supporting a coherent alignment across strategy, policy and guidance to succeed the achievement of effective risk governance;
- **determining a benchmark** towards a new holistic strategic direction in managing risks, emphasising an understanding of a *real-world* problem and proposing an alternative solution of *CsM - ERM Strategic Alignment Framework* to avoid the duplication of strategies, policies, guidelines, and procedures; the framework advocates a common mechanism of control, monitoring, measuring, and ultimately formulating a common solution to increase resiliency; the proposed Framework supports the acknowledgement of management directions (driving principles: philosophy, appetite, and directions) beforehand and optimises as needed to predict strategic requirements; furthermore, the proposed solution supports an informed implementation which assesses the organisational risk profile based on a tailored maturity model diagnosis extracted from industry standards best practices. The proposed approach can be readily used in practice because it articulates the gaps in each paradigm (ERM, CsM and strategic alignment) and recommends an approach to overcome drawbacks, understanding reimbursement and inhibitors.
- **evidencing the value of employing a comprehensive approach**. Demonstrated that the *CsM - ERM Strategic Alignment Framework* improves due care for risk oversight, the effectiveness of control, collaboration, communication, co-alignment, risk accountability, transparency, self-preservation, and response preparedness, limiting

and anticipating potential disruption. The framework provision shared communication across an organisation to promote a proactive strategy in achieving resiliency with careful consideration to internal and external requirements; thus, it contributes towards the improvement of a risk maturity-performance rapport.

8.9 Recommendations

Future research should focus on the implementation of the framework. It might be useful to focus on correlating both strategic and operational deployment. One avenue for further research would be to examine the specific determinants, reimbursement and inhibitors for any given industry. Without further research into holistic enterprise-wide risk, it will not be possible to sustain effective security practice. Further work is needed to fully understand the implications of internal and external determinants and the influence on risk governance. Questions that remain unanswered by literature are stranded in a lack of research on assessing the post-alignment implementation of CsM and ERM. The extent of the role that CsM plays in an organisation is yet to be discovered. How ERM is associated or not associated is the underlying cause of security failures. Thus, the possible link between the two creates the basis that orchestrates the security posture of an organisation. The underlying mechanism is strategic alignment-, resiliency- and effectiveness-centric by engaging integration between all three domains. Further research may include organisational methodology, attributing more transparent practices.

Another avenue of research might focus on legislation's effect on risk governance, gathering more information about transparency and better organisational behaviour to risk. If necessary, regulatory effects might be explored within the specifics of each country. Educational awareness level may be incorporated into research to help organisations mature. ERM should become a more integrated part of strategic decisions. The implementation of ERM within organisational culture and embedded within daily activities and processes might be another avenue of research. Perhaps risk governance practices would consider investing more research on how the knowledge and skillset of employees may support effectiveness. With regards to agility and optimisation, another avenue of research may address the research problem quantitatively.

The financial industry is using a mix of generic business standards (e.g. ISO family) and public sector standards (e.g. NIST), so perhaps another avenue of research would be to analyse why regulatory guidance fails to provide a strategic framework for cyber risk

governance. Alternatively, it may focus on improving the risk mapping mechanism, being able to support more integration for risk governance and even collate with the benefits of artificial intelligence. Additionally, it would be interesting to research creating appropriate technical tools to supplement the research framework in tracking, monitoring, collating and managing the risks holistically; a more bottom-up approach would be another advisable avenue of research.

On a practical issue, it depends on where the organisation is when considering implementing a strategy; it may focus on educating senior management and furthering an understanding of the industry and comprehension of business risks, costs, profiles, to name but a few. Some recommendations would be to create open and honest communication and fostering within the right culture (instil and plan risk culture), and to have the right talent and establish a common language for both the board and the organisation. Having the right people, trained and open-minded at the table to tackle these challenges is critical. Lastly, having set the foundation of policies, procedures, guidelines, reporting and accountability structural hierarchy, it would be prudent to reassess and return all related documents regularly and set limits and expectations regarding resiliency and alignment.

Ultimately, the trade-off of applying the recommended *CsM-ERM Alignment Framework* is to create, deploy, and further foster long-term sustainable risk governance for organisations with the financial industry. In summary, the *practical orientation* for risk governance should be maintained and enriched with *scholar research* to ensure that past lessons are acknowledged and to supports an evolution towards an intelligent financial system that responds accurately to current and future requirements.

References

Accenture (2009) 'Managing risk for high performance in extraordinary times: report on the Accenture global risk management study'. Available at: http://www.criticaleye.com/insights-servfile.cfm?id=1359 (Accessed: 10 August 2016).

Accenture (2016) 'The state of cybersecurity and digital trust 2016: identifying cybersecurity gaps to rethink state of the art'. Available at: https://www.accenture.com/t20160704T014005__w__/us-en/_acnmedia/PDF-23/Accenture-State-Cybersecurity-and-Digital-Trust-2016-Report-June.pdf (Accessed: 23 October 2016).

Accenture (2018) 'The cyber resilient enterprise: four questions every CEO must ask to build a cyber resilient business'. Available at: https://www.accenture.com/t20181018T020224Z__w__/ie-en/_acnmedia/PDF-88/Accenture-Cyber-Resilient-Enterprise-US-Digital.pdf (Accessed: 15 November 2018).

Accenture (2018a) 'Gaining ground on the cyber attacker: 2018 state of cyber resiliency'. Available at: https://www.accenture.com/t00010101T000000Z__w__/fr-fr/_acnmedia/PDF-84/Accenture-Security-State-of-Cyber-Resilience-2018.pdf (Accessed: 14 November 2018).

Aebi, V., Sabato, G. and Schmid, M. (2012) 'Risk management, corporate governance, and bank performance in the financial crisis', *Journal of Banking and Finance*, 36(12), pp. 3213–3226. doi: 10.1016/j.jbankfin.2011.10.020.

Agarwal, R. and Ansell, J. (2016) 'Strategic change in enterprise risk management', *Strategic Change*, 25(4), pp. 427–439. doi: 10.1002/jsc.2072.

Aguilera, R., Judge, W. and Terjesen, S. (2018) 'Corporate Governance Deviance', *Academy of Management Review*, 43(1), pp. 87-109.

AICPA (2018) '2018 The state of risk oversight, an overview of enterprise risk management practices'. Available at: https://www.aicpa.org/content/dam/aicpa/interestareas/businessindustryandgovernment/resources/erm/downloadabledocuments/aicpa-erm-research-study-2018.pdf (Accessed: 18 October 2018).

Amin, Z. (2019) 'A practical road map for assessing cyber risk', *Journal of Risk Research*, 22(1), pp.32-43.

Aitchison, C., and Guerin, C. (2014) *Writing groups for doctoral education and beyond: innovation in practice and theory*. Oxon: Routledge.

Alcaraz, C. and Zeadally, S. (2015) 'Critical infrastructure protection: requirements and challenges for the 21st century', *International Journal of Critical Infrastructure Protection*, 8, pp. 53–66. doi: 10.1016/j.ijcip.2014.12.002.

Alecsić, A. and Jelavić, S.R. (2017) 'Testing for strategy-structure fit and its importance for performance', *Management: Journal of Contemporary Management Issues,* 22(1), pp. 85-102.

Allan, N., Cantle, N., Godfrey, P. and Yin, Y. (2012) 'A review of the use of complex systems applied to risk appetite and emerging risks in ERM practice', *British Actuarial Journal*, 18(01), pp. 163-234.

Althonayan, A. (2003) *Integrating technology strategy with business strategy in the airline industry*, Buckinghamshire Business School.

Althonayan, A. (2008) 'The integration approach: integrating technology strategy with business strategy in the airline industry', in: *European and Mediterranean Conference on Information Systems*, 25-26 May. Available at: http://bura.brunel.ac.uk/bitstream/2438/4040/1/plugin-Abrahim%20Althonayn,%20The%20Integration%20Approach%20%20(paper,%20Apr%2008.pdf (Accessed: 16 January 2015).

Althonayan, A. and Andronache, A. (2018) 'Shifting from Information Security towards Cybersecurity Paradigm', in: *International Conference on Information Management and Engineering (ICIME 2018)*, Manchester, 22-24 September 2018.

Althonayan, A., Keith, J. and Misiura, A. (2011) 'Aligning enterprise risk management with business strategy and information systems', *European, Mediterranean & Middle Eastern Conference on Information Systems 2011 (EMCIS2011*), 30-31 May 2011, Athens, Greece, pp. 109-129.

Althonayan, A., Killackey, H. and Keith, J. (2012) 'ERM Culture Alignment to Enhance Competitive Advantage', *2012 ERM Symposium*.

Althonayan, A., Matin, S. M. and Andronache, A. (2018) '*Exploring the Ineffectiveness of ERM's and GRC's Role in the Maturity of Organisations' Risk Management*', in: Strategic Management Society, *SMS Special Conference, Hyderabad*, 15-18 December 2018.

American Institute of Certified Public Accountants (2017) '2017 the state of risk oversight: an overview of enterprise risk management practices'. Available at: http://www.aicpa.org/InterestAreas/BusinessIndustryAndGovernment/Resources/ERM/DownloadableDocuments/AICPA_ERM_Research_Study_2017.pdf (Accessed: 3 October 2017).

Amilevičius, A. (2012) Visuomenės saugumas ir viešoji tvarka [elektroninis išteklius], pp. 5–22.

Andrén, N. and Lundqvist, S. (2017) 'Incentive Based Dimensions of Enterprise Risk Management', *SSRN Electronic Journal*, pp. 1-48.

Antonucci, D. (2017) *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Hoboken: John Wiley and Sons.

Aon (2015) 'Global risk management survey'. Available at: http://www.aon.com/2015GlobalRisk/attachments/2015-Global-Risk-Management-Report-230415.pdf (Accessed: 28 September 2015).

Arena, M., Arnaboldi, M. and Azzone, G. (2010) 'The organizational dynamics of enterprise risk management', *Accounting, Organizations and Society*, 35(7), pp. 659–675. doi: 10.1016/j.aos.2010.07.003.

Armenia, S., Ferreira Franco, E., Nonino, F., Spagnoli, E. and Medaglia, C. (2018) 'Towards the Definition of a Dynamic and Systemic Assessment for Cybersecurity Risks', *Systems Research and Behavioral Science*, pp. 1-20. doi: 10.1002/sres.2556.

Arnold, V., Benford, T., Canada, J. and Sutton, S. G. (2011) 'The role of strategic enterprise risk management and organizational flexibility in easing new regulatory compliance', *International Journal of Accounting Information Systems*, 12(3), pp. 171–188. doi: 10.1016/j.accinf.2011.02.002.

Atoum, I., Otoom, A. and Abu Ali, A. (2014) 'A holistic cyber security implementation framework', *Information Management and Computer Security*, 22(3), pp. 251–264. doi: 10.1108/imcs-02-2013-0014.

Atoum, I., Otoom, A. and Abu Ali, A. (2017) 'Holistic cyber security implementation framework: a case study of Jordan International Journal of Information', *Business and Management*, 9 (1), pp. 108-119. Available at: https://www.researchgate.net/publication/313023066_Holistic_Cyber_Security_Implementation_Frameworks_A_Case_Study_of_Jordan (Accessed: 7 July 2017).

Australian/New Zeeland Standards (2004) *AS/NZS 4360:2004*. Available at: http://www.techstreet.com/standards/as-nzs-4360-2004?product_id=1181581 (Accessed: 13 May 2016).

Aven, E. and Aven, T. (2015) 'On the need for rethinking current practice that highlights goal achievement risk in an enterprise context', *Risk Analysis*, 35(9), pp. 1706–1716. doi: 10.1111/risa.12375.

Avison, D., Jones, J., Powell, P. and Wilson, D. (2004) 'Using and validating the strategic alignment model', *The Journal of Strategic Information Systems*, 13(3), pp. 223–246. doi: 10.1016/j.jsis.2004.08.002.

Baets, W. R. J. (1992) 'Aligning information systems with business strategy', *The Journal of Strategic Information Systems*, 1(4), pp. 205–213. doi: 10.1016/0963-8687(92)90036-v.

Baets, W. R. J. (1996) 'Some empirical evidence on IS strategy alignment in banking', *Information and Management*, 30(4), pp. 155–177. doi: 10.1016/0378-7206(95)00056-9.

Bainbridge, W. S. (2007) 'The scientific research potential of virtual worlds', *Science*, 317(5837), pp. 472–476. doi: 10.1126/science.1146930.

Baker, J. (2011) 'The technology–organization–environment framework', *Information systems theory*. 28 (1), pp. 231-245.

Bank of England (2013) *Technology and cyber resilience benchmarking report 2012*. Available at: http://www.bankofengland.co.uk/financialstability/fsc/Documents/technologyandcyberresiliencebenchmarkingreport2012.pdf (Accessed: 8 February 2015).

Bank of England (2018) 'Discussion Paper: building the UK financial sector's operational.' Available at: resiliencehttps://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf?la=en&hash=4238F3B14D839EBE6BEFBD6B5E5634FB95197D8A (Accessed: 2 November 2018).

Barbour, R. (2014) *Introducing qualitative research, a students' guide*. London: SAGE Publications.

Barley, S.R. and Tolbert, P.S. (1997) 'Institutionalization and Structuration: Studying the links between action and institution', *Organization Studies*, 18(1), pp. 93–117. doi: 10.1177/017084069701800106.

Basel Committee on Banking Supervision (2014) 'Implementation of Basel standard: a report to G20 leaders on'. Available online: http://www.bis.org/bcbs/publ/d299.pdf (Accessed: 20 September 2015).

Basel Committee on Banking Supervision (2015) 'Implementation of Basel standards: a report to G20 leaders on implementation of the Basel III regulatory reform'. Available online: http://www.bis.org/bcbs/publ/d328.pdf (Accessed: 29August 2015).

Basel Committee on Banking Supervision (2018) 'Cyber-resilience: range of practices'. Available at: https://www.bis.org/bcbs/publ/d454.pdf (Accessed: 9 December 2018).

Bashir, M., Afzal, M. T. and Azeem, M. (2008) 'Reliability and validity of qualitative and operational research paradigm', *Pakistan Journal of Statistics and Operation Research*, 4(1), p. 35. doi: 10.18187/pjsor.v4i1.59.

Baskerville, R., Spagnoletti, P. and Kim, J. (2014) 'Incident-centered information security: Managing a strategic balance between prevention and response', *Information & Management*, 51(1), pp. 138-151.

Baxter, R., Bedard, J. C., Hoitash, R. and Yezegel, A. (2013) 'Enterprise risk management program quality: determinants, value relevance, and the financial crisis', *Contemporary Accounting Research*, 30(4), pp. 1264–1295. doi: 10.1111/j.1911-3846.2012.01194.x.

Bayuk, J. L., Healey, J., Schmidt, J., Weiss, J., Sachs, M. H., and Rohmeyer, P. (2012) *Cyber security policy guidebook*. United States: Wiley.

Bazeley, P. (2013) *Qualitative Data Analysis: Practical Strategies*. London: SAGE Publications Ltd.

Beasley, M. S., Clune, R. and Hermanson, D. R. (2005) 'Enterprise risk management: an empirical analysis of factors associated with the extent of implementation', *Journal*

of Accounting and Public Policy, 24(6), pp. 521–531. doi: 10.1016/j.jaccpubpol.2005.10.001.

Beasley, M., Branson, B. and Pagach, B. D. (2015) 'An analysis of the maturity and strategic impact of investments in ERM', *Journal of Accounting and Public Policy*, 34(3), pp. 219–243. doi: 10.1016/j.jaccpubpol.2015.01.001.

Beasley, M.S., Pagach, D.P. and Warr, R.S. (2008) 'Information conveyed in hiring announcements of senior executives overseeing enterprise-wide risk management processes', *Journal of Accounting, Auditing and Finance*,23(3), pp.311-332.doi:10.1177/0148558X0802300303.

Beckford, J. (2009) *Quality: A critical introduction*, 3rd edition. United Kingdom: Taylor and Francis.

Bergeron, F., Raymond, L. and Rivard, S. (2004) 'Ideal patterns of strategic alignment and business performance', *Information and Management*, 41(8), pp. 1003–1020. doi: 10.1016/j.im.2003.10.004.

Berry-Stölzle, T. and Xu, J. (2016) 'Enterprise Risk Management and the Cost of Capital', *Journal of Risk and Insurance*, 85(1), pp. 159-201.

Betts, S.C. (2011) 'Contingency theory: Science or technology?', *Journal of Business and Economics Research (JBER)*, 1(8). doi: 10.19030/jber.v1i8.3044.

Bhattacherjee, A. (2012) *Social science research: Principles, methods, and practices*. 2nd edn. Tampa, FL: A. Bhattacherjee.

Blacker, K. and McConnell, P. (2015) *People risk management: A Practical Approach to Managing the Human Factors That Could Harm Your Business*. London: Kogan Page Publishers.

Blaikie, N. (2010) *Designing social research: The logic of anticipation*. 2nd edn. Cambridge, UK: Polity Press.

Blau, P.M. (1970) 'A formal theory of differentiation in organizations', *American Sociological Review*, 35(2), p. 201. doi: 10.2307/2093199.

Bloem, J., van Doorn, M. and Mittal, P. (2005) *Making IT governance work in a Sarbanes-Oxley world*. Hoboken, NJ: Wiley, John and Sons.

Bloomberg, L. D. and Volpe, M. (2015) *Completing your qualitative dissertation: A road map from beginning to end*. 3rd edn.

Blumberg, B.F., Cooper, D. R. and Schindler, P.S. (2014) *Business research methods*, 4th edn. Maidenhead: McGraw Hill Higher Education.

Blyth, M. (2008) *Risk and security management*. Hoboken: John Wiley and Sons, Inc.

Bogodistov, Y., and Wohlgemuth, V. (2017) 'Enterprise risk management: a capability-based perspective', *The Journal of Risk Finance*, Vol. 18 (3), pp. 234-251.

Bohnert, A., Gatzert, N., Hoyt, R. and Lechner, P. (2019) 'The drivers and value of enterprise risk management: evidence from ERM ratings', *The European Journal of Finance*, pp. 234–255.doi: 10.1080/1351847X.2018.1514314.

Bohnert, A., Gatzert, N., Hoyt, R. E. and Lechner, P. (2017) 'The drivers and value of Enterprise Risk Management: evidence from ERM ratings', (*forthcoming*) Available at : https://www.vwrm.rw.fau.de/files/2017/06/ERM-Europe-2017-06-21-WP.pdf (Accessed: 19 August 2017).

Bojanc, R. and Jerman-Blažič, B. (2008) 'An economic modelling approach to information security risk management', *International Journal of Information Management*, 28(5), pp. 413–422. doi: 10.1016/j.ijinfomgt.2008.02.002.

Boland, A., Cherry, G. and Dickson, R.(ed.) (2013) *Doing a systematic review: a student's guide*. London: Sage Publications Ltd.

Booth, A.D., Papaioannou, D. and Sutton, A. (2011) *Systematic approaches to a successful literature review*. Thousand Oaks, CA: Sage Publications.

Borek, A, Parlikad, A., Webb, J. and Woodall, P. (2013) *Total information risk management: maximizing the value of data and information assets*. Waltham: Elsevier Science.

Borison, A. and Hamm, G. (2010) 'How to manage risk (after risk management has failed)', *MIT Sloan Management Review*, 52 (1), pp. 50-57.

Boyatzis, R. (1998) *Transforming Qualitative Information: Thematic Analysis and Code Development*. Thousand Oaks, CA: Sage Publications.

Braumann, E. (2018) 'Analysing the Role of Risk Awareness in Enterprise Risk Management', *Journal of Management Accounting Research*, 30(2), pp. 241-268.

British Standard Institution (2009a) *BS ISO 31000:2009*. London: British Standards Institution.

