PHD IN RISK MANAGEMENT

Integrating Project Risk Management into Enterprise Risk Management

A THESIS SUBMITTED FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

NAIF ALDWAIS

Newcastle University Business School

December 20, 2024

Copyright statement and dedication

I confirm that the work presented in this thesis is entirely my own and I have not been registered for any other degree or qualification at any institution.

Abstract

Project Risk Management (PRM) with its long-standing presence in both the literature and the project profession is a formal methodology for managing risks at the project level and focuses primarily on project objectives. In contrast, Enterprise Risk Management (ERM) deals with risks at the organisational level, encompassing strategic, operational, reporting, and compliance objectives (Coso, 2004). The disparities in objectives and scope pose difficulties in integrating these two systems.

PRM empowers project managers to make decisions within their project's the scope of an individual project, while ERM's requirement for interdisciplinary expertise enables a holistic view of risks across the total projects, departments, and functions, fostering a comprehensive understanding that is unattainable when risks are managed in isolation. The evolution of risk perception, from an objective quantitative hazard to a subjective qualitative assessment influenced by cultural and human values, is evident in the risk management literature. While a positivist perspective dominates PRM, rooted in mathematical predictability, ERM acknowledges the need for subjectivity in managing uncertainties arising from a broader internal and external environment.

Nevertheless, integrating PRM into ERM can yield benefits by enhancing risk awareness and fostering strong collaboration among projects throughout the organisation. This integration facilitates the incorporation of risk considerations into broader business decision-making processes, aligning them with organisational objectives (Agarwal & Virine, 2019). Additionally, ERM contributes to improving PRM by enhancing the communication of project risk information, aiding management in making better-informed decisions and handling project risks more effectively (Zhao et al., 2015). Consequently, this research advocates for the incorporation of Complex Adaptive System (CAS) theory into these organisational risk management systems to accommodate the two distinct perspectives on risk, facilitating their integration to support decision making processes.

Stemming from a critical realism mindset, a qualitative methodological approach is adopted, employing three case studies in Saudi and British companies within the oil, petrochemical, and hospitality industries. Semi-structured interviews, supported by documentary analysis

form the basis of data collection. A deductive analysis, guided by the Institute for Risk Management's (IRM) successful risk culture criteria, was used to examine the risk cultures of the three organisations. Additionally, an inductive exploration of their risk governance structures was conducted to understand and explain their roles in integrating (PRM) and (ERM).

The findings reveal that Key cultural attributes such as openness, compliance, continuous learning, and adaptability were crucial for fostering a unified approach to risk management aiding the integration of PRM and ERM. Similarly, adaptable risk governance structures that consider their environment’s needs played an important role in shaping the risk governance structures that facilitate the integration. In contrast, siloed and closed risk cultures coupled with rigid governance structures hindered the integration of the two systems. Organisations with adaptive risk governance structures and open risk cultures showed alignment with their values, which acknowledged and responded to the complexities of their internal and external environments.

Acknowledgments

First and foremost, I would like to extend my heartfelt gratitude to my wife, Sarah, for standing by me throughout this long journey. Her unlimited support, love, and encouragement have been my greatest source of strength. To my two young boys, Khalid and Tamim, thank you for your patience I know that this thesis demanded time that should have been spent with you. I am also speechless to express my gratitude to my parents, without their support, completing this thesis would not have been possible.

I would also like to express my deepest appreciation to my supervisors, Karen Elliott and Rebecca Casey, for their invaluable guidance, patience, and encouragement. Their expertise, insightful advice, and constant support have been instrumental in shaping this thesis and pushing me to achieve my best.

My sincere thanks go to Newcastle University for providing the resources and a supportive environment that enabled me to carry out this research. I am especially grateful to my colleague and friend, Shaker Al Kaabneh, for his insightful feedback and encouragement as we went through this challenging journey together.

This thesis is dedicated to all who have supported and inspired me throughout this endeavour.

List of Tables

List of Figures

Table of Contents

Chapter One: Introduction

1.1 Background

Risk management is a core part of corporate governance (Jiang et al., 2023). In recent years the concept of risk management has advanced the government and private sector agendas. Some governance reforms such as the Basell II Capital Accord, the combined code in the UK (2003) (Woods, 2009), and the Corporate Governance Regulations (CGR) in Saudi Arabia (2006) have aimed to reduce the risk of further significant corporate failures by stricter regulation of internal control systems. Corporate governance is defined as "the systems by which companies are directed and controlled. Board of directors are responsible for the governance of their companies. The shareholders' roles in governance are to appoint the directors and the auditors and to satisfy themselves that an appropriate governance structure is in place" (FRC, 2024, p.3).

Since corporate governance regulates risk management guiding risk governance structure, which is essential in this thesis in relation to the ERM and PRM governance structure, the following two sections review the corporate governance regulations in both Saudi Arabia and the UK as the selected case studies are based on these two countries.