British Standard Institution (2009b) *BS ISO Guide 73:2009 Risk management. Vocabulary*. London: British Standards Institution.

British Standard Institution (2011a) *BS ISO/IEC 27005:2011 Information technology. Security techniques. Information security risk management*. London: British Standards Institution.

British Standard Institution (2011b) *BS ISO 31010:2011 Risk management. Code of practice for the implementation of BS ISO 31000*. London: British Standards Institution.

British Standard Institution (2011c*) BS 31100: 2011 Risk management. Code of practice and guidance for the implementation of BS ISO 31000*. London: British Standards Institution.

British Standard Institution (2012) *BS ISO/IEC 27032:2012 Information technology. Security techniques*. Guidelines for cybersecurity. London: British Standards Institution.

British Standard Institution (2013a) *PAS 555:2013 Cyber security risk-governance and management specification*. London: British Standards Institution.

British Standard Institution (2013b) *BS ISO 27001:2013 Information technology. Security techniques. Information management systems. Requirement*. London: British Standards Institution.

British Standard Institution (2013c) *ISO/IEC 27002:2013 Information technology. Security techniques. Code of practice for information security controls*. London: British Standards Institution.

British Standard Institution (2016a) *BS ISO/IEC 27000:2016 Information technology. Security techniques. Information security management systems. Overview and vocabulary*. London: British Standards Institution.

British Standard Institution (2016b) *BS ISO/IEC 27004:2016. Information technology— Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*. London: British Standards Institution.

British Standard Institution (2017b) *Information technology— Security techniques— Information security management systems —Overview and vocabulary BS EN ISO/IEC 27000:2017 (ISO/IEC 27000:2016)*. London: British Standards Institution.

British Standard Institution (2017c) *BS EN ISO/IEC 27002:2017. Information technology — Security techniques — Code of practice for information security controls (ISO/IEC 27002:2013)*. London: British Standards Institution.

British Standard Institution (2017d) *BS ISO/IEC 27003:2017. Information technology — Security techniques — Information security management systems — Guidance*. London: British Standards Institution.

British Standard Institution (2018b) *Guidelines for auditing management systems (ISO 19011:2018)*. London: British Standards Institution.

British Standard Institution (2018c) *ISO/IEC 27005 Information technology ─ security techniques ─ information security risk management*. London: British Standards Institution.

British Standards Institution (2017a) *BS EN ISO/IEC 27001:2017 Information technology─security techniques─information security management systems─requirements (ISO/IEC 29001: 2013)*. London: British Standards Institution.

British Standards Institution (2018a) *BSI Standard publication BS ISO 31000:2018 Risk management ─guidelines*. London: British Standards Institution.

Broadbent, M. and Weill, P. (1993) 'Improving business and information strategy alignment: Learning from the banking industry', *IBM Systems Journal*, 32(1), pp. 162–179. doi: 10.1147/sj.321.0162.

Bromiley, P., McShane, M., Nair, A. and Rustambekov, E. (2015) 'Enterprise risk management: Review, critique, and research directions', *Long Range Planning*, 48(4), pp. 265–276. doi: 10.1016/j.lrp.2014.07.005.

Brotby, W. (2009) *Information security management metrics*. Boca Raton: CRC Press.

Bryman, A. and Bell, E. (2015) *Business research methods*. 4th edn. Oxford: Oxford University Press.

Bryman, A. (2012) *Social research methods*. 4th edn. Oxford: Oxford University Press.

Bryman, A. (2016) *Social research methods*. 5th edn. Oxford, United Kingdom: Oxford University Press.

Bryman, A. and Bell, E. (2011) *Business research methods*. 3rd edn. UK: Oxford University Press.

Bryman, A. and Cramer, D. (2011) *Quantitative data analysis with IBM SPSS 17, 18 and 19*. London: Routledge.

Burgess, P. J. (ed.) (2010) *The Routledge handbook of new security studies*. United Kingdom: Routledge.

Burn, J. M. and Szeto, C. (2000) 'A comparison of the views of business and IT management on success factors for strategic alignment', *Information and Management*, 37(4), pp. 197–216. doi: 10.1016/s0378-7206(99)00048-8.

Burnaby, P. and Hass, S. (2009) 'Ten steps to enterprise-wide risk management', *Corporate Governance: The international journal of business in society*, 9 (5), pp. 539–550. doi: 10.1108/14720700910998111.

Calandro, J. (2015) 'A leader's guide to strategic risk management', *Strategy and Leadership*, 43(1), pp. 26–35. doi: 10.1108/sl-11-2014-0082.

Calder, A. and Watkins, S. (2010) *Information security, risk management for ISO27001/ISO27002*, 2nd edn. Cambridgeshire: IT Governance Publishing.

Calder, A. and Watkins, S. (2012) *IT Governance: an international guide to data security and ISO27001/ ISO27002*. London: Kogan Page Limited.

Campbell, B., Kay, R. and Avison, D. (2005) 'Strategic alignment: a practitioner's perspective', *Journal of Enterprise Information Management*, 18(6), pp. 653–664. doi: 10.1108/17410390510628364.

Caralli, R. A., Stevens, J. F., Young, L. R., and Wilson, W. R. (2007) *Introducing octave allegro: improving the information security risk assessment process* (No. CMU/SEI-2007-TR-012). Carnegie-Mellon University Pittsburgh PA Software Engineering INST.

Carretta, A., Farina, V. and Schwizer, P. (2017) 'Risk culture and banking supervision', *Journal of Financial Regulation and Compliance*, vol. 25, no. 2, pp. 209-226.

Casson, M. and Rose, M. B. (2014) *Institutions and the evolution of modern business*. London, United Kingdom: Taylor and Francis.

Castro, L. M., Gulías, V. M., Abalde, C. and Santiago Jorge, J. (2008) 'Managing the risks of risk management', *Journal of Decision Systems*, 17(4), pp. 501–521. doi: 10.3166/jds.17.501-521.

Casualty Actuarial Society (2003) 'Overview of enterprise risk management'. Available at: https://www.casact.org/area/erm/overview.pdf (Accessed: 13 May 2016).

Centre for Strategic and International Studies, CSIS (2015) *The evolution of cybersecurity requirements for the U.S. financial industry*. Available from: https://www.csis.org/analysis/evolution-cybersecurity-requirements-us-financial-industry (Accessed: 18 January 2016).

CERT-UK (2015) 'Annual report, Apr 2014- Mar 2015, including quarter 4'. Available at: https://www.cert.gov.uk/wp-content/uploads/2015/05/Annual-Report-including-4th-Quarter-FINAL.pdf (Accessed: 10 June 2015).

CESG (2012) 'Executive companion: 10 steps to cyber security'. Available at: https://www.cyberessentials.org/system/resources/W1siZiIsIjIwMTQvMDYvMDQvMTdfNDdfMTdfNjMwXzEwX3N0ZXBzX3RvX2N5YmVyX3NlY3VyaXR5LnBkZiJdXQ/10-steps-to-cyber-security.pdf (Accessed: 3 June 2016).

CESG (2015a) 'Common cyber-attacks: reducing the impact'. Available at: Https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf (Accessed: 29 May 2015).

CESG (2015b) 'The information assurance maturity model and assessment framework'. Available at https://www.cesg.gov.uk/guidance/information-assurance-maturity-model-and-assessment-framework-gpg-40 (Accessed: 6 July 2016).

Chan, Y. (2002) 'Why haven't we mastered alignment? The importance of the informal organizational structure', *MIS Quarterly Executive*, 1(2), pp. 97-112.

Chan, Y. E. and Reich, B. H. (2007) 'IT alignment: What have we learned?', *Journal of Information Technology*, 22(4), pp. 297–315. doi: 10.1057/palgrave.jit.2000109.

Chan, Y. E., Sabherwal, R. and Thatcher, J. B. (2006) 'Antecedents and outcomes of strategic IS alignment: An empirical investigation', *IEEE Transactions on Engineering Management*, 53(1), pp. 27–47. doi: 10.1109/tem.2005.861804.

Chang, C., Jiménez-Martín, J., McAleer, M. and Pérez-Amaral, T. (2011) 'Risk management of risk under the Basel accord: forecasting value-at-risk of VIX futures', *Managerial Finance*, 37(11), pp. 1088–1106. doi: 10.1108/03074351111167956.

Chang, S. E. and Ho, C. B. (2006) 'Organizational factors to the effectiveness of implementing information security management', *Industrial Management and Data Systems*, 106(3), pp. 345-361.

Chapman, R. (2011) *Simple tools and techniques for enterprise risk management. Chichester*, England: Wiley.

Charoensuk, S., Wongsurawat, W. and Khang, D. B. (2014) 'Business-IT alignment: a practical research approach', *The Journal of High Technology Management Research*, 25(2), pp. 132–147. doi: 10.1016/j.hitech.2014.07.002.

Chartered Global Management Accountant (CGMA) (2015) 'Global state of enterprise risk oversight'. Available at: http://www.cgma.org/Resources/Reports/DownloadableDocuments/2015-06-13-The-global-state-of-enterprise-risk-oversight-report.pdf (Accessed: 22 June 2015).

Chartered Institute of Internal Auditors (2018) 'Organisational culture'. Available at: https://www.iia.org.uk/culture?downloadPdf=true . (Accessed: 28 November 2018).

Chen, L. (2010) 'Business–IT alignment maturity of companies in China', *Information and Management*, 47(1), pp. 9–16. doi: 10.1016/j.im.2009.09.003.

Chenhall, R. H. (2003) 'Management control systems design within its organizational context: Findings from contingency-based research and directions for the future', *Accounting, Organizations and Society*, 28(2-3), pp. 127–168. doi: 10.1016/s0361-3682(01)00027-7.

Child, J. (1972) 'Organizational structure, environment and performance: The role of strategic choice', *Sociology*, 6(1), pp. 1–22. doi: 10.1177/003803857200600101.

Ching, H. Y. and Colombo, T. M. (2014) 'Enterprise risk management good practices and proposal of conceptual framework', *Journal of Management Research*, 6(3), p. 69. doi: 10.5296/jmr.v6i3.5404.

Chorn, N. H. (1991) 'The "Alignment" theory: Creating strategic fit', *Management Decision*, 29(1). doi: 10.1108/eum0000000000066.

Ciborra, C. U. (1997) 'De profundis? Deconstructing the concept of strategic alignment', *Scandinavian Journal of Information Systems*, 9(1), pp. 67-82.

Cicognani, A. (1998) 'On the linguistic nature of cyberspace and virtual communities', *Virtual Reality*, 3(1), pp. 16–24. doi: 10.1007/bf01409794.

Ciesielska, M. and Jemielniak, D. (2017) *Qualitative Methodologies in Organization Studies*. Springer.

CISCO (2014) 'Cisco 2014, annual security report'. Available at: http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf (Accessed: 21 September).

Clarke, J.C. and Varma, S. (1999) 'Strategic risk management: the new competitive edge', *Long Range Planning*, 32(4), pp. 414-424. doi: 10.1016/S0024-6301(99)00052-7.

Clarke, V. and Braun, V. (2013) Teaching thematic analysis: Overcoming challenges and developing strategies for effective learning. The psychologist, 26(2), pp. 120-123.

Clegg, S.R. and Hardy, C. (eds.) (1999) *Studying organization: Theory and method: V. 1*. Thousand Oaks, CA: Sage Publications.

Cohen, J., Krishnamoorthy, G. and Wright, A. (2017) 'Enterprise Risk Management and the Financial Reporting Process: The Experiences of Audit Committee Members, CFOs, and External Auditors', *Contemporary Accounting Research*, 34(2), pp.1178-1209.

Cole, G. A. (2004) *Management theory and practice*. 6th edn. London: Thomson Learning.

Collis, J. and Hussey, R. (2009) *Business research: A practical guide for undergraduate and postgraduate students*. 2nd edn. Houndmills, Basingstoke, Hampshire: Palgrave Macmillan.

Coltman, T., Tallon, P., Sharma, R. and Queiroz, M. (2015) 'Strategic IT alignment: Twenty-five years on', *Journal of Information Technology*, 30(2), pp. 91–100. doi: 10.1057/jit.2014.35.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (1992) 'Internal control-integrated framework-executive summary'. Available at: http://www.sarinasystem.com/fa/downloads/matlab/4/COSO%20Framework%201992.pdf (Accessed: 19 May 2016).

Committee on National Security Systems (2010) 'National information assurance (IA) glossary'. Available at: https://www.hsdl.org/?view&did=7447 (Accessed: 10 October 2016).

Communications Electronics Security Group (CESG), Cabinet Office, CPNI and Department for Business, Innovation and Skills (2012) *10 Steps to cyber security*. Available at: https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility (Accessed: 10 May 2016).

Conference of State Bank Supervisors (CSBS), (2014) *Cybersecurity 101: a resource guide for bank executives, executive leadership of cybersecurity*. Available at: http://www.csbs.org/CyberSecurity/Documents/CSBS%20Cybersecurity%20101%20Resource%20Guide%20FINAL.pdf (Accessed: 18 March 2015).

Corsaro, D. and Snehota, I. (2011) 'Alignment and misalignment in business relationships', *Industrial Marketing Management*, 40(6), pp. 1042–1054. doi: 10.1016/j.indmarman.2011.06.038.

COSO (2004) 'Enterprise risk management –integrated framework, executive summary'. Available at: http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf (Accessed: 10 March 2015).

COSO (2010) 'Developing key risk indicators to strengthen Enterprise Risk Management'. Available at: https://www.coso.org/Documents/COSO-KRI-Paper-Full-FINAL-for-Web-Posting-Dec110-000.pdf (Accessed: January 2018).

COSO (2012) 'Enterprise risk management: understanding and communicating risk appetite'. Available at: http://www.coso.org/documents/ERM-

Understanding%20%20Communicating%20Risk%20Appetite-WEB_FINAL_r9.pdf (Accessed: 21 September 2016).

COSO (2013) 'Internal control-integrated framework, executive summary'. Available at: http://www.coso.org/documents/990025P_Executive_Summary_final_may20_e.df (Accessed: 19 May 2016).

COSO (2015) 'Leveraging C O S O across the three line of defence'. Available at: https://www.coso.org/Documents/COSO-2015-3LOD.pdf (Accessed: October 2018).

COSO (2015a) 'COSO in the cyber age'. Available at: http://www.coso.org/documents/COSO%20in%20the%20Cyber%20Age_FULL_r11.pdf (Accessed: 3 March 2015).

COSO (2016) 'Enterprise risk management: aligning risk with strategy and performance'. (exposure draft). Available at: https://www.coso.org/Documents/COSO-ERM-draft-Post-Exposure-Version.pdf (Accessed: 11 November 2016)

COSO (2017) 'Enterprise risk management: integrating with strategy and performance, Executive Summary'. Available at: https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf (Accessed: 18 oct 2018).

Cottrell, R.R. and McKenzie, J. F. (2010) *Health promotion and education research methods: Using the five-chapter thesis/dissertation model*. 2nd edn. Sudbury, MA: Jones and Bartlett Publishers.

Coyle, B. (2014) *Corporate governance*. 4th edn. London: ICSA Information and Training Ltd.

Cragg, P., King, M. and Hussin, H. (2002) 'IT alignment and firm performance in small manufacturing firms', *The Journal of Strategic Information Systems*, 11(2), pp. 109–132. doi: 10.1016/s0963-8687(02)00007-0.

Craigen, D., Diakun-Thibault, N. and Purse, R. (2014) 'Defining cybersecurity', *Technology Innovation Management Review*, 4(10), pp. 13-21.

Creswell, J. (2015*) Research design: qualitative, quantitative, and mixed methods approach*. 4th edn. London: Sage Publication, Inc.

Creswell, J. W. (2014) *Research design: qualitative, quantitative, and mixed methods approaches*. 4th edn. Thousand Oaks: SAGE Publications.

Crockford, G. N. (1982) 'The bibliography and history of risk management: some preliminary observations', *The Geneva Papers and Risk and Insurance*, 7(23), pp. 169-179.

Crouhy, M., Galai, D. and Mark, R. (2014) *The essential of risk management*. 2nd edn. London: McGraw-Hill Education.

Crowston, K., Rubleske J. and Howison, J., 2006. A ten-year retrospective. *Human-Computer Interaction and Management Information Systems: Foundations*, pp. 120-135. Sharpe, M. E.: United States.

Da Veiga, A. and Eloff, J. (2010) 'A framework and assessment instrument for information security culture', *Computers and Security*, 29(2), pp. 196-207. doi: 10.1016/j.cose.2009.09.002.

Da Veiga, A. D. and Eloff, J. H. P. (2007) 'An information security governance framework', *Information Systems Management*, 24(4), pp. 361–372. doi: 10.1080/10580530701586136.

Dabari, I.J., Kwaji, S.F. and Ghazali, M.Z. (2017) 'Aligning Corporate Governance with Enterprise Risk Management Adoption in the Nigerian Deposit Money Banks', *Indian-Pacific Journal of Accounting and Finance*, 1(2), pp.4-14.

Daft, R. L. (2012) *Organization theory and design*. South-Western: Cengage Learning.

Daft, R. L., Murphy, J. and Willmott, H. (2014) *Organization theory and design: An international perspective*. 2nd edn. London, United Kingdom: Cengage Learning EMEA.

Dang, C., (Frank) Li, Z. and Yang, C. (2018) 'Measuring firm size in empirical corporate finance', *Journal of Banking & Finance*, 86, pp. 159-176.

de Bruijn, H. and Janssen, M. (2017) 'Building Cybersecurity Awareness: The need for evidence-based framing strategies', *Government Information Quarterly*, 34(1), pp. 1-7. doi: /10.1016/j.giq.2017.02.007.

De Haes, S. and Van Grembergen, W. (2009) 'An exploratory study into IT governance Implementations and its impact on business/IT alignment', *Information Systems Management*, 26 (2), pp. 123–137. doi: 10.1080/10580530902794786.

DeFranco, J. F. (2013) *What every engineer should know about cyber security and digital forensics*. Boca Raton: CRC Press.

Deibert, R.J. and Rohozinski, R. (2010) 'Risking security: policies and paradoxes of Cyberspace security', *International Political Sociology*, 4(1), pp. 15–32. doi: 10.1111/j.1749-5687.2009.00088.x.

Deloitte (2009) 'Global risk management survey, six edition: risk management in the spotlight'. Available at: http://www.ucop.edu/enterprise-risk-management/_files/deloitte_globalrskmgtsrvy.pdf (Accessed: 7 September 2016).

Deloitte (2012) 'Cyber security everybody's imperative: a guide for C-suite and boards on guarding against cyber risks'. Available at: https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-cyber-security-everybodys-imperative.PDF (Accessed: 21 September 2016).

Deloitte (2014a) 'Transforming cybersecurity, new approaches for an evolving landscape'. Available at: http://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-

services/us-fsi-Transformingcybersecurity-021114.pdf (Accessed: 10 January 2016).

Deloitte (2014b) 'Risk transformation: aligning risk and the pursuit of shareholder value'. Available at: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/gx_grc_risk_transformation_pdf.pdf (Accessed: 26 September 2016).

Deloitte (2015a) 'Top regulatory trends for 2015 in banking'. Available at: http://www2.deloitte.com/content/dam/Deloitte/us/Documents/regulatory/us-regu-2015regulatorytrendsinbanking-final-01082015.pdf (Accessed: 22 March 2015).

Deloitte (2015b) 'Global risk management survey, ninth edition: operating in the new normal: increased regulation and heightened expectation'. Available at: https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/performancemagazine/articles/lu-global-risk-management-survey-ninth-edition-06102015.pdf (Accessed: 25 September 2015).

Deloitte (2015c) 'Enterprise risk management, a risk intelligent approach'. Available at: http://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-enterprise-risk-management-a-risk-intelligent-approach.pdf (Accessed: 25 September 2015).