1.1.1 Overview of Corporate Governance and Risk Management in Saudi Arabia

Over the past two decades, Saudi Arabia has undergone significant political, social, and economic changes, which have reformed corporate governance as part of broader economic restructuring attempts (Mahsoon, 2023). Prior to 2006, corporate governance regulations were almost absent, with little acknowledgment of their importance in fostering transparency and accountability (Ali, 2019). International institutions such as the World Bank and OECD played an important role in encouraging the adoption of governance reforms to modernise the Saudi corporate governance codes. This led to the establishment of the Capital Market Authority (CMA) in 2003, which was seen as a turning point in corporate governance regulations in the country (Mahsoon, 2023).

However, the Saudi stock market crisis in 2006 was a turning point in the Kingdom's economic and political history, exposing critical weaknesses in corporate governance. Several causes for the crash were identified including insufficient investor knowledge about securities, and

limited financing options from financial institutions (Ali, 2019). Furthermore, the lack of transparency and disclosure practices among listed companies, banks, and relevant government agencies worsened the crisis. Accordingly, urgent corporate governance reforms were needed to restore confidence and protect investors' values.

In response, the CMA introduced the Corporate Governance Regulations (CGR) in 2006, which provides governance standards for joint-stock companies listed on the Saudi Stock Exchange Market (TADAWUL), highlighting the board of directors' role in managing and mitigating risks. The CGR mandated boards to establish and maintain robust internal control systems, predict potential risks, and disclose these transparently to stakeholders (Aleisa, 2017; CMA, 2006).

Subsequent amendments in 2009, 2010, and 2017 further enhanced the framework, aligning Saudi governance practices with global standards. Unlike the UK's Corporate Governance Code, which operates on a “comply or explain” basis, compliance with Saudi Arabia's Corporate Governance Regulations (CGR) is compulsory for all listed companies. The CGR mandates the board to create a committee named: “Risk Management Committee” where the chairman and the majority of the members should be non-executive directors.

The UK’s approach provides flexibility, allowing companies to tailor their governance practices. The background and framework of the UK’s Corporate Governance Code are discussed next.

1.1.2 Overview of Corporate Governance in the UK: Flexibility and Principles driven Governance

The UK’s corporate governance code was first published in 1992. The Code does not establish a fixed set of rules; instead, it provides flexibility through applying principles and through “comply or explain” reporting against provisions (Financial Reporting Council (FRC,2024))[1]. An example of a risk management principle according to the code is that the board should develop and sustain an effective risk management framework and explain the nature of the principle risks the company is willing to take (risk appetite) to achieve its long-term strategic objectives (FRC, 2024). As principles define “what” good governance looks like, provisions suggest “how” to achieve it. For example, the code mandates the board to explain in the annual report how the principal risks are being managed and mitigated.

[1] FRC is the UK’s regulator responsible for overseeing the UK Corporate Governance Code

Therefore, the code stresses that these operate on a 'comply or explain' basis and companies should avoid a 'tick-box approach'. Alternatively, the code suggests complying with a provision can be justified depending on the specific contexts based on a range of factors, including the size, complexity, history and ownership structure of a company (FRC, 2024). It is then the responsibility of the boards to employ this flexibility wisely and evaluate several governance approaches thoughtfully. Therefore, in the UK, there are no strict rules on how those responsible for governance should act to protect their primary stakeholders by creating systems to identify, assess and respond to the entity's risks (Woods, 2009).

However, the most recently updated Code (2024) focused on the application of the principles. The listing rules require companies to clarify by stating how they have applied the principles in a way that would allow stakeholders to assess how the principles have been applied. Therefore, the effective application of the principles should be reinforced by high-quality reporting on the provisions (FRC, 2024). The code recommends that listed firms adopt best RM practices, including the creation of holistic RM frameworks and wider involvement from boards of directors in risk governance (Malik et al., 2020). A growing number of UK-listed companies now adhere to these recommendations, which focus on the establishment of an ERM process and the creation of a board-level risk committee (BLRC) to enhance the board's risk oversight governance (Malik et al., 2020).

In addition to its emphasis on risk governance structure, and similar to the Saudi's CGR, the UK's code highlights the importance of a company's culture that fosters integrity, openness, value diversity, and is responsive to the perspectives of shareholders and stakeholders (FRC, 2024). Both risk governance structure and risk culture are key elements of this thesis which are explored in detail in Chapter Two, Sections 2.2.3 and 2.2.4.

In the following section, I introduce the research problem outlining the key challenges

1.2 Research Problem

These corporate governance codes provide the general guidelines for risk management. This includes the responsibility of the boards toward establishing risk governance structures and promoting a company's culture of openness, integrity, and diversity. Corporate governance codes expect the listed companies to adopt one or more of the risk management standards such as ISO 31000, IRM, or COSO (Woods, 2009). These standards discussed in the literature

review section 2.2.3 concentrate on ERM being embedded in the different organisational levels, but do not consider the unique nature of projects. Under Project Risk Management (PRM) risks are usually identified, mitigated, prevented, and controlled against the project constraints. In contrast, ERM conceptualises risks as opportunities for growing, making profits, or creating value based on the organisational risk appetite (Agarwal et al. 2019). Within these distinct management systems, an objective view of risk such as PRM concentrates on risks associated with project metrics of scope, time, and budget versus the subjective view of ERM that oversees and manages the interdependencies of risks across organisational objectives (See Table 1.1).

Table 1.1: Comparison between ERM and PRM (Liu et al., 2013)

Key features	Expressions in ERM	Expressions in PRM
Objectives	Align to the four enterprise objectives—strategic, operations, reporting, and compliance	To complete the project successfully
Scope	Internal and external events affecting achievement of an entity's objectives must be identified	Cost, time, quality, safety, and environment-related risks (that influence the implementation of the project)
Risk categories	Strategic risks, market risks, operation risks, financial risks, and compliance risks	Owner-contractor agreement, owner conditions, subcontractor conditions, project execution, project preparation and planning, contracting and administration procedures, and external risks
Framework and methods	Relatively stable in a period of time	Changing from project to project
Person in charge	Top managers (e.g., Chief Risk Officer) of the entity	Project managers

This disconnect creates challenges for organisations in aligning corporate governance regulations and guidelines with PRM and ERM interaction. Since these corporate governance codes do not offer guidance on how risk governance structure and culture address the relationship between ERM and PRM, achieving alignment between the two remains challenging. Addressing this gap is critical for ensuring an organisation can achieve its strategic objectives, creating and protecting values. Therefore to address the research problem, the next section defines the research aim and questions, focusing on the integration of PRM and ERM.

1.3 Research Aim, Objectives, and Questions

This thesis aims to explore strategies for strengthening the connection between ERM and PRM to improve integration, enhance decision-making, and promote both value creation and protection. To achieve this, I employ a qualitative study of risk management of three case studies by examining how each case study fosters a common understanding of risk perception across employees at different departmental and organisational levels, particularly within project settings. Additionally, I explore the risk governance structures and assess the risk culture maturity in each case study to understand how these factors influence self-organisation and the integration of PRM and ERM. Based on this, the main research question and three sub-questions are as follows:

How can the integration of ERM and PRM be achieved to enhance decision making, create and protect values?

The three sub-questions:

1- how do the organisations under study define risk?

2- how can governance, especially risk governance, influence the concept of self-organisation, a key element of CAS, in shaping the integration of PRM and ERM?

3- What role does risk culture play in the integration of PRM and ERM?

1.4 Research Significance

The misalignment between PRM and ERM presents challenges to organisations in the sense that PRM may operate in a different direction if not aligned with ERM strategic level. This means PRM if not aligned with ERM, does not enhance decision-making processes and may shift away from achieving the organisation strategic objectives.

Despite the widely accepted adoption of risk management standards such as ISO 31000 and COSO, their emphasis often overlooks the unique nature of project risks constrained by time, budget, and scope. In addition, the standards are set in a high level as one size fits all for all oeganisation regardless of their size, industry, and complexity. Therefore, as this thesis explores different organisations contexts, it offers multiple risk governance structures enriching the literature on ERM integration through the role of governance structure in relation to projects.

This thesis also informs the literature on risk culture which lacks empirical examples of the applicability of IRM's successful risk culture criteria by examining its criteria on three different organisations: a subsidiary, a project-based, and a parent company. By addressing the integration of PRM and ERM, this thesis contributes to building more resilient organisations capable of dealing with project-specific complexity within its border enterprise scope.

1.5 Conceptual framework

The conceptual framework of this thesis stems from corporate governance, which guides the risk management practices within both public and private companies. Following corporate governance is risk management with a specific focus on risk governance structure and risk culture looking at their impact on ERM/PRM integration (Figure 1.1).

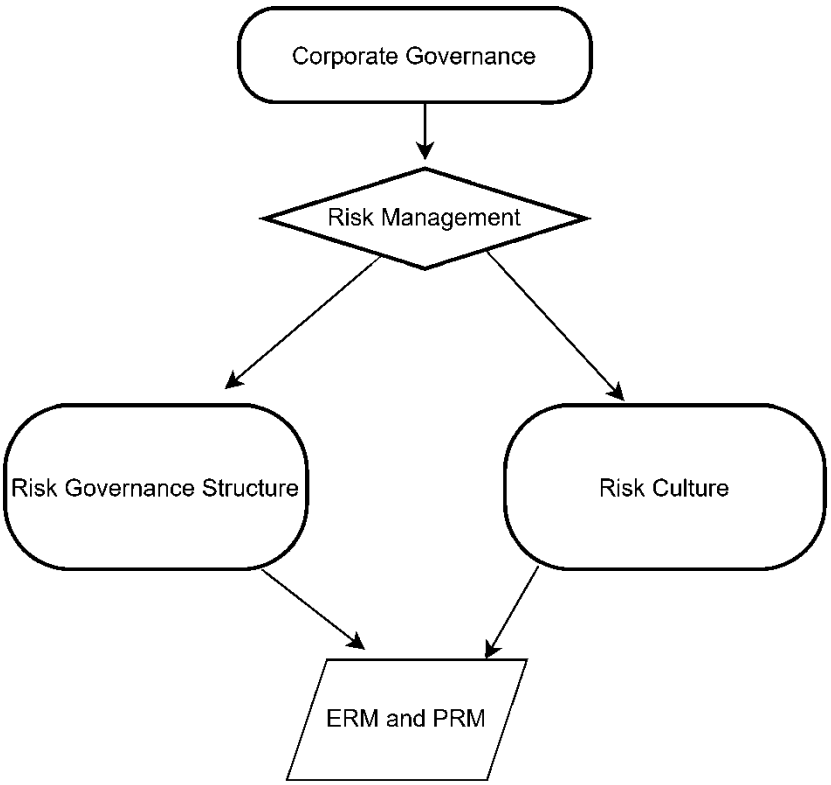


Figure 1.1: Conceptual Framework (Author's own)