Deloitte (2015d) 'COSO in the cyber age'. Available at: http://www.coso.org/documents/COSO%20in%20the%20Cyber%20Age_FULL_r11.pdf (Accessed: 3 March 2015).

Deloitte (2015e) 'Cybersecurity: the changing role of audit committee and internal audit'. Available at: http://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-security-changing-role-in-audit-noexp.pdf (Accessed: 22 September 2016).

Deloitte (2015f) 'Five essential steps to improve cybersecurity: trekking towards a more secure, vigilant, and resilient organisation'. Available at: http://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-risk-cyber-5-steps.pdf (Accessed: 23 October 2016).

Deloitte (2016) 'Raising the bar on managing enterprise risks, OMB's requirements for Enterprise Risk Management in Federal Agencies'. Available at: https://www2.deloitte.com/us/en/pages/public-sector/articles/managing-enterprise-risks.html (Accessed: 10 September 2017).

Deloitte (2017) 'Three Lines of Defense Time to rethink and reframe the model'. Available at:https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu-three-lines-defense-13072017.pdf (Accessed: 25 October 2018).

Deloitte (2018) 'The state of cybersecurity at financial institutions: there's no "one size fits all" approach'.Available at: https://www2.deloitte.com/content/dam/insights/us/articles/3926_FS-ISAC/DI_FS-ISAC.pdf (Accessed: 3 November 2018).

Deloitte (n.d.) 'Cyber incident response prepare for the inevitable. Respond to evolving threats. Recover rapidly. Available at : https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-deloitte-crisis-incident-response.pdf (Acceesd: September 2018).

Deng, X., Chen, T. and Pan, D. (2007), in IFIFP International Federation for Information Processing, *Research and practical issues of enterprise information systems II* ,254 (1), pp. 311-316.

Deng, X., Chen, T. and Pan, D. (2008) 'Organizational coordination theory and its application in virtual enterprise', in *Research and Practical Issues of Enterprise Information Systems II Volume 1*. Springer Science + Business Media, pp. 311–316. doi: 10.1007/978-0-387-75902-9_32.

Denscombe, M. (2017) *The good research guide for small-scale social research projects*, 6th edn. London: Open University Press.

Dickinson, G. (2001) 'Enterprise risk management: Its origins and conceptual foundation', *Geneva Papers on Risk and Insurance - Issues and Practice*, 26(3), pp. 360–366. doi: 10.1111/1468-0440.00121.

DiMaggio, P. J. and Powell, W.W. (1983) 'The iron cage revisited: Institutional Isomorphism and collective rationality in organizational fields', *American Sociological Review*, 48(2), p. 147. doi: 10.2307/2095101.

Dionne, G. (2013) 'Risk management: history, definition, and critique', *Risk Management and Insurance Review*, 16(2), pp. 147–166. doi: 10.1111/rmir.12016.

Dixon-Woods, M., Agarwal, S., Jones, D., Young, B., and Sutton, A. (2005) 'Synthesising qualitative and quantitative evidence: a review of possible methods', *Journal of Health Services Research*, 10(1), pp. 45-53.

Dobson, I., Fox, C. and Hietala, J. (2011) *Open Information Security Management Maturity Model (O-ISM3).* Reading, UK: Van Haren Pub.

Dodd-Frank Act (2010) 'Dodd-Frank Wall Street Reform and Consumer Protection Act'. H.R. 4173 (USA). Available at: http://www.cftc.gov/idc/groups/public/@swaps/documents/file/hr4173_enrolledbill.pdf (Accessed: 4 September 2016).

Donaldson, L. (2001) *The contingency theory of organizations (foundations for organizational science).* Thousand Oaks, CA: Sage Publications.

Donaldson, L. (2008) Resolving the conflict between contingency and institutional theories of organizational design. In *Designing Organizations* (pp. 21-40). Springer USA.

Drew, S. A. W. and Kendrick, T. (2005) 'Risk management: the five pillars of corporate governance', *Journal of General Management*, 31 (2), pp. 19-36.

Dzimbiri, L. B. (2009) *Organisation and management theories: An African focus integrating structure, people, processes and the environment for human happiness*. Göttingen: Cuvillier.

Eckles, D. L., Hoyt, R. E. and Miller, S. M. (2014) 'The impact of enterprise risk management on the marginal cost of reducing risk: Evidence from the insurance industry', *Journal of Banking and Finance*, 43, pp. 247–261. doi: 10.1016/j.jbankfin.2014.02.007.

El-Telbany, O. and Elragal, A. (2014) 'Business-information Systems Strategies: A Focus on Misalignment', *Procedia Technology*, 16, pp. 250-262.

Eriksson, P. and Kovalainen, A. (2008) *Qualitative methods in business research*. Los Angeles: Sage Publications.

Ernst and Young (2014a) 'Achieving resiliency in the cyber ecosystem'. Available at: http://www.ey.com/Publication/vwLUAssets/cyber_ecosystem/$FILE/EY-Insights_on_GRC_Cyber_ecosystem.pdf (Accessed: 9 October 2016).

Ernst and Young (2014b) 'Cyber program management: identifying ways to get ahead of cybercrime'. Available at: http://www.ey.com/Publication/vwLUAssets/EY-cyber-program-management/$FILE/EY-cyber-program-management.pdf (Accessed: 31 March 2015).

Ernst and Young (2015) 'Rethinking risk management, banks focus on non-financial risks and accountability'. Available at: https://www.ey.com/Publication/vwLUAssets/EY-rethinking-risk-management/%24File/EY-rethinking-risk-management.pdf (Accessed: 4 October 2010).

Ernst and Young (2015) 'Risk accountability: responsibility must be shared'. Available at: https://www.ey.com/Publication/vwLUAssets/EY-risk-governance-2020-risks-accountability/$FILE/EY-risk-governance-2020-risk-accountability.pdf (Accessed: 19 October 2018).

Ernst and Young (2016) 'Enterprise risk management: an integrated approach towards effective and sustainable risk management'. Available at: http://www.ey.com/Publication/vwLUAssets/EY-enterprise-risk-management/$FILE/EY-enterprise-risk-management.pdf (Accessed: 8 August 2016).

Ernst and Young (2017) 'Next generation enterprise risk management'. Available at: https://www.ey.com/Publication/vwLUAssets/ey-next-generation-enterprise-risk-management/$FILE/ey-next-generation-enterprise-risk-management.pdf (Accessed: 20 November 2018).

Ernst and Young (2018a) 'Cybersecurity for industry 4.0: cybersecurity implications for government, industry and homeland security'. Available at: https://www.ey.com/Publication/vwLUAssets/ey-cybersecurity-for-industry-4-0/$File/ey-cybersecurity-for-industry-4-0.pdf (Accessed: 3 December 2018).

Ernst and Young (2018b) 'Is cybersecurity about more than protection? EY Global Information Security Survey 2018–19'. Available at: https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-

survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf (Accessed: 10 December 2018).

European Network and Information Security Agency (2012) 'ENISA threat landscape: responding to the evolving threats environment'. Available at: http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat landscape/ENISA_Threat_Landscape/at_download/fullReport (Accessed: 20 May 2015).

European Union Agency for Network and Information Security (ENISA) (2017) Cyber Security Culture in organisations. Available at: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations/at_download/fullReport (Accessed: 12 September 2018).

Europol, (2014) 'The Internet organised crime threat assessment (iOCTA)'. Available at: https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web.pdf (Accessed: 28 April 2015).

Evans, D., Gruba, P. and Zobel, J. (2014) *How to Write a Better Thesis*, 3rd edn. London: Springer International Publishing.

Evans, J. R. (2007) *Quality and performance excellence: Management, organization, and strategy*. 5th edn. Cincinnati, OH, United States: Thomson Business and Economics.

Ezingeard, J. N., McFadzean, E. and Birchall, D. (2007) 'Mastering the art of corroboration: a conceptual analysis of information assurance and corporate strategy alignment', Journal *of Enterprise Information Management*, 20(1), pp. 96-118. doi: 10.1108/17410390710717165.

Fakhri, B., Fahimah, N. and Ibrahim, J. (2015) 'Information security aligned to enterprise management', *Middle East Journal of Business*, 10(1), pp. 62-66.

Falkner, E. M. and Hiebl, M. R.W. (2015) 'Risk management in SMEs: A systematic review of available evidence', *The Journal of Risk Finance*, 16(2), pp. 122–144. doi: 10.1108/jrf-06-2014-0079.

Farrell, M. and Gallagher, R. (2014) 'The valuation implications of enterprise risk management maturity', *Journal of Risk and Insurance*, 82(3), pp. 625–657. doi: 10.1111/jori.12035.

Farrell, M. and Gallagher, R. (2019) 'Moderating influences on the ERM maturity-performance relationship', *Research in International Business and Finance* (In Press).

Federation of European Risk Management Association (FERMA) (2003) 'A risk management standard'. Available at: http://www.ferma.eu/app/uploads/2011/11/a-risk-management-standard-english-version.pdf (Accessed: 29 April 2015).

Fenz, S., Heurix, J., Neubauer, T. and Pechstein, F. (2014) 'Current challenges in information security risk management', *Information Management and Computer Security*, 22(5), pp. 410–430. doi: 10.1108/imcs-07-2013-0053.

Financial Conduct Authority (2018) 'Cyber and technology resilience: themes from cross-sector survey 2017 – 2018'. Available at: https://www.fca.org.uk/publication/research/technology-cyber-resilience-questionnaire-cross-sector-report.pdf (Accessed: 12 December, 2018).

Financial Industry Regulatory Authority (2015) *Report on cybersecurity practices.* Available at: https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf (Accessed: 20 January 2016).

Financial Reporting Council (2005) 'Internal control-revised guidance for directors on the combined code (Turnbull Guidance)'. Available at: https://www.frc.org.uk/getattachment/5e4d12e4-a94f-4186-9d6f-19e17aeb5351/Turnbull-guidance-October-2005.aspx (Accessed: 20 May 2016).

Financial Reporting Council (2016) 'The UK corporate governance'. Available at: https://www.frc.org.uk/Our-Work/Publications/Corporate-Governance/UK-Corporate-Governance-Code-April-2016.pdf (Accessed: 4 September 2016).

Financial Stability Board (2017) 'Summary report on financial sector cybersecurity regulation'. Available at: http://www.fsb.org/wp-content/uploads/P131017-1.pdf (Accessed: 20 February 2018).

Firsova, N. and P. Vaghely, I. (2018) 'Strategic Options to Cultural Risk Management: A Theoretical Framework', *Universal Journal of Management*, 6(7), pp.248-262.

Fisher, C. (2004) *Researching and writing a Dissertation: A guidebook for business students*. Harlow, United Kingdom: Financial Times/ Prentice Hall.

Fisher, C. M. (2010) *Researching and writing a dissertation: An essential guide for business students*. 3rd edn. Harlow, England: Financial Times/Prentice Hall.

Fisher, J. G. (1998) 'Contingency theory, management control systems and firm outcomes: past results and future directions', *Behavioural Research in Accounting*, supplement 10, pp. 47-64.

Flick, U. (2008) *Managing quality in qualitative research (qualitative research kit)*. Los Angeles: Sage Publications Ltd, United Kingdom.

Flick, U. (2014) *An introduction to qualitative research*, 5th edn. London: Sage Publication Ltd.

Francis, S. and Paladino, B. (2008) 'Enterprise risk management: a best practice approach', *Journal of Corporate Accounting and Finance*, 19(3), pp. 19–33. doi: 10.1002/jcaf.20382.

Francis, S. and Richards, T. (2007) 'Why ERM matters and how to accelerate progress', *Risk Management*, pp. 28-30.

Fraser, J. and Simkins, B. (2016) 'The challenges of and solutions for implementing enterprise risk management', *Business Horizons*, 59(6), pp. 689-698. doi: 10.1016/j.bushor.2016.06.007.

Fraser, J., Schoening-Thiessen, K. and Simkins, B. (2011)'Who Reads What Most Often?: A Survey of Enterprise Risk Management Literature Read by Risk Executives'. *Enterprise Risk Management*, pp. 385-417.

Fredrickson, J. W. (1984) 'The comprehensiveness of strategic decision processes: Extension, observations, future directions', *Academy of Management Journal*, 27(3), pp. 445–466. doi: 10.2307/256039.

Frigo, M. and Anderson, R. (2011) 'Strategic risk management: A foundation for improving enterprise risk management and governance', *Journal of Corporate Accounting & Finance*, 22(3), pp. 81-88.

Fry, L. W. and Smith, D.A. (1987) 'Congruence, contingency, and theory building', *Academy of Management Review*, 12(1), pp. 117–132. doi: 10.5465/amr.1987.4306496.

Gartner (2016) 'Tech trends 2016: innovating in the digital era'. Available at: https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/technology/DUP_TechTrends2016.pdf (Accessed: 10 October 2016).

Gates, S. (2006) 'Incorporating strategic risk into enterprise risk management: a survey of current corporate practice', *Journal of Applied Corporate Finance*, 18(4), pp. 81-90. doi: 10.1111/j.1745-6622.2006.00114.x.

Gatzert, N. and Martin, M. (2015) 'Determinants and value of enterprise risk management: empirical evidence from literature', *Risk Management and Insurance Review*, 18 (1), pp. 29-53. doi: 10.1111/rmir,12028.

Gavrilova, M. L., Tan, C. J. K. and Sourin, A. (eds.) (2016) *Transactions on Computational Science XXVIII: Special Issue on Cyberworlds and Cybersecurity*. Springer: Berlin.

Gbangou, L. P. D. and Rusu, L. (2016) 'Factors hindering business-IT alignment in the banking sector of a developing country', *Procedia Computer Science*, 100, pp. 280–288. doi: 10.1016/j.procs.2016.09.156.

General Data Protection Regulation (2016) 'Regulation (EU) 2016/679 of the European Parliament and of the Council', *Official Journal of the European Union*, pp. 1-88. Available at: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf (Accessed: 10 May 2017).

Gerber, M. and Von Solms, R. (2005) 'Management of risk in the information age', *Computers and Security*, 24(1), pp. 16–30. doi: 10.1016/j.cose.2004.11.002.

Gerow, J. E., Thatcher, J.B. and Grover, V. (2015) 'Six types of IT-business strategic alignment: An investigation of the constructs and their measurement', *European Journal of Information Systems*, 24(5), pp. 465–491. doi: 10.1057/ejis.2014.6.

Gheorghe, M., (2011) 'Risk management in IT governance framework', *Economia. Seria Management*, 14(2), pp. 545-552.

Ghofar, A. and Islam, S. M. N. (2015) *Corporate governance and contingency theory: A structural equation modelling approach and accounting risk implications*. Switzerland: Springer International Publishing AG.

Gibbs, J. L. and Kraemer, K. L. (2004) 'A cross-country investigation of the determinants of scope of e-commerce use: An institutional approach', *Electronic Markets*, 14(2), pp. 124–137. doi: 10.1080/10196780410001675077.

Gilbert, G. and Stoneman, P. (eds.) (2016) *Researching social life*. 4th edn. London: Sage Publication Inc.

Ginsberg, A. and Venkatraman, N. (1985) 'Contingency perspectives if organizational strategy: A critical review of the empirical research', *Academy of Management Review*, 10(3), pp. 421–434. doi: 10.5465/amr.1985.4278950.

Gordon, L. A., Loeb, M. P. and Tseng, C.-Y. (2009) 'Enterprise risk management and firm performance: A contingency perspective', *Journal of Accounting and Public Policy*, 28(4), pp. 301–327. doi: 10.1016/j.jaccpubpol.2009.06.006.

Gordon, L., Loeb, M., Lucyshyn, W. and Zhou, L. (2018) 'Empirical Evidence on the Determinants of Cybersecurity Investments in Private Sector Firms', *Journal of Information Security*, 9(2), p. 133-153.

Grace, M. F., Leverty, J. T., Phillips, R. D. and Shimpi, P. (2014) 'The value of investing in enterprise risk management', *Journal of Risk and Insurance*, 82(2), pp. 289–316. doi: 10.1111/jori.12022.

Grant Thornton (2013) 'Banking risk: enhancing your enterprise-wide risk management framework'. Available at: http://www.mckinsey.com/business-functions/risk/our-insights/transforming-enterprise-risk-management-for-value-in-the-insurance-industry (Accessed: 12 September 2016).

Grant Thornton (2016) 'Risk frameworks: driving business strategy with effective risk frameworks'. Available at: http://www.grantthornton.co.uk/globalassets/1.-member-firms/united-kingdom/pdf/flyers/risk-frameworks-driving-business-strategy-with-effective-risk-frameworks.pdf (Accessed: 20 August 2017).

Grant Thornton (2016) 'Taking aim at cyber risk '. Available at: https://www.grantthornton.com/~/media/content-page-files/advisory/pdfs/2016/ADV-taking-aim-at-cyber-risk-2.ashx (Accessed: 16 January 2017).

Grant, M. J. and Booth, A. (2009) 'A typology of reviews: an analysis of 14 review types and associated methodologies', *Health Information and Libraries Journal*, 26: 91–108. doi:10.1111/j.1471-1842.2009.00848.x

Gray, D. (2014) *Doing research in the real world*. 3rd edn. London: Sage Publications Ltd.

Greenhalgh, T. (2004) 'Diffusion of Innovations in Service Organizations: Systematic Review and Recommendations', *The Milbank Quarterly*, 82(4), pp. 581-629. doi: 10.1111/j.0887-378x.2004.00325.x.

Greenwood, R., Hinings, C.R. and Whetten, D. (2014) 'Rethinking institutions and organizations', *Journal of Management Studies*, 51 (7) pp. 1206-1220. doi: 10.1111/joms.12070.

Gregor, S., Hart, D. and Martin, N. (2007) 'Enterprise architectures: enablers of business strategy and IS/IT alignment in government'. *Information Technology & People*, 20(2), pp. 96-120.

Gresov, C. (1989) 'Exploring fit and Misfit with multiple contingencies', *Administrative Science Quarterly*, 34(3), p. 431. doi: 10.2307/2393152.

Griffin, M. and Boomgaard, R. (1999) 'Enterprise risk and return management for financial institutions', *North American Actuarial Journal*, 3(2), pp. 48-56. doi: 10.1080/10920277.1999.10595799.

Guest, G., MacQueen, K. and Namey, E. (2011) *Applied thematic analysis*. Los Angeles: SAGE.

Gupta, P.P., Dirsmith, M. W. and Fogarty, T.J. (1994) 'Coordination and control in a government agency: Contingency and institutional theory perspectives on GAO audits', *Administrative Science Quarterly*, 39(2), p. 264. doi: 10.2307/2393236.

Gutierrez, A., Orozco, J. and Serrano, A. (2009) 'Factors affecting IT and business alignment: A comparative study in SMEs and large organisations', *Journal of Enterprise Information Management*, 22(1/2), pp. 197–211. doi: 10.1108/17410390910932830.

Hagen, J. M., Albrechtsen, E. and Hovden, J. (2008) 'Implementation and effectiveness of organizational information security measures', *Information Management & Computer Security*, 16 (4), pp. 337-397. doi: 10.1108/09685220810908796.

Hall, E. (1999) 'Risk management return on investment', *Systems Engineering*, 2(3), pp. 177-180.

Hambrick, D.C. and Lei, D. (1985) 'Towards an empirical prioritization of contingency for business strategy', *Academy of Management Journal*, 28(4), pp. 763–788. doi: 10.2307/256236.

Hampton, J. J. (2015) *Fundamentals of Enterprise risk management: how top companies assess risk, manage exposure, and seize opportunity*. 2nd edn. New York: American Management Association.

Hanson, E. M. (1979) 'School management and contingency theory: An emerging perspective', *Educational Administration Quarterly*, 15(2), pp. 98–116. doi: 10.1177/0013161x7901500209.

Harding, J. (2013) *Qualitative data analysis from start to finish*. Sage Publications Ltd: London.

Hardy, K., and Runnels, A. (2014) *Enterprise Risk Management: a guide for government professionals*. San Francisco: Wiley.

Hart, C. (2014) *Doing a literature review: releasing the social science research imagination.* Sage Publications Ltd: London.

Harvard Business Review (2011) *Aligning technology with strategy*. Boston: Harvard Business School Publishing.

Hatch, M. J. and Cunliffe, A. L. (2013) *Organization theory: Modern, symbolic, and postmodern perspectives*. 3rd edn. Oxford: Oxford University Press.

Hayne, C. and Free, C. (2014) 'Hybridized professional groups and institutional work: COSO and the rise of enterprise risk management', *Accounting, Organizations and Society*, 39(5), pp. 309–330. doi: 10.1016/j.aos.2014.05.002.

Henderson, H. (2009) *Encyclopedia of computer science and technology*. New York: Chelsea House Publishers.

Henderson, J. C. and Venkatraman, H. (1993) 'Strategic alignment: leveraging information technology for transforming organizations', *IBM Systems Journal*, 32(1), pp. 472–484. doi: 10.1147/sj.382.0472.

Henderson, J. C. and Venkatraman, N. (1989) *Strategic alignment: a framework for strategic information technology management*. Cambridge: Massachusetts Institute of Technology.

Henderson, J. C. and Venkatraman, N. (1990) *Strategic Alignment: a model for organizational transformation via information technology*. Sloan School of Management, Cambridge: Massachusetts Institute of Technology.

Hetcher, S.A. and Postema, G. (2004) *Social norms in a wired world*. Edited by Jules L. Coleman. Cambridge, United Kingdom: Cambridge University Press.

Hickson, D. J., Hinings, C. R., Lee, C. A., Schneck, R. E. and Pennings, J. M. (1971) A strategic contingency' theory of intraorganizational power, *Administrative Science Quarterly*, 15 (2), pp. 216-229.

Hillson, D. (2002) 'Extending the risk process to manage opportunities', *International Journal of Project Management*, 20(3), pp. 235–240. doi: 10.1016/s0263-7863(01)00074-6.

Hinkelmann, K., Gerber, A., Karagiannis, D., Thoenssen, B., van der Merwe, A. and Woitsch, R. (2015) 'A new paradigm for the continuous alignment of business and IT: Combining enterprise architecture modelling and enterprise ontology', *Computers in Industry*. doi: 10.1016/j.compind.2015.07.009.

HM Government (2014) 'HMG Security Policy Framework'. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework_-_web_-_April_2014.pdf (Accessed: 3 June 2016).

HM Government (2015a) 'FTSE 350 Cyber governance health check tracker report'. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/3992

60/bis-15-37-ftse-350-cyber-governance-health-check-tracker-report-2014.pdf (Accessed: 23 June).

HM Government (2015b) 'Small businesses: what you should need to know about cyber security'. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/412017/BIS-15-147-small-businesses-cyber-guide-March-2015.pdf (Accessed: 16 May 2015).

HM Government (2015c) 'Cyber Essentials Scheme: assurance framework'. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400914/bis-15-72-cyber-essentials-scheme-assurance-framework.pdf (Accessed: 5 July 2016).

HM Treasury (2004) 'The Orange book: management of risk – principles and concepts'. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/220647/orange_book.pdf (Accessed: 28 April 2015).

HM Treasury (2009) 'Risk management assessment framework: a tool for departments'. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/191516/Risk_management_assessment_framework.pdf (Accessed: 19 May 2016).

Hodgson, G. M. (2006) 'What are institutions?', *Journal of Economic Issues*, 40(1), pp. 1–25. doi: 10.1080/00213624.2006.11506879.

Hoffer, C. W. (1975) 'Toward a contingency theory of business strategy', *Academy of Management Journal*, 18(4), pp. 784–810. doi: 10.2307/255379.

Hofmann, M.A. (2009) 'Interest in enterprise risk management is growing', *Business insurance*, 43(18), pp. 14-16.

Hong, K., Chi, Y., Chao, L. R. and Tang, J. (2003) 'An integrated system theory of information security management', *Information Management and Computer Security*, 11(5), pp. 243–248. doi: 10.1108/09685220310500153.

Hopkin, P. (2014) *Fundamentals of risk management: understanding and implementing effective risk management.* London: Kogan Page.

Hopkin, P. (2017) *Fundamentals of Risk Management: Understanding, evaluating and implementing effective risk management*, 4th edn. London: Kogan Page Publishers.

Hopkin, P. (2018) *Fundamentals of Risk Management*. London: Kogan Page, Limited.

Hopkins, D. (2005) *The practice and theory of school improvement*. New York, NY, United States: Springer-Verlag New York.

Hosseinbeig, S., Moghadam, D.K., Vahdat, D. and Moghadam, R.A.(2011) 'Combination of IT strategic alignment and IT governance to evaluate strategic alignment maturity', *In Application of Information and Communication Technologies (AICT)*, 2011 5th International Conference on (pp. 1-10). IEEE.

Hoyt, R. E. and Liebenberg, A. P. (2011) 'The value of enterprise risk management', *Journal of Risk and Insurance*, 78(4), pp. 795–822. doi: 10.1111/j.1539-6975.2011.01413.x.

Hsu, C., Lee, J.-N. and Straub, D. W. (2012) 'Institutional influences on information systems security innovations', *Information Systems Research*, 23(3-part-2), pp. 918–939. doi: 10.1287/isre.1110.0393.

Hu, Q., Hart, P. and Cooke, D. (2007) 'The role of external and internal influences on information systems security – a neo-institutional perspective', *The Journal of Strategic Information Systems*, 16(2), pp. 153–172. doi: 10.1016/j.jsis.2007.05.004.

Huang, C. D. and Hu, Q. (2007) 'Achieving IT-business strategic alignment via enterprise-wide implementation of Balanced Scorecards', *Information Systems Management*, 24(2), pp. 173–184. doi: 10.1080/10580530701239314.

Humphreys, E. (2008) 'Information security management standards: Compliance, governance and risk management', *Information Security Technical Report*, 13(4), pp. 247–255. doi: 10.1016/j.istr.2008.10.010.

ICAEW (2014) 'Cyber-security in corporate finance'. Available at: https://www.sec.gov/comments/4-673/4673-3.pdf (Accessed: 1 April 2015).

Iden, J., Methlie, L. and Christensen, G. (2016) 'The nature of strategic foresight research: A systematic literature review', Technological Forecasting and Social Change, 116, pp.87-97.

Ignatow, G. and Mihalcea, R. (2017) *An introduction to text mining: research design, data collection, and analysis*. SAGE Publications.

Imenda, S. (2014) 'Is there a conceptual difference between theoretical and conceptual frameworks', *Journal of Social Sciences*, 38(2), pp. 185-195.

Information Security Forum (2011) 'The 2011 standard of good practice for information securit'y. Available at: https://www.uninett.no/webfm_send/730 (Accessed: 14 May 2016).

Information Systems Security Association (ISSA) (2004) 'Generally accepted information security principles'. Available at: https://citadel-information.com/wp-content/uploads/2010/12/issa-generally-accepted-information-security-practices-v3-2004.pdf (Accessed: 1 February 2016).

Institute of Risk Management (2002) 'A risk management standard'. Available at: https://www.theirm.org/media/886059/ARMS_2002_IRM.pdf (Accessed: 28 April 2015).

Institute of Risk Management (2018) 'A Risk Practitioners Guide to ISO 31000: 2018: Review of the 2018 version of the ISO 31000 risk management guidelines and commentary on the use of this standard by risk professionals'. Available at: https://www.theirm.org/media/3513119/IRM-Report-ISO-31000-2018-v3.pdf (Accessed: 2 November 2018).

International Monetary Fund (2017) 'Cyber Risk, Market Failures, and Financial Stability', *IMF Working Papers*, 17(185), p.1-36.

ISACA (2012) *Cobit 5: A business framework for the governance and management of enterprise IT*. Rolling Meadows. IL: ISACA.

ISACA (2013) *Transforming cybersecurity using COBIT 5*. Rolling Meadows, IL: ISACA.

Iswajuni, I., Arina Manasikana, A. and Soetedjo, S. (2018) 'The effect of enterprise risk management (ERM) on firm value in manufacturing companies listed on Indonesian Stock Exchange year 2010-2013', *Asian Journal of Accounting Research*, doi: 10.1108/AJAR-06-2018-0006.

IT Governance (2015) 'ISO 27001 global report'. Available at: http://www.itgovernance.co.uk/download/ISO27001-Global-Report-2015.pdf (Accessed: 30 March 2015).

Iyengar, G. (2007) *Introduction to banking*. New Delhi: Excel Books.

Jaffee, D. (2001) *Organization theory: Tension and change*. London, United Kingdom: McGraw-Hill Higher Education.

Jankowicz, A. D. (2005) *Business research projects*. 4th edn. London: International Thomson Business Press.

Jesson, J., Matheson, L. and Lacey, F. M. (2011) *Doing your literature review: Traditional and systematic techniques*. London: SAGE Publications.

Jevtić, M., Jovanović, M. and Krivokapić, J. (2018) 'A New Approach to Measuring the Correlation of Organizational Alignment and Performance', *Management: Journal of Sustainable Business and Management Solutions in Emerging Economies*, 23(1), p.41.

Johnson, A. M. and Lederer, A. L. (2010) 'CEO/CIO mutual understanding, strategic alignment, and the contribution of IS to the organization', *Information and Management*, 47(3), pp. 138–149. doi: 10.1016/j.im.2010.01.002.

Jorion, P. (2009) 'Risk management lessons from the credit crisis', *European Financial Management*, 15(5), pp. 923–933. doi: 10.1111/j.1468-036x.2009.00507.x.

Jøsang, A., Ismail, R. and Boyd, C. (2007) 'A survey of trust and reputation systems for online service provision', *Decision Support Systems*, 43(2), pp.618-644.

Joshi, A., Bollen, L., Hassink, H., De Haes, S. and Van Grembergen, W. (2018) 'Explaining IT governance disclosure through the constructs of IT governance maturity and IT strategic role', *Information & Management*, 55(3), pp. 368-380.

Julisch, K. (2013) 'Understanding and overcoming cyber security anti-patterns', *Computer Networks*, 57(10), pp. 2206–2211. doi: 10.1016/j.comnet.2012.11.023.

Kaplan, J., Bailey, T. and Rezek, C. (2015) *Beyond cybersecurity: protecting your digital business*. United States: Wiley.

Kaplan, R. and Norton, D. (2003) *Strategy Maps: Converting Intangible Assets into Tangible Outcomes*. Boston, Mass.: Harvard Business School Press.

Karpovsky, A. and Galliers, R. D. (2015) 'Aligning in practice: From current cases to a new agenda', *Journal of Information Technology*, 30(2), pp. 136–160. doi: 10.1057/jit.2014.34.

Kast, F. E. and Rosenzweig, J. E. (1973) *Contingency views of organization and management*. Chicago: Science Research Associates Inc., USA.

Kauspadiene, L., Cenys, A, Goranin, N., Tjoa, S. and Ramanauskaite, S. (2017) 'High-level self-sustaining Information Security management framework', *Baltic J. Modern Computing*, 5(1), pp. 107-123. Available at: http://www.bjmc.lu.lv/fileadmin/user_upload/lu_portal/projekti/bjmc/Contents/5_1_07_Kauspadiene.pdf (Accessed: 11 August 2017).

Kearns, G. and Lederer, A. (2000) 'The effect of strategic alignment on the use of IS-based resources for competitive advantage', *The Journal of Strategic Information Systems*, 9(4), pp. 265–293. doi: 10.1016/s0963-8687(00)00049-4.

Keith, J. L. (2014) *Developing a strategic ERM alignment framework-finance sector*. PhD. Brunel University London. Available at: http://bura.brunel.ac.uk/handle/2438/10981 (Accessed: 26 January 2016).

Kerstin, D., Simone, O. and Nicole, Z. (2014) 'Challenges in implementing enterprise risk management', *ACRN Journal of Finance and Risk Perspectives*, 3(3), pp. 1-14.

Khan, M., Hussain, D. and Mehmood, W. (2016) 'Why do firms adopt enterprise risk management (ERM)? Empirical evidence from France', *Management Decision*, 54(8), pp.1886-1907.

Kimbrough, R. and Componation, P. (2009) 'The Relationship Between Organizational Culture and Enterprise Risk Management', *Engineering Management Journal*, 21(2), pp.18-26.

Kitchenham, B. and Charters, S. (2007) 'Guidelines for performing systematic literature reviews in software engineering', *Evidence-Based Software Engineering (EBSE) Technical Report Engineering.* Available at: https://www.elsevier.com/__data/promis_misc/525444systematicreviewsguide.pdf (Accessed: 17 September 2017).

Kleffner, A. E., Lee, R. B. and McGannon, B. (2003) 'The effect of corporate governance on the use of enterprise risk management: Evidence from Canada', *Risk Management and Insurance Review*, 6(1), pp. 53–73. doi: 10.1111/1098-1616.00020.

Klüppelberg, C. Straub, and D Welpe, I. (2014) *Risk: a multidisciplinary introduction.* London: Springer International Publishing.

Korovessis, P., Furnell, S., Papadaki, M. and Haskell-Dowland, P. (2017) 'A toolkit approach to information security awareness and education', *Journal of Cybersecurity Education, Research and Practice*, 5(2), p. 1-32.

Kotulic, A. G. and Clark, J. G. (2004) 'Why there aren't more information security research studies', *Information and Management*, 41(5), pp. 597–607. doi: 10.1016/j.im.2003.08.001.

Kouns, J. and Minoli, D. (2010) *Information technology risk management in enterprises environments: a review of industry practices and practical guide to risk management teams*. Hoboken: John Wiley and Sons, Inc.

KPMG (2009) 'Placing a value on enterprise risk management'. Available at: https://www.kpmg.com/PT/pt/IssuesAndInsights/Documents/erm22432PHL.pdf (Accessed: 10 September 2016).

KPMG (2013a) 'The five most common cyber security mistakes: management's perspective on cyber security'. Available at: https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/five-most-common-cyber-security-mistakes.PDF (Accessed: 28 April 2015).

KPMG (2013b) 'Expectations of risk management: outpacing capabilities-it's time for action'. Available at: https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/risk-management-outpacing-capabilities/Documents/expectations-risk-management-survey.pdf (Accessed: 9 September 2016).

KPMG (2014a) 'Aligning IT risk management with the enterprise through effective KRIs'. Available at: http://www.kpmg-institutes.com/content/dam/kpmg/kpmginstitutes/pdf/2014/aligning-it-risk-management.pdf (Accessed: 6 March 2015).

KPMG (2014b) 'Cyber security: it's not just about technology: the five most common mistakes'. Available at: http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-security-not-just-technology.pdf (Accessed: 1 April 2015).

KPMG (2014c) 'Governance strategies for managing the data lifecycle: knowing when to fold versus hold and protect', *Frontiers in Finance*, April 2014 http://www.kpmg.com/BE/en/IssuesAndInsights/ArticlesPublications/Frontiers-in-finance/Documents/fif-april-2014.pdf (Accessed: 5 March 2015).

KPMG (2014d) 'Cyber Security: from threat to opportunity'. Available at: https://www.kpmg.com/NL/nl/IssuesAndInsights/ArticlesPublications/Documents/PDF/IT-Advisory/Cyber-Security-From-threat-to-opportunity.pdf (Accessed: 11 May 2015).

KPMG (2014e) 'Global boardroom insights: the cyber security challenge'. Available at: https://audit-committee-institute.de/docs/aci_gbi_3_cyber_security_challenge.pdf (Accessed: 20 May 2015).

KPMG (2015) 'Connecting the dots: a proactive approach to cybersecurity oversight in the boardroom'. Available at: https://assets.kpmg.com/content/dam/kpmg/pdf/2016/05/Cyber-Security-and-Board-Oversight-Whitepaper.pdf (Accessed: August 2016).

KPMG (2017a) 'Enterprise wide risk management'. Available at: https://assets.kpmg.com/content/dam/kpmg/ch/pdf/enterprise-wide-risk-management-en.pdf (Accessed: 20 August 2017).

KPMG (2017b) 'Enterprise risk management: protecting and enhancing value'. Available at: https://home.kpmg.com/content/dam/kpmg/at/images/Themen/corporate-risk-management/enterprise-risk-management-protecting-and-enhancing-value.pdf?logActivity=true (Accessed: January 2018).

Kuehl, D.T. (2009) 'From cyberspace to cyberpower: Defining the problem'. *Cyberpower and national security*, pp. 26-28. Available at: http://ctnsp.dodlive.mil/files/2014/03/cyberpower-i-chap-02.pdf (Accessed: 10 October 2016).

Kurbalija, J. (2014) 'An introduction to internet governance', 6th ed. Switzerland: DiploFoundation. Available at: (http://www.diplomacy.edu/sites/default/files/An%20Introduction%20to%20IG_6th%20edition.pdf (Accessed: 11 October 2016).

Kvale, S. (2010) *Doing interviews: The Sage qualitative research kit*. Los Angeles: Sage Publications Ltd, United Kingdom

Lalitha, S. M., and A. Satya Nandini (2015) 'Impact of effective enterprise risk management on business relationship', *Reflections-Journal of Management*, 4 (1).

Lam, J. (2017) *Implementing enterprise risk management: from methods to applications*. New Jersey: John Wiley & Sons.

Lauder, M. (2016) *In pursuit of foresight: disaster incubation theory Re-imagined*. New York: Routledge.

Laudon, K. C. And Laudon, J. (2010) *Management information systems: managing the digital firm*. 11th edn. London: Pearson Education, Ltd.

Lawrence, P. R. and Lorsch, J. W. (1967) Differentiation and integration in complex organization, *Administrative Science Quarterly*, 2 (1), pp. 1-47.

Lawrence, T. B. and Shadnam, M. (2008) *Institutional Theory*. In: Donsbach, Wolfgang, (ed.) The International Encyclopedia of Communication. Blackwell Publishers, Oxford, pp. 2288-2293. ISBN 978-1-4051-3199-5.

Leavy, P. (2017) *Research design: Quantitative, qualitative, mixed methods, arts-based, and community-based participatory research approaches*. New York: Guilford Publications.

Lechner, P. and Gatzert, N. (2018) 'Determinants and value of enterprise risk management: empirical evidence from Germany', *The European Journal of Finance*, (24)10, pp. 867-887, doi: 10.1080/1351847X.2017.1347100.

Lehto, M. and Neittaanmäki, P. (eds.) (2015) *Cyber security: Analytics, technology and automation*. United States: Springer International Publishing.

Lenssen, J. J. A. Dentchev, N. and Roger, L. (2014) 'Sustainability, risk management and governance: Towards an integrative approach', *Corporate Governance: The International Journal of Business in Society*, 14(5), pp. 670–684. doi: 10.1108/cg-07-2014-0077.

Lewis-Beck, M., Bryman, A. and Liao, T. F. (eds.) (2004) *The sage encyclopedia of social science research methods*. Thousand Oaks, CA: SAGE Publications.

Li, L. S. (2018) 'A study on enterprise risk management and business performance', Journal of Financial', *Risk Management*, 7, pp.123-138.

Li, L., He, W., Xu, L., Ash, I., Anwar, M. and Yuan, X. (2019) 'Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior', International Journal of Information Management, 45, pp.13-24.

Liebenberg, A. P. and Hoyt, R. E. (2003) 'The determinants of enterprise risk management: Evidence from the appointment of chief risk officers', *Risk Management and Insurance Review*, 6(1), pp. 37–52. doi: 10.1111/1098-1616.00019.