1.5 Thesis structure

The thesis is structured as follows:

Chapter Two: The chapter introduces the reader to the risk management history in short, linking the development of the concepts over the years with two prominent definitions in the literature of risk management. The objective definition suits the project management mindset driven by a narrow focus on project constraints, while the subjective definition reflects the ERM-wide perspective which looks at the interdependency of all risks facing the different departments of the organisation instead of looking at each individually. Finally, through the lens of CAS theory, the chapter examines the role of risk governance structure and risk culture in the integration of PRM and ERM.

Chapter Three: Stemmed from a critical realist mindset, this chapter outlines the case studies, followed by detailed explanations of the processes undertaken for the data collection methods: semi-structured interviews and documentary analysis. Then, diving into the data analysis in which template analysis was chosen to support the abduction approach. Moving on to address the methodological rigor, followed by a description of ethical considerations underpinning this research.

Chapter Four: The chapter presents and discusses the research findings addressing the research questions. The first theme presents different strategies the organisations adopt to bridge the gap between PRM and ERM perceptions. The second theme examines the role of corporate governance in PRM/ERM integration, including an analysis of the successful risk culture criteria outlined by the Institute for Risk Management (IRM, 2012) in the three case studies. The third theme addresses the connection between organisations' values and risk management practices, highlighting their influence on PRM and ERM integration.

Chapter Five: This chapter synthesises the key findings discussed in the findings and discussion chapter, highlighting several theoretical and practical implications that collectively contribute to an effective approach for integrating PRM into ERM. The chapter concludes with the limitations encountered in this study and the implications for future research.

Chapter Two: Literature Review

2.1 Introduction

The literature review is structured into two parts: the first part reviews the historical evolution of risk and risk management, tracing the impact of both objective and subjective concepts on shaping definitions to explore the different perceptions of risk offered in the literature to explore how organisations can accommodate diverse perceptions of risk, particularly within the context of ERM and PRM. The second part introduces ERM, and briefly reviews the current literature leading to the definitions presented in this review. ERM is then conceptualised from the perspective of systems thinking, moving on to the application of the complex adaptive system (CAS) as a lens to guide the review of ERM and PRM, particularly in identifying the issue of risk governance and culture (2.2.3 and 2.2.4). Finally, a dedicated section (2.2.5) reviews the CAS literature and explains the proposed CAS framework for this research.

2.1 Part One: the history of risk and risk management concepts

2.1.1 A brief history of risk

The concept of risk has evolved, reflecting several and sometimes conflicting risk perspectives. During the premodern era (pre-18th century), risk was associated with natural phenomena such as volcanic eruptions and earthquakes, moving to being applied to human involvement and the management of risk (Spira & Page, 2003). Thereafter, in early modernity (18th to 20th century), potential dangers (such as chemical spills) were to some extent known and expected to be treated or at least mitigated (Beck & Holzer, 2007). At the end of modernity (late 20th century), the world was shaped by the laws of probability, and thus, risk was perceived as a comparatively explicit case, measurable and calculable (Carlsson-Wall et al., 2019). Risk was known in statistical idioms as the probability of an event multiplied by the bulk of losses or gains connected with the event (Gephart Jr et al., 2009). It was considered an objective incident existing in a real-world form and can pre-occur in nature, to be classified by scientific calculations and measurements, and to be controlled using available knowledge (ibid., 2009). Hence, objectivists (or frequentists) believe that probability is largely a physical property that is expressed by the relative frequency within a repeatable experiment. A case in point reflecting this perspective is found in project management, where literature such as Kerzner

and Saladis (2009) define project risk as an assessment of the likelihood and impact of failing to achieve the project objective. Therefore, from this perspective, project risk management (PRM) aims to successfully complete a project considering risks related to cost, time, quality, safety, and the environment (Liu et al., 2013; Zou et al., 2007). Thus, it is understandable to see PRM extensively using quantitative risk assessment such as probabilistic models (e.g. Monte Carlo Simulation) and statistical analyses to assess and mitigate risks. This adds an objective and numerical dimension to risk assessment.

Later, postmodernists[2] (late 20th century until present day) refuted the tendency of objectivity and certainty in knowledge and rationality, believing that people cannot make unquestionable knowledge claims, rather their knowledge depends on beliefs which can be held implicitly and undoubtedly, referred to as tacit knowledge (Reid, 1959). Accordingly, risk is not an objective or specified definition of social or technological features of society, but instead a means of envisaging society and decisions (Miller, 2009). From a subjective perspective, probability is a personal conviction, and it is impossible to determine probabilities with certainty. Accordingly, probability is merely one method for attempting to deal with uncertainty (Nisula, 2018). Black swans, or high-impact, low-probability catastrophes such as COVID-19, are other significant contributions to the conventional understanding of risk. Such risks must be handled even though traditional risk management would disregard them owing to their low probability[3]. A clear illustration of subjectivity arising from heightened uncertainty is observed in ERM. Unlike PRM, which concentrates on individual projects, ERM takes a holistic view, considering both internal and external events that impact the overarching objectives of the entire organisation (COSO, 2004). ERM's subjective element is further accentuated by its emphasis on assessing the interdependencies of risks across different departments and functions within the organisation, acknowledging the complex relationships that may exist and their potential impact on organisational objectives.