Lin, Y., Wen, M. M. and Yu, J. (2012) 'Enterprise risk management: strategic antecedents, risk integration, and performance', *North American Actuarial Journal*, 16(1), pp. 1–28. doi: 10.1080/10920277.2012.10590630.

Lindberg, D. L. and Seifert, D. L. (2011) 'Enterprise risk management (ERM) can assist insurers in complying with the Dodd-Frank Act', *Journal of Insurance Regulation*, 30(1), pp. 319-337.

Lloyd's (2010) 'Globalisation and risks for business: implications for an increasingly interconnected world'. Available at: https://www.lloyds.com/~/media/lloyds/reports/360/360%20globalisation/lloyds_360_globalisaton.pdf (Accessed: 28 April 2015).

Lorsch, J. (2013) 'Contingency Theory', in Kessler, E.H. (ed.) *Encyclopaedia of Management Theory*. SAGE Publications

Luburić, R. (2017) 'Strengthening the Three Lines of Defence in Terms of More Efficient Operational Risk Management in Central Banks', Journal *of Central Banking Theory and Practice*, 6(1), pp. 29-53.

Luftman, J. (2000) 'Assessing business-IT alignment maturity', *Communication of the Association for Information Systems*, 4(14), pp. 1-50.

Luftman, J. (2001) 'Assessing business-IT alignment maturity', *Opportunities for Competitive Advantage*, pp. 135–149. doi: 10.4018/978-1-878289-87-2.ch006.

Luftman, J. and Kempaiah, R. (2007) 'An update on IT: business alignment: "a line" has been drawn', *MIS Quarterly Executive*, 6(3), pp. 165–177.

Luftman, J. N., Papp, R. and Brier, T. (1999) 'Enablers and inhibitors of business-IT alignment', *Communications of the Association for Information Systems*, 1(11), pp. 1–33.

Luftman, J., Lyytinen, K. and ben Zvi, T. (2015) 'Enhancing the measurement of information technology (IT) business alignment and its influence on company performance', *Journal of Information Technology*, doi: 10.1057/jit.2015.23.

Luhman, N. (1991) *Risk: a sociological theory*. Berlin: Walter de Gruyter and Co.

Lundqvist, S. A. (2014) 'An exploratory study of enterprise risk management: Pillars of ERM', *Journal of Accounting, Auditing and Finance*, 29(3), pp. 393–429. doi: 10.1177/0148558x14535780.

Lundqvist, S. A. (2015) 'Why firms implement risk governance – stepping beyond traditional risk management to enterprise risk management', *Journal of Accounting and Public Policy*, 34(5), pp. 441–466. doi: 10.1016/j.jaccpubpol.2015.05.002.

Lundqvist, S. and Vilhelmsson, A. (2016) 'Enterprise Risk Management and Default Risk: Evidence from the Banking Industry', *Journal of Risk and Insurance*, 85(1), pp. 127-157.

Luthans, F. and Stewart, T. I. (1977) 'A general contingency theory of management', *The Academy of Management Review*, 2(2), pp. 181–195. doi: 10.2307/257902.

Lyons, V. S. (2015) 'Enterprise risk management and five lines of corporate defence', *The Journal of Enterprise Risk Management*, 1(1), pp. 72-97.

Ma, Q., Schmidt, M. B. and Pearson, J. M (2009) 'An integrated framework for information security management', *Review of Business*, 30 (1), pp. 58-69.

Maguire, M. and Delahunt, B. (2017) 'Doing a thematic analysis: A practical, step-by-step guide for learning and teaching scholars. *AISHE-J: The All Ireland Journal of Teaching and Learning in Higher Education*, 9(3).

Majdalawieh, M. and Gammack, J. (2017) 'An Integrated Approach to Enterprise Risk: Building a Multidimensional Risk Management Strategy for the Enterprise', *International Journal of Scientific Research and Innovative Technology*, 4(2), pp.95-114.

Malone, T. W. and Crowston, K. (1990) 'What is coordination theory and how can it help design cooperative work systems?', Association for Computing Machinery (ACM). pp. 357–370. doi: 10.1145/99332.99367

Malone, T. W. and Crowston, K. (1994) 'The interdisciplinary study of coordination', *ACM Computing Surveys*, 26(1), pp. 87–119. doi: 10.1145/174666.174668.

Mandani, A. and Ramirez R. (2019) 'Cybersecurity: Current State of Governance Literature', in: *Twenty-fifth Americas Conference on Information Systems*, Cancun, 15-17 August, Cancun.

Manigent (2009) 'Aligning risk appetite and exposure'. Available at: http://riskbasedperformance.com/2009/09/22/aligning-risk-appetite-and-exposure/ (Accessed: 6 August 2016).

Manigent (2011) 'Embedding risk appetite within the strategy process'. Available at: http://static1.1.sqspcdn.com/static/f/239218/14725422/1319101184223/Embedding+Risk+Appetite+within+the+Strategy+Process.pdf?token=tPVpFtTsXYuU5IddVWSABvfyjM4%3D (Accessed: 8 August 2016).

Marotta, A., and McShane, M. (2018) 'Integrating a proactive technique into a holistic cyber risk management approach', *Risk Management and Insurance Review*, 21(3), 435-452. doi:10.1111/rmir.12109.

Marsh (2015) 'UK 2015 Cyber risk survey report'. Available at: http://uk.marsh.com/Portals/18/Documents/UK%202015%20Cyber%20Risk%20Survey%20Report-06-2015.pdf (Accessed: 22 June 2015).

Mayer, N., Aubert, J., Grandry, E., Feltus, C., Goettelmann, E. and Wieringa, R. (2019) 'An integrated conceptual model for information system security risk management supported by enterprise architecture management', *Software & Systems Modeling*, 18(3), pp.2285-2312.

Mason, J. (2002) *Qualitative researching*. 2nd edn. Thousand Oaks, CA: Sage Publications.

Matthews, B. and Ross, L. (2010) *Research methods: A practical guide for the social sciences*. New York, NY: Pearson Longman.

Maxwell, J. (1992) 'Understanding and validity in qualitative research', *Harvard Educational Review*, 62(3), pp. 279–301. doi: 10.17763/haer.62.3.8323320856251826.

Maxwell, J. (2012) *Qualitative research design*. 1st ed. Thousand Oaks, Calif.: SAGE Publications.

Maxwell, J. (2013) *Qualitative research design: an interactive approach*. Thousand Oaks, Calif.: SAGE Publications.

Maylor, H. and Blackmon, K. L. (2005) *Researching business and management*. Basingstoke, Hampshire: Palgrave Macmillan.

Maynard, S. B., Tan, T., Ahmad, A., and Ruighaver, T. (2018) 'Towards a Framework for Strategic Security Context in Information Security Governance', *Pacific Asia Journal of the Association for Information Systems*, 10(4), pp. 65-88.

McAfea (2018) 'The economic impact of cybercrime—no slowing down'. Available at: https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf (Accessed: 29 November 2018).

McAfee (2013) 'The economic impact of cybercrime and cyber espionage'. Available at: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf (Accessed: 14 November 2016).

McAfee (2014) 'Net losses: estimating the global cost of cybercrime, economic impact of cybercrime II'. Available at: http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf (Accessed: 28 April 2015).

McKinsey and Company (2010) 'Top-down ERM: a pragmatic approach to managing risk from the C-suite'. Available at: http://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Top-down%20ERM/Topdown%20ERM.ashx (Accessed 10 August 2016).

McKinsey and Company (2013a) 'Enterprise risk management –shaping the risk revolution'. Available at: http://www.rmahq.org/File%20Library/ERM/ERM---Shaping-the-Risk-Revolution.pdf (Accessed: 1 July 2015).

McKinsey and Company (2013b) 'Getting to ERM: a roadmap for banks and other financial institutions'. Available at: http://www.mckinsey.com/business-functions/risk/our-insights/getting-to-erm-a-road-map-for-banks-and-other-financial-institutions (Accessed: 20 August 2017).

McKinsey and Company (2014) 'Enterprise-risk-management: where's the evidence? a survey across two European countries'. Available at: http://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/risk/working%20papers/53_risk_paper_schmalenbach-survey.ashx (Accessed: 17 June 2015).

McKinsey and Company (2016) 'Transforming enterprise risk management for value in the insurance industry'. Available at: http://www.mckinsey.com/business-functions/risk/our-insights/transforming-enterprise-risk-management-for-value-in-the-insurance-industry (Accessed: 10 September 2016).

McShane, M. (2018) 'Enterprise risk management: history and a design science proposal', *The Journal of Risk Finance*, 19(2), pp. 137-153.

McShane, M. K., Nair, A. and Rustambekov, E. (2011) 'Does enterprise risk management increase firm value?', *Journal of Accounting, Auditing and Finance*, 26(4), pp. 641–658. doi: 10.1177/0148558x11409160.

Mehan, J. (2014) *Cyberwar, Cyberterror, Cybercrime & Cyberactivism (2nd Edition): An in-depth guide to the role of standards in the cybersecurity environment*. IT Governance Ltd.

Mekawy, M. E., AlSabbagh, B. and Kowalski, S. (2014) 'The impact of business-IT alignment on information security process', *In Lecture Notes in Computer Science*, Springer Science + Business Media. pp. 25–36. doi: 10.1007/978-3-319-07293-7_3.

Mensah, G. and Gottwald, W. (2016) 'Enterprise Risk Management: factors associated with effective implementation', *Risk Governance and Control: Financial Markets & Institutions*, 6(4).

Merhi, M. and Ahluwalia, P. (2018)' Examining the impact of deterrence factors and norms on resistance to Information Systems Security', Computers *in Human Behavior*.

Merna, T. and Thani, F. A. (2008) *Corporate risk management*. 2nd edn. West Sussex: John Wiley and Sons, Ltd.

Mertler, C.A. (2015) *Introduction to educational research*. United States: Sage Publications.

Meyer, J. W. and Rowan, B. (1977) 'Institutionalized organizations: Formal structure as myth and ceremony', *American Journal of Sociology*, 83(2), p. 340. doi: 10.1086/226550.

Meyer, R. E. and Höllerer, M.A. (2014) 'Does institutional theory need redirecting?', *Journal of Management Studies*, 51 (7), pp. 1221–1233. doi: 10.1111/joms.12089.

Mikes, A. (2009) 'Risk management and calculative cultures', *Management Accounting Research*, 20(1), pp. 18–40. doi: 10.1016/j.mar.2008.10.005.

Miles, R. E., Snow, C.C., Meyer, A.D. and Coleman, H.J. (1978) 'Organisational strategy, structure and process', *The Academy of Management Review*, 3 (3), pp. 546-562.

Miller, K. D. (1992) 'A framework for integrated risk management in international business', *Journal of International Business Studies*, 23(2), pp. 311–331. doi: 10.1057/palgrave.jibs.8490270.

Min, K.-S., Chai, S.W. and Han, M. (2015) 'An international comparative study on Cyber security strategy', *International Journal of Security and Its Applications*, 9(2), pp. 13–20. doi: 10.14257/ijsia.2015.9.2.02.

Mindell, D.A. (2000) 'Cybernetics: knowledge domains in engineering systems'. Available at: http://web.mit.edu/esd.83/www/notebook/Cybernetics.PDF (Accessed: 10 October 2016).

Mintzberg, H. (1979) *The structuring of organizations*. United States: Pearson Education (US).

Mitra, A. and Schwartz, R. L. (2006) 'From Cyber space to Cybernetic space: Rethinking the relationship between real and virtual spaces', *Journal of Computer-Mediated Communication*, 7(1), pp. 0–0. doi: 10.1111/j.1083-6101.2001.tb00134.x.

Mohammed, D. (2015) 'Cybersecurity compliance in the financial sector', *Journal of Internet Banking and Commerce*, 20(1), pp. 1-11.

Molina, L. D. (2015) *Basic research strategies*. iUniverse. doi: 9781491774809.

Morrison, E.D., Ghose, A.K., Dam, H.K., Hinge, K.G. and Hoesch-Klohe, K. (2011) 'Strategic alignment of business processes'. In *International Conference on Service-Oriented Computing* (pp. 9-21). Springer, Berlin, Heidelberg.

Moschovitis, C. (2018) *Cybersecurity Program Development for Businesses: The Essential Planning Guide*. 1st ed. John Wiley and Sons.

Myers, M. D. (2013) *Qualitative research in business and management*. 2nd edn. London: SAGE Publications.

Nag, R., Hambrick, D. C. and Chen, M.-J. (2007) 'What is strategic management, really? Inductive derivation of a consensus definition of the field', *Strategic Management Journal*, 28(9), pp. 935–955. doi: 10.1002/smj.615.

Nair, A., Rustambekov, E., McShane, M. and Fainshmidt, S. (2013) 'Enterprise risk management as a dynamic capability: a test of its effectiveness during a crisis', *Managerial and Decision Economics*, 35(8), pp. 555–566. doi: 10.1002/mde.2641.

Nasir, A., Arshah, R., Hamid, M. and Fahmy, S. (2019) 'An analysis on the dimensions of information security culture concept: A review', *Journal of Information Security and Applications*, 44, pp. 12-22.

Nason, R. and Fleming, L. (2018) *Essentials of Enterprise Risk Management: Practical Concepts of ERM for General Managers*. New York, United States: Business Expert Press.

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) (2015) 'National cyber security organization: United Kingdom'. Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_UK_032015_0.pdf (Accessed: 19 June 2015).

Nazareth, D. L. and Choi, J. (2015) 'A system dynamics model for information security management', *Information and Management*, 52(1), pp. 123–134. doi: 10.1016/j.im.2014.10.009.

New York Stock Exchange (2014) 'NYSE: Corporate governance guide'. Available at: https://www.nyse.com/publicdocs/nyse/listing/NYSE_Corporate_Governance_Guide.pdf (Accessed: 5 September 2016).

Nilsen, P. (2015) 'Making sense of implementation theories, models and frameworks', *Implementation Science*, 10(1). doi: 10.1186/s13012-015-0242-0.

NIST (2011) 'Managing information security risk: organization, mission, and system view, NIST Special Publication 800-39'. Available at: http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf (Accessed: 22 March 2015).

NIST (2013a) 'NIST special publication 800-53: security and privacy controls for federal information systems and organizations'. Available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf (Accessed: 6 July 2016).

NIST (2013b) *Glossary of key information security terms*. Available at: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf (Accessed: 3 February 2016).

NIST (2014) 'Framework for improving critical infrastructure cybersecurity'. Available at: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf (Accessed: 10 March 2015).

Nocco, B. W. and Stulz, R. M. (2006) 'Enterprise risk management: theory and practice', *Journal of Applied Corporate Finance*, 18(4), pp. 8–20. doi: 10.1111/j.1745-6622.2006.00106. x.

Nowell, L., Norris, J., White, D. and Moules, N. (2017) 'Thematic Analysis. *International', Journal of Qualitative Methods*, 16(1), p.160940691773384.

O'Hara, M., Carter, C., Dewis, P., Kay, J. and Wainwright, J. M. (2011) *Successful dissertations: The complete guide for education, childhood and early childhood studies students*. New York: Continuum International Pub. Group.

O'Leary, Z. (2014) 'The essential guide to doing your research project'. London: Sage Publication Ltd.

O'Reilly, C., Caldwell, D., Chatman, J., Lapiz, M. and Self, W. (2010). How leadership matters: The effects of leaders' alignment on strategy implementation, *The Leadership Quarterly*, 21(1), pp. 104-113.

OCEG (2009) *GRC Capability model ''Red Book'' 2.0*. Available at: http://thegrcbluebook.com/wp-content/uploads/2011/12/uploads_OCEG.RedBook2-BASIC.pdf (Accessed: 19 May 2016).

OCEG (2015) *GRC capability model version 3.0*. Available at: http://www.oceg.org/resources/red-book-3/#fullcontent (Accessed: 19 May 2016).

OECD (2002) 'OECD guidelines for the security of information systems and networks'. Available at: https://www.oecd.org/sti/ieconomy/15582260.pdf (Accessed: 6 May 2016).

O'Gorman, K. D. and MacIntosh, R. (2014) *Research methods for business and management: a guide to writing your dissertation*, Goodfellow Publishers, Oxford.

Oldfield, G. S. and Santomero, A.M. (1997) 'Risk management in financial institutions', *Sloan Management Review*, 39(1), pp. 33-46.

Oliveira, K., Méxas, M., Meiriño, M. and Drumond, G. (2018) 'Critical success factors associated with the implementation of enterprise risk management', *Journal of Risk Research*, pp. 1-16.

Oliveira, T. and Martins, M. F. (2011) 'Literature review of information technology adoption models at firm level', *The Electronic Journal Information Systems Evaluation*, 14 (1), pp. 110-121.

Oliver Wyman (2018a) 'When the going gets tough, the tough get going, overcoming the cyber risk appetite challenge'. Available at: https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2018/april/Oliver-Wyman-Overcoming-The-Cyber-Risk-Appetite-Challenge.pdf (Accessed: 26 October 2018).

Oliver Wyman (2018b) 'Large-scale cyber-attacks on the financial system: a case for better coordinated response and recovery strategies'. Available at:

https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2018/march/Large-Scale-Cyber-Attacks-DTCC-2018.pdf (Accessed: 5 December 2018).

Oliver, C. (1991) 'Strategic responses to institutional processes', *Academy of Management Review*, 16(1), pp. 145–179. doi: 10.5465/amr.1991.4279002.

Oliver, P. (2014) Writing *your thesis*. 3rd edn. London: Sage Publication Ltd.

Olson, D. and Wu, D. (2007) 'Enterprise risk management'. Hackensack, NJ: World Scientific Publishing Company.

Olum, Y. (2004) *Modern management theories and practices*. Uganda: Makerere University.

Olutoyin, O. and Flowerday, S. (2016) 'Successful IT governance in SMES: An application of the Technology–Organisation–Environment theory', *SA Journal of Information Management*, 18(1). doi: 10.4102/sajim.v18i1.696.

Organization for Economic Co-operation and Development (2014) 'Corporate governance: risk management and corporate governance'. Available at: http://www.oecd.org/daf/ca/risk-management-corporate-governance.pdf (Accessed: 12 June 2015).

Oxford Economic (2014) 'Cyber-attacks: effects on UK companies'. Available at:: http://www.cpni.gov.uk/documents/publications/2014/oxford-economics-cyber-effects-uk-companies.pdf?epslanguage=en-gb (Accessed: 28April 2015).

Paape, L. and Speklé, R. F. (2012) 'The adoption and design of enterprise risk management practices: An empirical study', *European Accounting Review*, 21 (3) pp. 533-564. doi: 10.1080/09638180.2012.661937.

Pagach, D., and R. Warr (2011) 'The characteristics of firms that hire chief risk officers', *Journal of Risk and Insurance*, 78: 185-211.

Paltridge, B., and Starfield, S. (2007) *Thesis and dissertation writing in a second language: A Handbook for Supervisors*. Oxon: Routledge.

Papp, R. (1999) 'Business-IT alignment: Productivity paradox payoff?', *Industrial Management and Data Systems*, 99(8), pp. 367–373. doi: 10.1108/02635579910301810.

Papp, R., Luftman, J. and Brier, T. (1996) 'Business and IT in harmony: enablers and inhibitors to alignment'. In Americas *Conference on Information Systems–AIS/ICIS* (Vol. 2).

Pellissier, R. (2007) *Business research made easy*. Cape Town, South Africa: Juta Legal and Academic Publishers.

Pennings, J. M. (1975) 'The relevance of the structural-contingency model for organizational effectiveness', *Administrative Science Quarterly*, 20(3), p. 393. doi: 10.2307/2391999.

Peppard, J. and Ward, J. (2004) 'Beyond strategic information systems: towards an IS capability', *The Journal of Strategic Information Systems*, 13(2), pp. 167–194. doi: 10.1016/j.jsis.2004.02.002.