In summary, our comprehension of risk has significantly developed. Historically, it was linked to natural disasters in the premodern era, moving to the modern era, where the concept of

[2] Postmodernism refers to a philosophical and cultural movement that responds critically to modernist beliefs, particularly those regarding epistemology, and offers event (Gephart Jr et al., 2009).

[3] Traditional risk management often focuses on specific, isolated risks and is typically associated with a more structured and linear approach.

risk has evolved into a field of study within cognitive science, allowing for the prediction of risk through the calculation of probability and impact. In the postmodern era, risk has come to be understood as a subjective phenomenon, dependent on the specific context of a particular place, conditions, and time.

The following section explores how the evolving perspectives of risk over time have influenced the definitions of risk within the literature.

2.1.2 Definitions of risk

Risk is an abstract concept with no agreed definition. The Institute of Risk Management (IRM, 2002, p.2) refers to risk as "the combination of the probability of an event and its positive or negative consequences." This definition represents the modernists' view to understand risk considering probabilities and consequences which has been adopted by multiple industries. For example, the nuclear industry has formalised a quantitative definition of risk, where each scenario is associated with the corresponding probability and associated consequences (Nisula, 2018). This is a positivist view which sees risks as phenomena that exist independently and objectively, "risk consists of physical facts that can be explained, predicted, and controlled" (Nisula, 2018, p.33). In contrast, ISO 31000 (2018, p.2)[4] defines risk as "the effect of uncertainty on objectives." Similarly, the Institute of Internal Auditors defines risk as the uncertainty of an event occurring, which may impact achieving the objectives and likewise, The Treasury Board Secretariat defines risk as the uncertainty around future events that may impact on achieving organisations' objectives (Lalonde, 2020). Such definitions represent the postmodernists' view which associates risk with uncertainty, that is, risk only exists in the minds of people because it lacks predictability of problem structure or consequence of a decision (Aven & Renn, 2010). Therefore, "in the shift from modernism to postmodernism, individual objectivity gave way to interpersonal subjectivity as the basis for understanding and conduct" (Gephart Jr et al., 2009, p.147). This indicates that risk is a complex phenomenon rather than a simple, linear concept that can be easily predicted. Due to this complexity, complexity theory becomes relevant in guiding my discussion of risk as a lens, which will later enable the conceptualisation of ERM and PRM as complex adaptive systems (CAS) (see Section

[4] ISO 31000 is a risk management standard developed by the International Organisation for Standardisation and was last updated in 2018.

2.2.5). Complexity theory seeks to understand complex thought as a multidimensional form of knowledge, emphasising the importance of recognising the connections between agents such as projects with ERM, distinguishing these connections without isolating them from each other (Morin, 2008). In project management, tools like lesson-learned registers are valuable for assessing the likelihood and consequences of events occurring based on similar prior projects. However, the current conditions of a present project may not necessarily align with those of previous projects. For instance, factors such as changes in technology, team composition, regulatory environments, or market conditions can lead to different risk assessment outcomes, even if the projects share similar scopes. In ERM, the scope expands further to encompass both internal and external environments, which can introduce knowledge gaps, especially when entering new markets. Monitoring risks across various organisational departments and external markets in ERM introduces a broader spectrum of uncertainties compared to PRM which focuses more on individual projects.

Therefore, I concur with the postmodernist in that risk has come to be understood as a subjective phenomenon dependent on the specific context of a particular place, conditions, and time. Specifically, Alberts (2006) identified four fundamental elements that are necessary for the existence of risk: context, actions, conditions, and consequences. The term "context" pertains to the fundamental circumstances, background, or environment in which risk is being evaluated (ibid., 2006), thus, it is the understanding of this context that informs our knowledge of the specific actions, conditions, and consequences that are relevant to a given situation. Byrne and Callaghan (2013) argue that knowledge is inherently local, contextual, and specific to time and space. Cilliers (1998) further emphasises that knowledge is not only contextual but also subjective, meaning that the dynamic nature of risks implies their significance can change over time because the underlying circumstances, conditions, and actions associated with a particular situation today may not remain constant in the future. Consequently, the likelihood and consequences of a risk occurring at present or in a particular location may differ from the assessment of the likelihood and consequences of that same risk occurring in the future or a different location. Once the context is defined, it is critical to properly examine the remaining risk aspects appropriately. Alberts (2006, p.6) defines action as "the specific act or event that initiates or gives rise to a potential risk." It is the active component of risk that is required for risk to materialise and must be accompanied by one or

more particular conditions (Alberts, 2006) which are regarded as the passive component of risk. They define the current situation or the set of conditions that may give rise to potential risks. When conditions are combined with a certain triggering action, they have the potential to produce a series of consequences or outcomes. As the last component of risk, consequences relate to the potential results or impacts of an activity when paired with specified condition(s) (Alberts, 2006).

To sum up the first part, the literature reveals different perspectives on risk, with objectivists such as PRM focusing on completing individual projects within the scope of time, quality, and budget (Agarwal & Virine, 2019), and subjectivists such as ERM aiming to improve decision-making by aligning the four enterprise objectives of strategic, operation, reporting, and compliance (Liu et al., 2013). Given the inherent complexity of projects, which are temporary, evolving, and cross-functional in nature, integrating PRM into ERM requires an understanding of how different risk perceptions across organisational units interact. Projects, unlike stable departments, must continuously adapt to shifting conditions and collaborate with diverse stakeholders, leading to sociopolitical complexity as different agendas, such as those of PRM and ERM coexist. This complexity is not easily quantified as it is shaped by subjective perceptions and influenced by both conscious and subconscious factors (Murray-Webster & Hillson, 2008). How organisations create their perception of risk directly impacts their interactions and decision-making processes (Millo & MacKenzie, 2009). Moreover, managers experience and manage complexity based on individual interpretations and collective experiences within their teams, emphasising the need for a shared understanding of risk (Maylor et al., 2013).

Given this context, Complex Adaptive Systems (CAS) theory is adopted as the most appropriate theoretical lens because it accounts for non-linearity, interdependence, and emergent behaviour of risks. CAS enables exploration of how agents such as ERM and PRM actors interact dynamically and adaptively without assuming equilibrium or linearity. Alternative theories were considered but found to be inappropriate; for example, while systems theory views organisations as interconnected parts of a whole, it typically assumes a level of stability and predictability that is incompatible with the fluid, evolving nature of projects and the nature of risks. Instead, as outlined in Section 2.2.2, this study begins by framing ERM within a systems perspective, before demonstrating that its dynamic, evolving,

and dual centralised and decentralised nature aligns more closely with the principles of a complex adaptive system, thereby justifying the use of CAS as the most appropriate theoretical framework. Similarly, while stakeholder theory has influenced the evolution of corporate governance and risk management by promoting accountability to a broad range of actors (Freeman, 1984; Chairani & Siregar, 2021), its practical application in complex risk environments remains limited. As Albasteki (2021) highlights, even leading frameworks such as ISO 31000 and COSO ERM often neglect the inclusion of key stakeholders, suggesting a disconnect between theoretical ideals and operational realities. Stakeholder theory assumes that all relevant interests can be identified, understood, and managed—a premise that becomes unrealistic in dynamic and uncertain settings (Shaikh & Randhawa, 2022). This limitation undermines its utility in environments where risks are emergent, distributed, and not attributable to clearly defined actors. In contrast, CAS theory better captures the non-linear, systemic nature of risk by emphasising adaptation, both centralised and decentralised control, and learning in response to uncertainty. Thus, as a first step towards integrating PRM into ERM and looking for common dimensions of risk perceptions, theoretically, within these different ERM and PRM agendas causing sociopolitical complexity[5], the first research question is: How do the organisations under study define and manage risk and how adeptly do they accommodate diverse perceptions?

2.2 Part Two: Enterprise Risk Management and Project Risk Management

2.2 ERM

2.2.1 Overview

The literature on risk management contains a wealth of trade and commercial publications about ERM, aimed at the executive level, albeit rare, there are scholarly works on ERM. However, because ERM is a relatively new risk management paradigm, academic research in this area is fragmented covering some topics such as the fundamentals of ERM (Hampton, 2009), the determinants of ERM (Hoyt & Liebenberg 2011), the adoption of ERM practices (Paape & Speklé, 2012), the relationship between ERM and firm performance and value (Malik et al., 2020b; Florio & Leoni, 2017; Kommunuri et al., 2020). My primary focus is on the

[5] "The number of stakeholders represents a structural complexity but their different agendas cause sociopolitical complexity"(Maylor et al., 2013, p.47).

integration of ERM with other risk systems, specifically PRM. This emphasis stems from my personal experience in project management where I've encountered dynamic, time-constrains that differ significantly from the more structured and ongoing nature of ERM. This has sparked my curiosity to explore methods for effectively accommodating PRM within the established and structured framework of ERM.

Approximately three decades ago, several governments (e.g., United Kingdom, Australian and Canadian Federal) and their organisations established guidelines and commanded risk reporting for different departments and institutions in both public and private sectors (Lalonde, 2020) because risk management can be a powerful instrument for development (World Bank, 2014, p. 3; UN, 2020a). Simultaneously, there was a reform during the 1980s, predominantly in the UK and Australia to bring best practices of private sector managerial and administrative performance to public sector organisations known in some countries as New Public Management (NPM) (Lapsley, 2009). In other countries such as Saudi Arabia, the reform started during the last decade. These guidelines, along with the development of ISO 31000 (See next section), have endorsed the concept of ERM which applies the process and methods of risk management at an organisational-wide level (Lalonde, 2020). ERM is the newest field of risk management after financial and project risk management and is a paradigm shift in the 21st century from traditional risk management that perceives and treats risks in a solitary manner. Instead, ERM is a holistic process, integrating all risks facing an organisation with corporate governance and organisational strategic objectives. For example, to support organisations in making informed business decisions involving calculated risks, improving operational efficiency, and boosting resilience, it's important to show suppliers and customers that risks are being detected and addressed at an early stage.