Perrow, C. (1967) 'A framework for the comparative analysis of organizations', *American Sociological Review*, 32(2), p. 194. doi: 10.2307/2091811.

Pirson, M. and Turnbull, S. (2011) 'Corporate governance, risk management, and the financial crisis: An information processing view', *Corporate Governance: An International Review*, 19(5), pp. 459–470. doi: 10.1111/j.1467-8683.2011.00860.x.

Pitt, M. R. and Koufopoulos, D. (2012) *Essentials of strategic management*. United Kingdom: Sage Publications.

Ponemon Institute (2011) 'The role of governance, risk management and compliance in organizations study of GRC practitioners'. Available at: http://www.emc.com/collateral/about/news/ponemon-report-egrc.pdf (Accessed: 21 September 2015).

Ponemon Institute (2013) 'Managing cyber security as a business risk: cyber insurance in the digital age'. Available at: http://www.ponemon.org/local/upload/file/Cyber%20Insurance%20white%20paper%20FINAL%207.pdf (Accessed: 12 June 2015).

Ponemon Institute (2015) '2015 Cost of data breach study: United States'. Available at: http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03055usen/SEW03055USEN.PDF (Accessed: 28 May 2015).

Posthumus, S. and Von Solms, R. von (2004) 'A framework for the governance of information security', *Computers and Security*, 23(8), pp. 638–646. doi: 10.1016/j.cose.2004.10.006.

Powell, T. C. (1992) 'Organizational alignment as competitive advantage', *Strategic Management Journal*, 13(2), pp. 119–134. doi: 10.1002/smj.4250130204.

Power, M. (2009) 'The risk management of nothing', *Accounting, Organizations and Society*, 34(6-7), pp. 849–855. doi: 10.1016/j.aos.2009.06.001.

Power, M., Ashby, S. and Palermo, T. (2013) *Risk culture in financial organisations: A research report*. CARR-Analysis of Risk and Regulation.

Preston, D. S. and Karahanna, E. (2009) 'Antecedents of IS strategic alignment: A Nomological network', *Information Systems Research*, 20(2), pp. 159–179. doi: 10.1287/isre.1070.0159.

PricewaterhouseCoopers (2012) 'Black swans turn grey: the transformation of risks'. Available at: http://www.pwccn.com/webmedia/doc/635116518906857384_ia_risk_transform_aug2013.pdf (Accessed: 28 April 2015).

PricewaterhouseCoopers (2013a) 'UK Cyber security standards: research report, survey conducted by PwC'. Available at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/261681/bis-13-1294-uk-cyber-security-standards-research-report.pdf (Accessed: 29 April 2015).

PricewaterhouseCoopers (2013b) 'CTC Guide to enterprise risk management, beyond theory, a practitioner perspective on ERM'. Available: https://www.pwc.com/us/en/risk-management/assets/beyond-theory.pdf (Accessed: 6 October 2015).

PricewaterhouseCoopers (2014) 'Threat smart: building a cyber-resilient financial institution'. Available at: http://www.pwc.com/en_US/us/financial-services/publications/viewpoints/assets/pwc-cyber-resilient-financial-institution.pdf (Accessed: 31 March 2015).

PricewaterhouseCoopers (2015) 'Risk in review: decoding uncertainty, delivering value'. Available at: http://www.pwc.com/us/en/risk-assurance-services/risk-in-review/assets/risk-management-financial-leadership.pdf (Accessed: June 2015).

PricewaterhouseCoopers (2016) 'Moving forward with cybersecurity and privacy: how organisations are adopting innovative safeguards to manage threats and achieve competitive advantages in a digital era'. Available at: http://www.pwc.com/gx/en/information-security-survey/assets/gsiss-report-cybersecurity-privacy-safeguards.pdf (Accessed: 23 October 2016).

PricewaterhouseCoopers (2018) 'Enterprise risk management'. Available at : https://www.pwc.co.uk/audit-assurance/assets/pdf/enterprise-risk-management.pdf (Accessed 17 November 2018).

PricewaterhouseCoopers (PwC) (2009) 'Extending enterprise risk management to address emerging risks'. Available at: http://www.pwc.com/us/en/sap-implementation/assets/exploring_emerging_risk.pdf (Accessed: May 2016).

Prioteasa, A. and Ciocoiu, C. (2017) 'Challenges in implementing risk management: a review of the literature'. In *Proceedings of the International Management Conference* (Vol. 11, No. 1, pp. 972-980). Faculty of Management, Academy of Economic Studies, Bucharest, Romania.

Protivity (2012) 'Defining risk appetite: early mover series: integrating corporate performance management and risk management'. Available at: http://www.protiviti.co.uk/en-US/Documents/White-Papers/Risk-Solutions/Defining-Risk-Appetite-Early-Mover-Protiviti.pdf (Accessed: 6 September 2016)

Protivity (2018) 'Navigating changing dynamics of first line risk and control function'.Available at: https://www.protiviti.com/sites/default/files/united_kingdom/insights/agileriskgovframework_navigating_changing_dynamics_of_first_line_control_functions_sec.pdf (Accessed: 26 November 2018).

Pupke, D. (2008) *Compliance and corporate performance*. United States: Books on Demand.

PwC (2017) 'How your board can be effective in overseeing cyber risk: companies are under constant attack, making it critical that they get cybersecurity right'. Available at: https://www.pwc.dk/da/publikationer/2018/pwc-how-your-board-can-be-effective-in-overseeing-cyber-risk.pdf (Accessed: 7 September 2018).

PwC (2018b) 'Know the game, not just the rules: the changing face of cybersecurity'. Available at: https://www.pwc.co.uk/cyber-security/pdf/know-the-game-not-just-the-rules-march-18.pdf (Accessed: 4 December 2018).

Pym, A. (2014) *Status of the translation profession in the European unio*n. [n.i]: Anthem Press.

Quinland, C., Babin, B., Carr, C., Griffin, M. and Zikmund, W. (2015) *Business research methods*. 9th edn. Hampshire: Cengage Learning.

Raban, Y. and Hauptman, A. (2018) 'Foresight of cyber security threat drivers and affecting technologies'. *Foresight*. doi:10.1108/FS-02-2018-0020.

Rahman, S. and Donahue, S. (2010) 'Convergence of corporate and information security', *International Journal of Computer and Information Security*, 7(1), pp. 63-68.

Ramalingam, D., Arun, S. and Anbazhagan, N. (2018) 'A Novel Approach for Optimizing Governance, Risk management and Compliance for Enterprise Information security using DEMATEL and FoM', *Procedia Computer Science*, 134, pp.365-370.

Randolph, J. J. (2009) 'A guide to writing the dissertation literature review', *Practical Assessment, Research and Evaluation*, 14(13), pp.1-13.

Raz, T. and Hillson, D. (2005) 'A comparative review of risk management standards', *Risk manager (Bas)*, 7(4), pp. 53–66. doi: 10.1057/palgrave.rm.8240227.

Reed, T., Abbott, R. G., Anderson, B., Nauer, K. and Forsythe, C. (2014) 'Simulation of Workflow and threat characteristics for Cyber security incident response teams', *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 58(1), pp. 427–431. doi: 10.1177/1541931214581089.

Reich, B. H. and Benbasat, I. (2000) 'Factors that influence the social dimension of alignment between business and information technology objectives', *MIS Quarterly*, 24(1), p. 81-113. doi: 10.2307/3250980.

Reuvid, J. (2014) *Managing business risk: a practical guide to protecting your business.* 10th ed. London: Kogan Page.

Reynolds, P. and Yetton, P. (2015) 'Aligning business and IT strategies in multi-business organizations', *Journal of Information Technology*, 30(2), pp. 101–118. doi: 10.1057/jit.2015.1.

RIMS (2011) 'An overview of widely used risk management standards and guidelines'. Available at: https://www.rims.org/resources/ERM/Documents/RIMS%20Executive%20Report%20on%20Widely%20Used%20Standards%20and%20Guidelines%20March%202010.pdf (Accessed: 10 May 2016).

RIMS (2014) 'Transitioning to enterprise risk management'. Available at: https://rims.org/RiskKnowledge/RISKKnowledgeDocs/transitioningtoerm_4192017_122623.pdf (Accessed: 5 May 2017).

RIMS (2015) 'About the RIMS risk maturity model'. Available at: http://rims.logicmanager.com/LogicERM/documents/About%20the%20RIMS%20Risk%20Maturity%20Model%202015.pdf (Accessed: 16 May 2016).

Robinson, M., Jones, K. and Janicke, H. (2015) 'Cyber warfare: Issues and challenges', *Computers and Security*, 49, pp. 70–94. doi: 10.1016/j.cose.2014.11.007.

Robson, C. (2011) *Real world research: A resource for users of social research methods in applied settings*. 3rd edn. United Kingdom: Wiley-Blackwell (an imprint of John Wiley and Sons Ltd).

Rodriguez, E. and Edwards, J. (2010) 'People, technology, processes and risk knowledge sharing', *Electronic Journal of Knowledge Management*, 8(1), pp. 139-150.

Rosenberg, J. V. and Schuermann, T. (2006) 'A general approach to integrated risk management with skewed, fat-tailed risks', *Journal of Financial Economics*, 79(3), pp. 569–614. doi: 10.1016/j.jfineco.2005.03.001.

Roslan, A., Yusoff, N.D. and Dahan, H.M. (2017) 'Risk Management Support and Organizational Performance: The Role of Enterprise Risk Management as Mediator', *Journal of International Business, Economics and Entrepreneurship*, 2 (2), pp. 43-48.

Rubin, H. and Rubin, I. (2012) *Qualitative interviewing: the art of hearing data*. 3rd edn. Thousand Oaks: Sage Publication, Inc.

Rubino, M. (2018) 'A Comparison of the Main ERM Frameworks: How Limitations and Weaknesses can be Overcome Implementing IT Governance', *International Journal of Business and Management*, 13(12), p.203.

Rubino, M. and Vitolla, F. (2014) 'Corporate governance and the information system: How a framework for IT governance supports ERM', *Corporate Governance: The international journal of business in society*, 14(3), pp. 320–338. doi: 10.1108/cg-06-2013-0067.

Rudestam, K. E. and Newton, R.R. (2014) *Surviving your Dissertation: A comprehensive guide to content and process*. Sage Publications.

Saeidi, P., Saeidi, S.P., Sofian, S., Saeidi, S.P., Nilashi, M. and Mardani, A. (2018) 'The Impact of Enterprise Risk Management on Competitive Advantage by Moderating Role of Information Technology', *Computer Standards & Interfaces*. 10.1016/j.csi.2018.11.009 (In press).

Salaheddine, A. and Ilias, C. (2017) 'Continuous Improvement of Strategic Alignment Model', *Lecture Notes in Networks and Systems*, pp. 12-20.

Saleh, M. S. and Alfantookh, A. (2011) 'A new comprehensive framework for enterprise information security risk management', *Applied Computing and Informatics*, 9(2), pp. 107–118. doi: 10.1016/j.aci.2011.05.002.

Sapsford, R. and Jupp, V. R. (eds.) (2008) *Data collection and analysis*. 2nd edn. Thousand Oaks, CA: SAGE Publications in association with The Open University.

Sarbanes-Oxley Act (2002) 'Sarbanes-Oxley Act of 2002'. Corporate Responsibility. Public Law 107-204 (USA). Available at: https://www.sec.gov/about/laws/soa2002.pdf (Accessed: 4 October 2016).

Saunders, M. and Lewis, P. (2012) *Doing research in business and management: An essential guide to planning your project*. Essex: United Kingdom: Pearson Education Limited.

Saunders, M. N. K. and Lewis, P. (2018) *Doing research in business and management*. 2nd edn, Harlow: Pearson Education Limited.

Saunders, M. N. K., Lewis, P. and Thornhill, A. (2006) *Research methods for business students*. 4th edn. Harlow, England: Financial Times/Prentice Hall.

Saunders, M. N. K., Lewis, P. and Thornhill, A. (2015) *Research methods for business students*. 7th edn. Harlow, United Kingdom: Pearson Education.

Saunders, M. N. K., Lewis, P., Thornhill, A. and Thorn, A. (2009) *Research methods for business students (5th edition)*. 5th edn. New York: Financial Times Prentice Hall.

Sax, J. and Andersen, T. (2018) 'Making Risk Management Strategic: Integrating Enterprise Risk Management with Strategic Planning', *European Management Review*. doi: 10.1111/emre.12185.

Scarlat, E., Chirita, N. and Bradea, I. A. (2012) 'Indicators and metrics used in the enterprise risk management (ERM)', *Economic Computation and Economic Cybernetics Studies and Research Journal*, 4(46), pp. 5-18.

Schiavone, S., Garg, L., and Summers, K. (2014) 'Ontology of information security in enterprises', 17 (1), pp. 71-86 *The Electronic Journal Information Systems Evaluation*, 17(1).

Schiller, F. and Prpich, G. (2013) 'Learning to organise risk management in organisations: What future for enterprise risk management?', *Journal of Risk Research*, 17(8), pp. 999–1017. doi: 10.1080/13669877.2013.841725.

Schmit, J. T. and Roth, K. (1990) 'Cost effectiveness of risk management practices', *The Journal of Risk and Insurance*, 57(3), p. 455. doi: 10.2307/252842.

Schoonhoven, C. B. (1981) 'Problems with contingency theory: Testing assumptions hidden within the language of contingency "theory"', *Administrative Science Quarterly*, 26(3), p. 349. doi: 10.2307/2392512.

Schroeder, H. (2014) 'An art and science approach to strategic risk management', *Strategic Direction*, 30(4), pp. 28–30. doi: 10.1108/sd-04-2014-0056.

Scott, W.R. (1987) 'The adolescence of institutional theory', *Administrative Science Quarterly*, 32(4), p. 493. doi: 10.2307/2392880.

Seale, C. (2007) *Qualitative research practice*. London: SAGE Publication Ltd.

Sekaran, U. and Bougie, R. (2013) *Research methods for business: A skill-building approach*. 6th edn. West Sussex: United Kingdom: John Wiley and Sons Ltd.

Selamat, M. and Ibrahim, O. (2018) 'The Moderating Effect of Risk Culture in Relationship between Leadership and Enterprise Risk Management Implementation in Malaysia', *Business Management and Strategy*, 9(1), p.244.

Semler S.W. (1997) 'Systematic agreement: a theory of organizational alignment', *Human Resource Development Quarterly*, 8 (1), pp. 23–40.

Servaes, H., Tamayo, A. and Tufano, P. (2009) 'The theory and practice of corporate risk Management', *Journal of Applied Corporate Finance*, 21(4), pp. 60–78. doi: 10.1111/j.1745-6622.2009.00250.x.

Shad, M. K. and Woon, L. F. (2015) 'A conceptual framework for enterprise risk management performance measure through economic value added', *Global Business and Management research: An International Journal*, 7 (2), pp. 1-11.

Shad, M., Lai, F., Fatt, C., Klemeš, J. and Bokhari, A. (2018) 'Integrating sustainability reporting into enterprise risk management and its relationship with business performance: A conceptual framework', *Journal of Cleaner Production*, 208, pp. 415-425.

Shao, Z. (2018) 'Interaction effect of strategic leadership behaviours and organizational culture on IS-Business strategic alignment and Enterprise Systems assimilation'. *International Journal of Information Management*, 44, pp. 96-108.

Silva, J., da Silva, A. and Chan, B. (2019) 'Enterprise Risk Management and Firm Value: Evidence from Brazil', *Emerging Markets Finance and Trade*, 55(3), pp. 687-703.doi: 10.1080/1540496X.2018.1460723.

Silverman, D. (2007) *Interpreting qualitative data*. 3rd edn. London: Sage Publications Ltd.

Silverman, D. (2014) *Interpreting qualitative data*. 5th edn. London, United Kingdom: Sage Publications.

Silvius, A., Smit, J. and Driessen, H. (2010) 'The relationship between organizational culture and the alignment of business and IT'. In proceedings of the *Sixteenth Americas Conference on Information Systems*, Lima, Peru, August 12-15, 2010.

Simeon, R. (2012) *Working in the global economy: How to develop and manage your career across borders*. New York, NY: Routledge.

Singer, P., and Friedman, A. (2014) *Cybersecurity and cyberwar: what everyone needs to know*. New York: Oxford University Press.

Singh, N. A., Gupta, M. P. and Ojha, A. (2014) 'Identifying factors of "organizational information security management"', *Journal of Enterprise Information Management*, 27(5), pp. 644–667. doi: 10.1108/jeim-07-2013-0052.

Siponen, M. and Willison, R. (2009) 'Information security management standards: Problems and solutions', *Information and Management*, 46(5), pp. 267–270. doi: 10.1016/j.im.2008.12.007.

Slagmulder, R. and Devoldere, B. (2018) 'Transforming under deep uncertainty: A strategic perspective on risk management', *Business Horizons*, 61(5), pp. 733-743.

Sledgianowski, D. and Luftman, J. (2005) 'IT-business strategic alignment maturity', *Journal of Cases on Information Technology*, 7(2), pp. 102–120. doi: 10.4018/jcit.2005040107.

Smaczny, T. (2001) 'Is an alignment between business and information technology the appropriate paradigm to manage IT in today's organisations?', *Management Decision*, 39(10), pp. 797–802. doi: 10.1108/eum0000000006521.

Smaga, P. (2014) *The concept of systemic risk*, SRC Special Paper No 5. London: Systemic Risk Centre.

Smit, J. (2014) 'The Relationship between Organizational Culture and Innovation'. In *25th Annual Conference of the International Information Management Association* (IIMA).

Smith, C. W. (1995) 'Corporate risk management', *The Journal of Derivatives*, 2(4), pp. 21–30. doi: 10.3905/jod.1995.407920.

Soomro, Z. A., Shah, M. H. and Ahmed, J. (2016) 'Information security management needs more holistic approach: A literature review', *International Journal of Information Management*, 36(2), pp. 215–225. doi: 10.1016/j.ijinfomgt.2015.11.009.

Stair, R., Reynolds, G. and Chesney, T. (2015) *Principles of business information systems*. 2nd edn. Hampshire: Cengage Learning EMEA.

Standard and Poor's (2008) 'Enterprise risk management: Standard and Poor's to apply enterprise risk analysis to corporate rating'. *Standard and Poor's*, May 2008, pp. 1-7.

Stewart, J. M., Chapple, M. and Gibson, D. (2015) *CISSP (ISC)2 certified information systems security professional official study guide*. United States: John Wiley and Sons.

Stokes, P. and Wall, T. (2014) *Research methods*. London: Palgrave.

Stoll, M. (2015) 'From information security management to enterprise risk management', *Financial Times*. Available at: http://link.springer.com/chapter/10.1007/978-3-319-06773-5_2 (Accessed: 21 January 2015).

Stoll, M. (2014) 'From information security management to enterprise risk management', *Innovations and Advances in Computing, Informatics, Systems*

Sciences, Networking and Engineering, pp. 9–16. doi: 10.1007/978-3-319-06773-5_2.

Strate, L. (1999) 'The varieties of cyberspace: Problems in definition and delimitation', *Western Journal of Communication*, 63(3), pp. 382–412. doi: 10.1080/10570319909374648.

Stulz, R. M. (1996) 'Rethink risk management', *Journal of Applied Corporate Finance*, 9(3), pp. 8–25. doi: 10.1111/j.1745-6622.1996.tb00295.x.

Suddaby, R. (2010) 'Challenges for institutional theory', *Journal of Management Inquiry*, 19(1), pp. 14–20. doi: 10.1177/1056492609347564.

Sutton, R.I. and Staw, B. M. (1995) 'What theory is not', *Administrative Science Quarterly*, 40 (3), p. 371. doi: 10.2307/2393788.