Defining ERM can be a nuanced task because it involves considering the unique characteristics and needs of a particular organisation while also aligning with relevant standards and best practices. It is complex and requires an understanding of both risk management principles and the specific context in which ERM is being applied. ISO 31000, while it offers a comprehensive standard for risk management, does not present a specific definition tailored to ERM, whereas COSO in its 2004 framework defines ERM as, “A process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk

to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives" (Coso, 2004, p.2). However, it is important to note that even with COSO's 2017 update which places a greater emphasis on integrating risk management with strategy and performance, the definition still falls short of acknowledging the complexity of risks. The COSO Enterprise Risk Management Framework (2017) defines ERM as, "The culture, capabilities, and practices, integrated with strategy-setting and its execution, that organisations rely on to manage risk in creating, preserving and realising value". This definition recognises that risk management processes, policies, procedures, and other supporting information, are of no use on their own, rather it is the culture, capabilities and practices within an organisation that are integrated to ensure action is taken to change the risks that bring value. However, this does not clarify the characteristics of this culture and does not account for multiple individual-level perspectives or comprehensively define the integration of various risk management systems. Instead, the definition primarily leans towards a top-down approach, where risk management is predominantly integrated into the organisation's strategic planning and governance processes. As such, to better conceptualise ERM from a theoretical perspective, I adopt the lens of systems thinking to visualise ERM and make sense of its components prior to conceptualising ERM from a CAS perspective, later in the thesis (see 2.2.5).

2.2.2 Exploring ERM from the Systems Thinking Perspective

Ackoff (1972, p.662), a renowned contributor to the development of systems thinking, described a system as "a set of interconnected elements". Similarly, Meadows defines a system as "an interconnected set of elements that is coherently organised in a way that achieves something" (Meadows & Wright, 2008, p.16) and emphasises that a system must have three components, elements, interconnections, and a function or purpose. Governance, process, communication and reporting, documentation, feedback and continuous improvement, and risk culture and awareness are all elements of a risk management system according to ISO 31000, COSO, and PMI's Risk Management Standard. Additionally, according to Meadows, these elements refer to anything that interacts with another thing. From my perspective informed by CAS, I consider PRM to be a component of ERM as it interacts with ERM through various forms of communication including reporting, participating in risk workshops, and conducting risk identification brainstorming sessions.

Another essential component is the interconnections of a system. Interconnections encompass various forms of communication, such as those between ERM and PRM, as well as between ERM and internal and external stakeholders. These interconnections involve compliance with guidelines, rules, values, and culture related to risk management. These so-called *attractors* act as governing forces that determine the behaviour of a complex system (Cox et al., 2009). In complexity theory, attractors can be categorised into various types, such as point attractors, periodic attractors, and strange attractors (Kauffman, 1993; Merali, 2006). Aligning with the perspectives of scholars in CAS literature (e.g., Osborn et al., 2002; Boal & Schultz, 2007), this study concentrates on strange attractors that characterise systems that operate in complex yet inherently unpredictable ways, while simultaneously self-organising into an emergent order and structure (Pryor & Bright, 2007). Thus, strange attractors are linked to the potential for evolution, adaptability, and change (Boal & Schultz, 2007).

The third component is the purpose of a system. According to Meadows and Wright (2008), the purpose is not always explicitly communicated through speech, writing, or explicit expression, instead, purposes are inferred from behaviour rather than relying on stated goals. Although all elements of ERM including PRM have the ultimate objective of facilitating informed decision-making to crate and protect value (Project Management Institute, 2017; Coso, 2004; IS0 31000, 2018), the behaviour of the system in ERM/PRM literature struggles to achieve this objective. The literature identifies a clear gap between the establishment of ERM and the actual implementation (for example, see Jean-Jules & Vicente, 2021; Albasteki, 2021; Al-Tayan, 2022). In particular, Jean-Jules and Vicente (2021) point to the prevailing description of ERM in technical terms tending to prevent both scholars and practitioners from being fully sensitive to the social issues associated with ERM implementation, research frequently devotes little attention to social theories about ERM implementation. In response, I employ the lens of CAS to explore how governance and culture influence ERM/PRM integration. This approach begins by examining the core standards, particularly focusing on the dominant ERM standard, ISO 31000, and referencing COSO where relevant, as both are widely regarded as the leading global standards in ERM (IRM, 2020). ISO 31000 is recognised for its broad applicability and influence on risk management practices across various sectors, making it the foundation of ERM in many organisations (Frigo & Anderson, 2011). Additionally, COSO, as a globally respected framework, offers an integrated model of risk management that

complements ISO 31000. Furthermore, the PMI's Risk Management Standard, first introduced in 2009 and revised in 2019, is essential for understanding PRM. Its emphasis on managing risks across portfolios, programs, and projects (PMI, 2019) aligns with the intent to explore the intersection of ERM and PRM, making it highly relevant to this research.