Sweeting, P. (2011) *Financial enterprise risk management*. International Series on Actuarial Science. Cambridge: Cambridge University Press.

Talabis, M. and Martin, J. (2012) *Information security risk assessment toolkit: Practical Assessments through Data Collection and Data Analysis*. Waltham, Mass.: Syngress.

Tarafdar, M. and Qrunfleh, S. (2009) 'IT-business alignment: a two-level analysis', *Information Systems Management*, 26(4), pp. 338–349. doi: 10.1080/10580530903245705.

Tashi, I. and Ghernouti-Hélie, S. (2009) 'Information security management is not only risk management', *2009 Fourth International Conference on Internet Monitoring and Protection*, doi: 10.1109/icimp.2009.31.

Taylor, L. (2014) *Practical enterprise risk management: how to optimize business strategies through managed risk taking*. London: Kogan Page Limited.

Taylor, S. J., Bogdan, R. and DeVault, M. (2016a) *Introduction to qualitative research methods: A guidebook and resource*. 4th edn. Hoboken, NJ, United States: John Wiley and Sons.

Tekathen, M. and Dechow, N. (2013) 'Enterprise risk management and continuous re-alignment in the pursuit of accountability: A German case', *Management Accounting Research*, 24(2), pp. 100–121. doi: 10.1016/j.mar.2013.04.005.

Teo, H. H., Wei, K. K. and Benbasat, I. (2003) 'Predicting Intention to Adopt Interorganizational Linkages: An Institutional Perspective'. *MIS Quarterly*, 27(1), pp. 19-49.

Thakor, A. (2015) '*The Financial Crisis of 2007–2009: Why Did It Happen and What Did We Learn*?', Review of Corporate Finance Studies, 4(2), pp.155-205.

The Institute of Chartered Accountants in England and Wales (1999) *Internal control: guidance for directors on the combined code*. Available at: http://www.ecgi.org/codes/documents/turnbul.pdf (Accessed: 11 July 2016).

The Institute of Risk Management (2012) 'Risk culture under the microscope guidance for boards'. Available at: https://www.theirm.org/media/885907/Risk_Culture_A5_WEB15_Oct_2012.pdf (Accessed: July 2018).

The International Association of Accountants and Technology Consultants (2012) *ICAS (The Institute of Chartered Accountant of Scotland) information security framework*. Available at: http://www.iaaitc.org/LinkClick.aspx?fileticket=OvoJba6OgYg%3D&tabid=205 (Accessed: 8 March 2016).

Thomas, D. and Hodges, I. (2010) *Designing and planning your research project: Core Skills for Social and Health Research*. London: Sage.

Thomas, G. (2017) *How to do your research project: a guide for students*. 3rd edn. London: Sage Publications Ltd.

Thomson Reuters (2015) 'Practical guidance: seven steps for effective enterprise risk management'. Available at: https://web.actuaries.ie/sites/default/files/erm-resources/233_Seven_Steps_to_Enterprise_Risk_Management.pdf (Accesses: 9 August 2016).

Thomson Reuters Accelus (2014) *Cybercrime: the fast-moving menace: a special report* Available at: http://accelus.thomsonreuters.com/sites/default/files/GRC01950.pdf (Accessed: 8 April 2015).

Tilman, L. M. (2001) 'Risk management revolution: The morning after',*The Journal of Risk Finance*, 2(2), pp. 56–60. doi: 10.1108/eb043462.

Tornatzky, L. G., Fleischer, M., and Chakrabarti, A. K. (1990) *The processes of technological innovation*. Lexington, Mass: Lexington Books.

Tosi, H.L. and Slocum. J. W. (1984) 'Contingency theory: Some suggested directions', *Journal of Management*, 10(1), pp. 9–26. doi: 10.1177/014920638401000103.

Tower Watson (2010) 'Embedding ERM: a process of evolution'. Available at: https://www.towerswatson.com/DownloadMedia.aspx?media=%7B48826C34-F2DF-4141-8D77-9C5132657A85%7D (Accessed: 10 August 2016).

Tower Watson (2014) 'The rise of ERM as a strategic partner, eight biennial global enterprise risk management survey'. Available at: https://www.towerswatson.com/en/Insights/IC-Types/Survey-Research-Results/2015/06/report-the-rise-of-erm-as-a-strategic-partner?webSyncID=671e4077-7632-a8e5-a61c-246961146a5d&sessionGUID=9271e4e3-d78b-0571-0cd9-b3d5c6b78bd1 (Accessed: 9 August 2016).

Tracy, S. J. (2012) *Qualitative research methods: Collecting evidence, crafting analysis, communicating impact*. United Kingdom: Wiley-Blackwell (an imprint of John Wiley and Sons Ltd).

Tricker, B. (2015) *Corporate governance: principles, policies, and practices*.3rd edn. Oxford: Oxford University Press.

Turban, E. and Volonino, L. (2010) *Information technology for management: Transforming organizations in the digital economy*. 7th edn. Hoboken: John Wiley and Sons.

Tyagi, C.R. (2014) *Understanding Cyber warfare and its implications for Indian armed forces*. United States: Vij Books India.

UK Cabinet Office (2009) 'Cyber security strategy of the United Kingdom: safety, security and resilience in cyber space'. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf (Accessed: 10 October 2016).

UK Cabinet Office (2011) 'The UK cybersecurity strategy: protecting and promoting the UK in a digital world'. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf (Accessed: 27 April 2015).

Legislation.gov.uk (1998) UK Data Protection Act (1998) Available at: http://www.legislation.gov.uk/ukpga/1998/29/contents (Accessed: 1 December 2016).

UK London Chamber of Commerce and Industry (2014) 'Cyber secure: making London business safe against online crime'. Available at: http://www.londonchamber.co.uk/DocImages/12773.pdf (Accessed: 26 January 2015).

USA (2010) 'Dodd-Frank Wall Street Act'. Available at: https://www.sec.gov/about/laws/wallstreetreform-cpa.pdf (Accessed: 20 September 2016).

USA Department of Defense (2016) 'Dictionary of military and associated terms'. Available at: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (Accessed: 10 October 2016).

USA Department of Financial Services, (2014) 'Report on cyber security in the banking sector, New York State, USA.' Available at: http://www.dfs.ny.gov/about/press2014/pr140505_cyber_security.pdf (Accessed: 11 March 2015).

USA Department of Homeland Security (2002) 'Federal Information Security Management Act of 2002 (FISMA)'. Available at: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf (Accessed: 21 May 2015).

USA Department of Homeland Security (2011) 'Enabling distributed security in cyberspace'. Available at: https://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf (Accessed: 10 October 2016).

USA Department of Treasury (2015) 'Annual report, Financial Stability Oversight Council'. Available at: http://www.treasury.gov/initiatives/fsoc/studies-reports/Documents/2015%20FSOC%20Annual%20Report.pdf (Accessed: 25 June 2015).

USA Department of Treasury, Office of the Comptroller of Currency (2014) 'OCC guidelines establishing heightened standards for certain large insured national banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of Regulations'. Available at: http://www.occ.gov/news-issuances/news-releases/2014/nr-occ-2014-117a.pdf (Accessed: 22 September 2015).

USA New York State Department of Financial Services (2017), 'Cybersecurity requirements for financial services companies', 23 NYCRR 500. Available at: http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf (Accessed: 20 January 2017).

USA Office of Management and Budget (2015) 'Federal information security management act'. Available at: https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf (Accessed: 6 May 2016).

Vaismoradi, M., Turunen, H. and Bondas, T. (2013) 'Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study', *Nursing & Health Sciences*, 15(3), pp. 398-405.

Van de Ven, A.H., Ganco, M. and Hinings, C.R. (2013) 'Returning to the frontier of contingency theory of organizational and institutional designs', *The Academy of Management Annals*, 7(1), pp. 393–440. doi: 10.1080/19416520.2013.774981.

Venkatraman, N., Henderson, J. C. and Oldach, S. (1993) 'Continuous strategic alignment: Exploiting information technology capabilities for competitive success', *European Management Journal*, 11(2), pp. 139–149. doi: 10.1016/0263-2373(93)90037-i.

Verbano, C. and Venturini, K. (2011) 'Development paths of risk management: Approaches, methods and fields of application', *Journal of Risk Research*, 14(5), pp. 519–550. doi: 10.1080/13669877.2010.541562.

Verizon (2015) 'Data breach investigations report'. Available at: http://www.verizonenterprise.com/DBIR/2015/ (Accessed: 21 May 2015).

Verizon (2016) 2016 'Data Breach Investigations Report'. Available at: https://regmedia.co.uk/2016/05/12/dbir_2016.pdf (Accessed: 14 December 2018).

Verizon (2017) 2017 'Data Breach Investigations Report'. Available at: https://www.knowbe4.com/hubfs/rp_DBIR_2017_Report_execsummary_en_xg.pdf (Accessed: 11 December 2018).

Verizon (2018) '2018 Data breach investigations report'. Available at: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf (Accessed: 1 December 2018).

Viscelli, T. R., Hermanson, D. R. and Beasley, M.S. (2017) 'The integration of ERM and strategy: implications for corporate governance', *American Accounting Association*, 31 (2), pp. 69-82. doi: 10.2308/acch-51692.

Volberda, H. W., van der Weerdt, N., Verwaal, E., Stienstra, M. and Verdu, A. J. (2012) 'Contingency fit, institutional fit, and firm performance: A Metafit approach to

Organization–Environment relationships', *Organization Science*, 23(4), pp. 1040–1054. doi: 10.1287/orsc.1110.0687.

Volk, S. and Zerfass, A. (2018) 'Alignment: Explicating a Key Concept in Strategic Communication', *International Journal of Strategic Communication*, 12(4), pp.433-451.

Von Solms, B. and Von Solms, R. (2004) 'The 10 deadly sins of information security management', *Computers and Security*, 23(5), pp. 371–376. doi: 10.1016/j.cose.2004.05.002.

Von Solms, B. and Von Solms, R. (2018) 'Cyber security and information security – what goes where?' *Information and Computer Security*. DOI: https://doi.org/10.1108/ICS-04-2017-0025.

Von Solms, R. and Van Niekerk, J. (2013) 'From information security to cyber security', *Computers and Security*, 38, pp. 97–102. doi: 10.1016/j.cose.2013.04.004.

Wakefield A. (2014) *Corporate Security and Enterprise Risk Management*. In: Walby K., Lippert R.K. (eds) Corporate Security in the 21st Century. Crime Prevention and Security Management. doi 10.1057/9781137346070_13. London: Palgrave Macmillan.

Walsh, J.P., Meyer, A.D. and Schoonhoven, C. B. (2006) 'A future for organization theory: Living in and living with changing organizations', *Organization Science*, 17(5), pp. 657–671. doi: 10.1287/orsc.1060.0215.

Walter, J., Kellermanns, F. W., Floyd, S. W., Veiga, J. F. and Matherne, C. (2013) 'Strategic alignment: a missing link in the relationship between strategic consensus and organizational performance', *Strategic Organization*, 11(3), pp. 304–328. doi: 10.1177/1476127013481155.

Ward, S. (2003) 'Approaches to integrated risk management: A multi-dimensional framework', *Risk Management*, 5(4), pp. 7–23. doi: 10.1057/palgrave.rm.8240161.

Webb, J., Ahmad, A., Maynard, S. B. and Shanks, G. (2014b) 'A situation awareness model for information security risk management', *Computers and Security*, 44, pp. 1–15. doi: 10.1016/j.cose.2014.04.005.

Webb, J., Maynard, S., Ahmad, A. and Shanks, G. (2014a) 'Information security risk management: an intelligence-driven approach', *Australasian Journal of Information Systems*, 18(3), pp. 391-404. doi: 10.3127/ajis.v18i3.1096.

Websense Security Labs (2015) '2015 Industry drill-down report, financial services'. Available at: http://www.websense.com/assets/reports/report-2015-industry-drill-down-finance-en.pdf?mkt_tok=3RkMMJWWfF9wsRokv6vAde%2FhmjTEU5z14uopXKawhokz2EFye%2BLIHETpodcMRcNjPa%2BTFAwTG5toziV8R7DEJM1u0dMQWxHq (Accessed: 24 June 2015).

Weill, P. and Olson, M. H. (1989) 'An assessment of the contingency theory of management information systems', *Journal of Management Information Systems*, 6(1), pp. 59–86. doi: 10.1080/07421222.1989.11517849.

Whitman, A. F. (2015) 'Is ERM legally required? Yes for financial and governmental institutions, no for private enterprises', *Risk Management and Insurance Review*, 18(2), pp. 161–197. doi: 10.1111/rmir.12045.

Williamson, G. and Whittaker, A. (2017) *Succeeding in literature reviews and research project plans for nursing students*. Learning Matters.

Womer, N. K., Bougnol, M., Dula, J. H. and Retzlaff-Roberts, D. (2006) 'Benefit-cost analysis using data envelopment analysis', *Annals of Operations Research*, 145(1), pp. 229–250. doi: 10.1007/s10479-006-0036-5.

World Business Council for Sustainable Development (2017) 'Sustainability and enterprise risk management: the first step towards integration'. Available at: https://www.wbcsd.org/contentwbc/download/2548/31131 (Accessed: 20 November 2018).

World Economic Forum (2017) 'Advancing cyber resilience principles and tools for boards'. Available at: https://www.google.co.uk/search?q=Advancing+Cyber+Resilience+Principles+and+Tools+for+Boards&oq=Advancing+Cyber+Resilience+Principles+and+Tools+for+Boards&aqs=chrome..69i57.12321j0j7&sourceid=chrome&ie=UTF-8# (Accessed: 17 March 2018).

World Economic Forum and Deloitte (2015) 'Partnering for cyber resilience: towards the quantification of cyber threats'. Available at: http://www2.deloitte.com/content/dam/Deloitte/it/Documents/risk/deloitte-nl-cyber-risk-report-2015.pdf (Accessed: 29 May 2015).

Wu, D. D., Chen, S.-H. and Olson, D. L. (2014) 'Business intelligence in risk management: Some recent progresses', *Information Sciences*, 256, pp. 1–7. doi: 10.1016/j.ins.2013.10.008.

Wu, S.P., Straub, D. W., Liang, T. (2015) 'How Information Technology Governance Mechanisms and Strategic Alignment Influence Organizational Performance: Insights from a Matched Survey of Business and IT Managers', *MIS Quarterly*, vol. 39, no. 2, pp. 497-518.

Yang, S.., Ishtiaq, M. and Anwar, M. (2018) 'Enterprise Risk Management Practices and Firm Performance, the Mediating Role of Competitive Advantage and the Moderating Role of Financial Literacy', *Journal of Risk and Financial Management*, 11(35), pp. 1-17.

Yaraghi, N. and Langhe, R. G. (2011) 'Critical success factors for risk management systems', *Journal of Risk Research*, 14(5), pp. 551–581. doi: 10.1080/13669877.2010.547253.

Yarifard, R., Taheri, M. and Zafarzadeh, S., 2016. *Business-IT Strategic Alignment Focused on Social and Technical Dimensions*, Journal of Money and Economy, 11(1), pp. 87-118.

Yilmaz, A.K. and Flouris, T. (2010) 'Managing corporate sustainability: Risk management process-based perspective', *African journal of business management*, 4(2), pp. 162-171.

Youngberg, B. (2010) *Principles of risk management and patient safety*. Sudbury, MA: Jones and Bartlett Publishers.

Zéghal, D. and El Aoun, M. (2016) 'Enterprise risk management in the U.S. banking sector following the financial crisis', *Modern Economy*, 7(4), pp. 494–513. doi: 10.4236/me.2016.74055.

Zeithaml, V.A., Varadarajan, P.R. and Zeithaml, C. P. (1988) 'The contingency approach: Its foundations and relevance to theory building and research in marketing', *European Journal of Marketing*, 22(7), pp. 37–64. doi: 10.1108/eum0000000005291.

Zickmund, W. G, Babin, B. J., Carr, J. C and Griffin, M. (2013) *Business research methods*. 9th edn. USA: Cengage Learning.

Zickmund, W. G. (2012) *Business research methods*. 9th edn. Mason: South -Western, Cengage Learning.

Zucker, L. (1987) 'Institutional theories of organization', *Annual Review of Sociology*, 13(1), pp. 443–464. doi: 10.1146/annurev.soc.13.1.443.

Appendix A: Cross-reference table of key research terms and phrases

RM	Risk governance; silo risk management; traditional RM; siloed governance of risks.
ERM	Enterprise risk management; holistic risk governance; organisational risk governance; Governance, Risk Management and Compliance.
CsM	Cyber-security; cyber security management; cybersecurity risk management; information security governance; computer security; IT security; electronic security; digital security; internet security; IT Risk Management; Data Security; Information Security Management Systems; Cyber Threat Management; Cybersecurity Risk Management; Cybersecurity Management.
Alignment	Integration; unification; non-alignment; misalignment; fit; co-aligned; linked; congruent; contingent; matched; harmony; fusion; synchronization; integration; synergy; convergence.

Appendix B: Participant Information

PARTICIPANT INFORMATION SHEET FOR INTERVIEWS

Title of Research: Aligning Cybersecurity Management with Enterprise Risk Management in the Financial Industry

Researcher: Alina Andronache, PhD Student at Brunel Business School, Brunel University London

Purpose: This research aims to explore the related area to risk governance as Cybersecurity Management and Enterprise Risk Management with the purpose to understand risk attention, decisions, experiences, behaviours and attitude towards risk oversight. This research investigates possible methods for facilitating a more enhanced strategic approach to respond to the extended exposure to wide-ranging risks and cyber risks. More specifically, how financial organisations manage their exposure to risks and explore what is required to improve risk governance.

Participant selection

You are being asked to participate in this study because you have been identified as an expert within the financial industry. You have been chosen because your valuable expertise within organisational risk governance can bring benefits to others. The decision to take part in this research is voluntary and a withdrawal at any given point is possible, without justification. If you have decided to participate in this research, you will be required to sign a consent form. The estimated number of participants for interviews is around 30 interviewees across the globe.

Confidentiality: All your responses are confidential and anonymous so please be assured that under no circumstances will any of the collected or retained information contain information about your identity. Research records will be kept in a locked file and all electronic information will be coded and secured using a password protected file. We will not include any information in any report that would render it possible to identify you. Any recordings taken during the interview will be kept secret (codified and anonymised) and will be kept in a secure place in accordance to Data Protection Act.

Withdrawal: You have the right not to answer any single question, as well as to withdraw completely from the interview at any point during the process. Additionally, you have the right to request the interviewer not use any of the interview material.

Description of interview procedure: If you agree to participate, a typical interview length is approximately about 30-40 minutes. However, it can go up to a maximum of 1 hour, depending on how much information you decide to communicate. The interview will be recorded but if required this method can be changed at your request and replaced with note taking during the interview.

What is expected from an interview?

The interview is expected to take place at a time and location convenient for you. During the interview, I will be the only person to interview you and the format of question are open-ended (semi-

structured interview), so you can openly answer question as you wish. The expected number of questions is 30 and are particularly related to risk governance. In case you may find some questions uncomfortable, you are not obliged to answers to questions. With your permission, the interview will be audio recorded in order to capture accurately what has been said.

Description of procedure after interview
The audio recording will be transcribed and labelled with a code number to assure anonymity. If requested, a copy of the transcribed interview can be provided. Moreover, if you later wish to make changes on your statements, to remove specific information or you want more information on how your identity is hidden, your request will be fulfilled. A report of findings will be available to all participants a later date.

Indirect benefits: Even though there is no financial gain involved in taking part in this research, the potential indirect benefits of your involvement contribute towards recommending to the financial industry how risk governance should be dealt with based on findings from various organisations.

Report concerns
While I do not anticipate any problems during the interview, if there are any problems or concerns that occur as a result of your participation, you can communicate them directly to me or should you require any further information, you can alternatively contact my supervisor (where relevant). Complaints, on the other hand, should be directed, in the first instance, to the relevant Research Ethics Committee of Brunel University London.

Contact details are as follows:

- Researcher: Alina Andronache, PhD Student at Brunel Business School, Brunel University London, contact email: Alina.Andronache@brunel.ac.uk, contact phone number: [removed]
- Faculty advisor: Dr Abraham Althonayan, Brunel Business School, Brunel University London, email contact: Abraham.Althonayan@brunel.ac.uk
- Faculty ethics committee: College of Business, Arts and Social Sciences: Cbass-ethics@brunel.ac.uk

Many thanks for accepting the invitation to take part in this research project and thank you for reading this Participant Information Sheet for Interviews.

This research will be undertaken in accordance with the Brunel University London Ethical Framework, Brunel University London Code of Research Ethics, and Brunel University London Research Integrity Code. ***Ethics approval has been obtained from the relevant Research Ethics Committee.***

Appendix C: Consent Form

CONSENT FORM OF PARTICIPATION IN A RESEARCH STUDY

Title of Research: Aligning Cybersecurity Management with Enterprise Risk Management in the Financial Industry

Researcher: Alina Andronache, PhD Student at Brunel Business School, Brunel University London, contact email: Alina.Andronache@brunel.ac.uk, contact phone number: [removed].

Consent statements	**Please initial box** Yes	No
1. I hereby confirm that I have read and understand the participation information sheet for the above-mentioned research and have had the opportunity to ask questions.	☐	☐
2. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving reason.	☐	☐
3. I understand that my participation involves one interview session. Only in some exceptional cases, the Researcher might contact me for further details or clarifications, but in such case, I can decline such request without any obligation.	☐	☐
4. I understand that my confidentially will be accomplished by name anonymization, thus the Researcher assumes the responsibility to assure confidentiality and anonymization both my name and my organisation.	☐	☐
5. At this phase, I am aware that if there are any problems or questions, I can contact the Researcher, his/her faculty advisor or the faculty ethics committee should I consider it necessary.	☐	☐
6. I agree to the interview consultation being audio recorded	☐	☐
7. I grant my permission for anonymised quotes to be used in publications.	☐	☐
8. A copy of this document has been given to me and I have read the above, and I am knowingly confirming my interest for participating voluntarily to the interview. I confirm that I read and understood the information provided to me (pre-interview).	☐	☐
9. I agree to take part in the above study.	☐	☐

A verbal agreement can replace the signature on this form if preferable. Your recorded verbal agreement indicates that you have decided to volunteer as a research participant for this study, and that you have read and understood the information provided above.

Appendix D: Interview Questions

INTERVIEW QUESTIONS

Title of Research: Aligning Cybersecurity Management with Enterprise Risk Management in the Financial Industry

Researcher: Alina Andronache, PhD Student at Brunel Business School, Brunel University London

Organisation profile

1. Please specify in which geographical region your current organisation primarily resides (headquarter).

- Please specify……...

2. In which sector within the financial industry does your organisation primarily operates?

- Depository institution (e.g. retail bank, commercial bank, private bank, savings bank, building society, credit union)
- Insurance and pension fund institution (e.g. insurance organisations)
- Brokers and investments institution (e.g. asset management, investments bank, corporate finance, mutual funds, hedge funds, mortgage brokers, clearing houses, finance organisation, investment organisation)
- Other (please specify)
  ……..

3. Please specify the size of your organisation in terms of employee numbers.

- between 100-500
- between 501-1,000
- between 1,001-2,000
- between 2,001-3,000
- between 3,001-4,000
- between 4,001-5,000
- above 5,001 but below 10,000
- above 10,000
- Other (please specify)
  ……..

Interviewee profile

4. What is your position within the organisation?

- Please specify……...

5. On which aspect of risk oversight are you mostly focused?

- Risk assessment/measurement
- Audit
- Compliance

- Education/awareness/training
- Enterprise-wide risk control
- Implementation – operational
- Implementation – strategic
- Risk control
- Other (please specify)……...

6. In terms of years' experience in your current role, how would you define your employment status?

- At least 1 year but fewer than 3 years
- At least 3 years but fewer than 5 years
- At least 5 years but fewer than 10 years
- Other (please specify)……

7. Per total, how many years of experience have you acquired in similar roles related to risk governance?

- At least 1 year but fewer than 3 years
- At least 3 years but fewer than 5 years
- At least 5 years but fewer than 10 years
- Other (please specify)……

8. As a professional, is your current role conditioned by specific industry professional certifications?

- Not required
- Specifically required, the certification(s) name is/are:
  ……
  ……

9. How do you describe your direct experience in terms of your interaction with risk governance within your organisation (your job aims)?

- Please specify ……...

Research focus questions

10. What can you tell me about your organisation's position in terms of preparation against risks?

- Please specify ……

11. In terms of risk level, how would you describe the velocity of risks/attacks encountered by your organisation?

- Low-almost inexistent
- Medium, within acceptable tolerance
- High, exceeds the tolerance
- At critical capacity, above expectations
- Other (please specify)
  ……

12. What is the name of the managerial component/department of your organisation carries a duty of care/responsibility regarding enterprise risks?

- Department Managers

- Enterprise Risk Management
- Executive Boards
- Governance Risk Management and Compliance (GRC)
- Resilience Management
- Risk Management
- Steering Committee
- Other (please specify)

  ……
  ……

13. How would you describe the overall status of risk governance maturity (e.g. Risk Management, Enterprise Risk Management) within your organisation for protecting the organisation against risks? (on a scale of 1-5, 1 representing the low value).

- Robust (5)
- Mature risk governance embedded at enterprise level (4)
- Evolved risk governance but partially implemented across units/departments (3)
- Developed but not yet applied enterprise-wide (2)
- Very immature - at its early stages of preparation (1)
- Other (please specify)

  ……
  ……

14. In general, how would you describe the role of organisation risk governance (e.g. Risk Management (RM) /Enterprise Risk Management (ERM))?

- Common governance tool
- Competitive advantages advocate
- Compliance requirement
- Cross-domain risk knowledge
- Effective strategic prioritization (operational efficiency) tool
- Supportive business strategy and objectives alignment tool
- Value creation tool
- Risk control function
- Other (please specify)

  ……
  ……

15. In your opinion, what are the three main determinants/drivers (internal and external) on which an organisation decides to implement a risk governance (RM/ERM)?

- Competition
- Customers' expectations
- Consultancy organisations
- Insurance prerequisites
- Laws
- Organisation's own initiative
- Organisational risk oversight culture
- Organizational internal norms
- Post-financial crisis lessons
- Practitioners' recommendations
- Regulatory requirements
- Shareholders' requirements
- Standards/Frameworks-driven

- Other (please specify)
  ……
  ……

16. From your experience, what are the main inhibitors (internal and external) that might impede the successful implementation of RM/ERM?

- Please specify

  ……

17. Moving from enterprise protection to cyber-related threats, what is the name of the managerial component/department of your organisation that carries a duty of care/responsibility regarding the protection of your organisation against cyber risks?

- Please specify

  ……

18. In your opinion, what are the main determinants that determine the implementation of cyber risk oversight? (Please tick as many as you deem appropriate).

- Competition
- Consultancy organisations
- Insurance prerequisites
- Laws
- Organisation's own initiative
- Organisational risk oversight culture
- Organizational internal norms
- Practitioners' recommendations
- Regulatory pressure
- Shareholders' requirements
- Standards/Frameworks-driven
- Technology advancement
- The velocity and complexity of cyber threats
- Other (please specify)
  ……
  ……

19. From your experience, what are the main inhibitors (internal and external) that might impede the good practice of cyber risk governance?

- Communication
- Cost of compliance
- Cost of implementation
- Lack of awareness
- Lack of collaboration
- Lack of enterprise-wide risk culture
- Lack of employees' competencies
- Late risk identification.
- Misalignment to organizational goals
- Silo approaches
- Silo strategies (double effort, cost & time consuming), difficulties in integration
- Strategic directions
- Weak support of management (organizational dysfunctions)

- Other (please specify)
  ……
  ……

20. Referring to departments/units and the practical side of risks, how would an employee (any department) encountering a cyber incident handle such situation? What should do?

- Please specify
  ……
  ……
  ……

21. Considering the broad spectrum of risks and cyber threats, which are the three most unwanted effects of poor risk oversight within your organisation? (Please tick as many as you deem appropriate)

- Biased decisions
- Business interruption
- Financial loss
- Ineffective loss prevention
- Loss of customer trust
- Loss of resilience
- Loss of sensitive data
- Post-incident premium insurance chargers
- Regulatory consequences/fines/prejudices
- Reputational loss
- Unjustified investments on risk oversight
- Other (please specify)
  ……
  ……

22. In terms of security strategy, does your organisation rely on a specific industry framework, security management programme or standards in dealing with its exposure to wide-ranging protection and cyber risks?

- If applicable, please specify
  ……
  ……

23. Regarding implementation benefits of risk oversight, on which return on investment (ROI) does your organisation focus more specifically?

- Competitive advantage
- Compliance
- Organisational effectiveness
- Resilience
- Sustainability
- Other (please specify)
  ……

24. In your opinion, what are the executive board expectations regarding your department in terms of enterprise risks and cyber risk governance?

- Please specify
  ……
  ……

25. In your organisation, how well do departments communicate with others in the case of an incident if more types of risks (enterprise and cyber) are involved? (on a scale of 1-5, 1 representing the low value).

- Very effective (5)
- Somewhat effective (4)
- Neutral (3)
- Somewhat ineffective (2)
- Very ineffective (1)

26. Based on your personal observations and experiences, do you think that it is a good approach to manage each risk or incident at departmental level rather than at an enterprise level?

- Please specify
  ……
  ……

27. How does your organisation deal with all type of risks within each department?

- Each department deals with its own risks
- Risks are treated holistically
- Risk are treated through both silo and enterprise-wide approach
- Other (please specify)
  ……..

28. Do you think the implementation of a unified strategy for cyber and RM governance would have a positive or negative effect on an organisation?

- Very positive
- Somewhat positive
- Neutral
- Somewhat negative
- Very negative

29. Does your organisation have a unified mechanism by which your organisation identifies, assesses and mitigates both cyber and enterprise risks across your organisation? Could you tell me more about it?

- Please specify
  ……
  ……

30. What is your understanding about strategic alignment; for example, what is the purpose, who is responsible, how can be achieved, etc.?

- Please specify
  ……
  ……

31. What do you think are the benefits of alignment regarding risk governance and organisation objective achievement?

- Unified management

- Unified departmental communication
- Unified risk response mechanism
- Avoidance of duplication
- Risk mitigation optimisation
- Strategy alignment
- Informed prioritisation of decisions
- Unified resilience
- Enterprise-wide risk measurement
- Other (please specify) ……..…….

32. In dealing with risk governance, have you considered the alignment of Cybersecurity Management with Enterprise Risk Management?

- Yes
- No
- I don't know
- Other (please specify) ……

33. Do you think that a strategic alignment of Cybersecurity Management with Enterprise Risk Management is a feasible approach in terms of organisational risk governance in the long-term?

- Strongly disagree
- Disagree
- Neither agree nor disagree
- Agree
- Strongly agree
- Other (please specify) ……..……

34. In your opinion, what is the overall status of cybersecurity maturity alignment with ERM within your organisation?

- Mature (fully optimised)
- Somewhat mature, optimised to organisational needs
- Slightly mature, implemented but not fully integrated
- Immature, implementation initiation phase
- Neutral
- Considered but not yet applied
- Not considered
- Other (please specify) ……

35. From your experience, what are the main inhibitors that might impede a strategic alignment of CsM and ERM specifically in the financial industry?

- Overlap of governances
- Employees skills deficiencies
- Inappropriate governance
- Dispersed compliance settings
- Plethora of guidance's/practices
- Silo approach /overlap of functions
- Heightened regulatory expectations
- Unclear policy and risk statements
- Organisational cultural deficiencies
- Uncorrelated theory with applicability
- Inappropriate alignment/low maturity
- Preparedness to overcome deficiencies

- Uncoordinated efforts of staff involved
- Overconfidence in systems and procedures
- Inconsistent regulations (national specific vs. global)
- Other (please specify) ……..

*If the next 2 questions do not apply, please go to the question **38**.*

36. How does your organisation achieve strategic alignment? How it can be established?

- Do not apply
- Applies, please specify

  ……
  ……
  ……

37. If applicable, how does your organisation assess the alignment? Are there any mechanisms in place?

- Please specify

  ……
  ……
  ……

38. Which are most worthwhile risk oversight practices that you would recommend to other managers facing drawbacks in the implementation of ERM and CsM alignment?

- Please specify

  ……
  ……
  ……

39. Lastly, how do you think risk governance within your organisation will (if) change over the next five years? Any predictions/forecasts of future trends?

- Please specify

  ……
  ……
  ……

I have no further questions. Is there anything else you would like to bring up or ask before closing the interview?

- Please specify

  ……
  ……
  ……

Appendix E: Frameworks evaluation form

No.	Task	Derivations identified
1.	Main focus (CsM, ERM, alignment)	
2	Research gap indicated	
2a	How the gap relates to the research problem?	
3	Understanding the external requirements (regulatory, stakeholders) and limitation of internal and external factors	
4	Contrasting the desired state; cost-benefit analysis	
5	How will impact the theory and practice	
6	Main focus (quadrants) Quadrant 1 Adoption Quadrant 2 Implementation Quadrant 3 Maturity assessment Quadrant 4 Assesses compliance	
7	Continuous self-assessment (regulatory, guidelines, standards)	
8	Type of alignment indicated (strategically aligned) • Strategic • Structural • Operational • Social • Cultural	
9	Is alignment of CsM and ERM considered?	
10	Prescriptive/descriptive	
11	Industry specific (financial, others)	
12	Strengths and limitations	
13	Derivates extracted	

Annex F: Correlation of interview questions with research questions, the research framework and the research aims

	Focus / *Research questions*		**Theme One: Respondent and Organisation Profile**	**Research Framework themes addressed in interview questions**	**Research aims**
		Validation	1. Please specify in which geographical region your current organisation primarily resides (headquarter). 2. In which sector within the financial industry does your organisation primarily operates? 3. Please specify the size of your organisation in terms of employee numbers. 4. What is your position within the organisation? 5. On which aspect of risk oversight are you mostly focused? 6. In terms of years' experience in your current role, how would you define your employment status? 7. Per total, how many years of experience have you acquired in similar roles related to risk governance? 8.As a professional, is your current role conditioned by specific industry professional certifications? 9. How do you describe your direct experience in terms of your interaction with risk governance within your organisation (your job aims)?		
Objective 1	1. Why does a strategic alignment of CsM and ERM sustain a financial business in the long-term?	Rationale	**Theme Two: Enterprise Risk Oversight Maturity** Q10. What can you tell me about your organisation's position in terms of preparation against risks? Q11. In terms of risk level, how would you describe the velocity of risks/attacks encountered by your organisation? Q12. What is the name of the managerial component/department of your organisation carries a duty of care/responsibility regarding enterprise risks? Q13. How would you describe the overall status of risk governance maturity (e.g. Risk Management, Enterprise Risk Management) within your organisation for protecting the organisation against risks? (on a scale of 1-5, 1 representing the low value).	**Phase One**: 'baseline expectations' ✓ Baseline expectations-preparation ✓ Cybersecurity Management ✓ Enterprise Risk Management ✓ Strategic alignment/ Interconnectivity and Partnership ✓ Context of alignment (internal and external) ✓ Organisation mission and vision; ✓ Barriers ✓ Benefits • Purpose of alignment • Alignment objectives • Alignment strategy **Phase Two**: 'mandate managerial directions' • Managerial directions-administration • Strategic directions	**1) To investigate the alignment of CsM with ERM within the financial industry.** **2) To develop a framework that assists CsM with ERM alignment within the financial industry, supported by practical guidance for the implementation of the proposed framework.**
Objective 2	2. What are the key issues that impede the alignment process in the financial industry regarding CsM and ERM?	Gap consideration	Q14. In general, how would you describe the role of organisation risk governance (e.g. Risk Management (RM) /Enterprise Risk Management (ERM))? Q15. In your opinion, what are the three main determinants (internal and external) on which an organisation decides to implement a risk governance (RM/ERM)? Q16. From your experience, what are the main inhibitors (internal and external) that might impede the successful implementation of RM/ERM?		
Objective 3	3 How are theory, practice, and regulation direction applied regarding the current alignment of CsM and ERM within the financial industry?	Maturity	**Theme Three: Cyber Risk Oversight Maturity** Q17. Moving from enterprise protection to cyber-related threats, what is the name of the managerial component/department of your organisation that carries a duty of care/responsibility regarding the protection of your organisation against cyber risks? Q18. In your opinion, what are the main determinants that determine the implementation of cyber risk oversight? Q19. From your experience, what are the main inhibitors (internal and external) that might impede the good practice of cyber risk governance? Q20. Referring to departments/units and the practical side of risks, how would an employee (any department) encountering a cyber incident handle such situation? What should do?		

			Q21. Considering the broad spectrum of risks and cyber threats, which are the three most unwanted effects of poor risk oversight within your organisation? Q22. In terms of security strategy, does your organisation rely on a specific framework, security management programme, standards, policies, procedures, guidance or regulatory framework compliance in dealing with its exposure to enterprise and cyber risks? Q23. Regarding implementation benefits of risk oversight, on which return on investment (ROI) does your organisation focus more specifically? Q24. In your opinion, what are the executive board expectations regarding your department in terms of enterprise risks and cyber risk governance?	• Context of alignment **Phase Three**: 'establishment of strategic directions' • Strategic alignment • Structural alignment **Phase Four**: 'implement managerial directions' • risk profile • risk practices **Phase Five**: 'Monitoring and reviewing practices' - improvement • Monitor, measure, plan, re-align • Barriers and limitations of CsM with ERM alignment • Benefits of alignment assessment	
Objective 4	4. What effects have the implementation of the new framework?	Benefits and Limitations	**Theme Four: Strategic Alignment** Q25. In your organisation, how well do departments communicate with others in the case of an incident if both types of risks (enterprise and cyber) are involved? (on a scale of 1-5, 1 representing the low value). Q26. Based on your personal observations and experiences, do you think that it is a good approach to manage each risk or incident at departmental level rather than at an enterprise level? Q27. How does your organisation deal with all type of risks within each department? Q28. Do you think the implementation of a unified strategy for cyber and RM governance would have a positive or negative effect on an organisation? Q29. Does your organisation have a unified mechanism by which your organisation identifies, assesses and mitigates both cyber and enterprise risks across your organisation? Could you tell me more about it? Q30. What is your understanding about strategic alignment; for example, what is the purpose, who is responsible, how can be achieved, etc.? Q31. What do you think are the benefits of alignment regarding risk governance and organisation objective achievement? Q32. In dealing with risk governance, have you considered the alignment of Cybersecurity Management with Enterprise Risk Management? Q33. Do you think that a strategic alignment of Cybersecurity Management with Enterprise Risk Management is a feasible approach in terms of organisational risk governance in the long-term? Q34. In your opinion, what is the overall status of cybersecurity maturity alignment with ERM within your organisation? Q35. From your experience, what are the main inhibitors that might impede a strategic alignment of CsM and ERM specifically in the financial industry? Q36. How does your organisation achieve strategic alignment? How it can be established? Q37. If applicable, how does your organisation assess the alignment? Are there any mechanisms in place? Q38. Which are most worthwhile risk oversight practices that you would recommend to other managers facing drawbacks in the implementation of ERM and CsM alignment? Q39. Lastly, how do you think risk governance within your organisation will (if) change over the next five years? Any predictions/forecast of future trends?		