2.2.3 Examining Governance in ERM and PRM Standards

The first widely utilised ERM framework was ISO 31000 (see Figure 2.1), which operates under the assumption that risk management is built upon principles, a framework, and a process. The principles establish the foundation for effective risk management, clarifying its value, intentions, and purpose. In other words, these principles outline what needs to be achieved. ISO 31000 identifies eight key principles. The first is *integration*, meaning that risk management must be embedded into all organisational activities; the second is *structure and comprehensiveness*, suggesting that a well-structured and comprehensive approach ensures consistent and comparable outcomes. However, the third principle—*tailoring/customising* calls for risk management to be adapted to the unique context of each organisation, often leaving companies without clear guidance on how to adopt to their unique context.

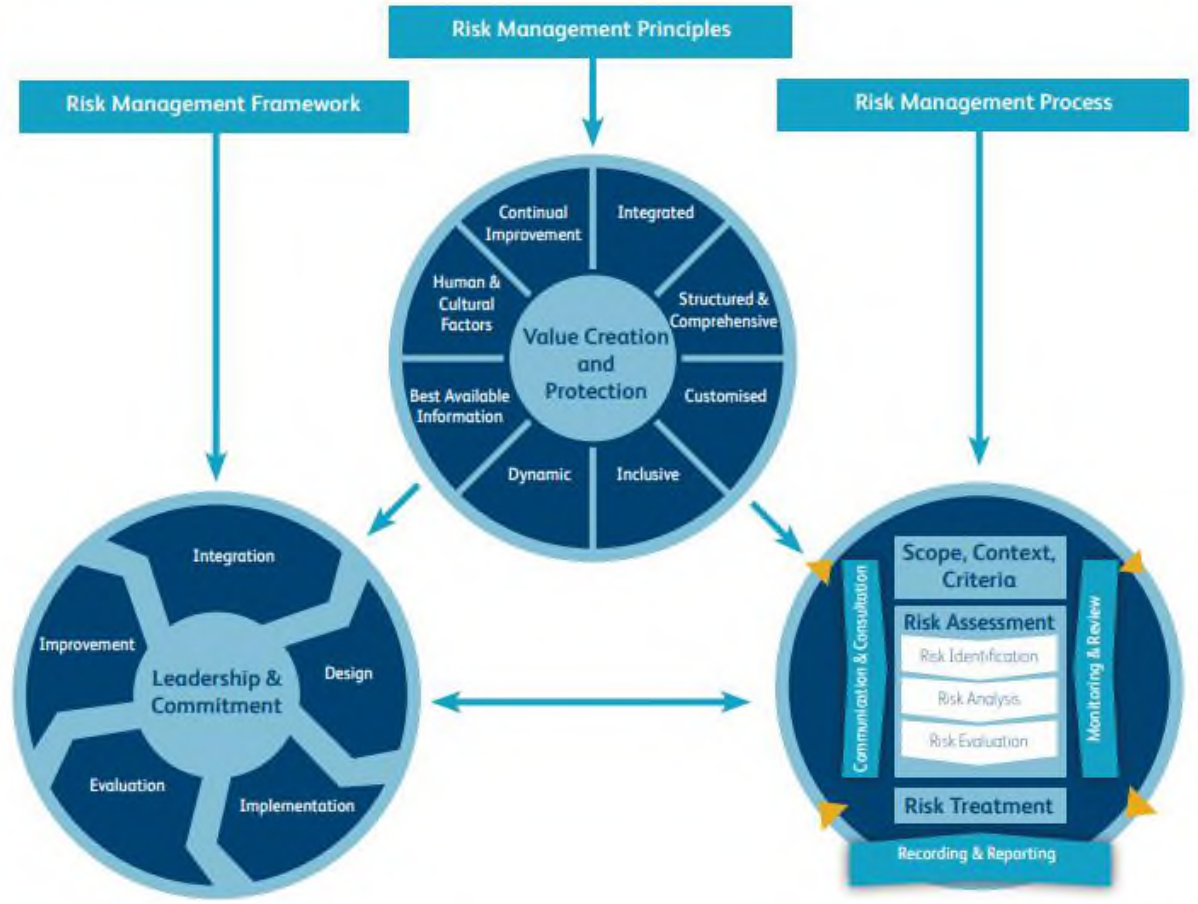


Figure 2.1: ERM principles, framework, and process (ISO,2018 P.11)

The literature on ERM shows that companies struggle to implement ERM governance within its components. For example, Makmor et al. (2023) highlight the need for studies on ERM that focus on the implementation of ERM within conglomerate groups with diverse subsidiaries. The absence of key stakeholders in ISO and COSO was discussed by Albasteki (2021) through the lens of stakeholder theory. The study of corporate governance examines how companies are directed and controlled to ensure accountability and alignment of interests among shareholders, managers, and other stakeholders (Jensen & Meckling, 1976; Freeman, 1984; Corporate Governance Institute, 2022). This literature includes agency theory which focuses on the conflicts between owners and managers and stakeholder theory which broadens governance to include all parties affected by the company's operations (Freeman, 1984). These governance perspectives are relevant to PRM, conceptualised from a system perspective as part of ERM's broader governance, linking it directly to top management. In the project and portfolio governance literature, Martinsuo (2013) critiques the rational

approach that assumes companies have full awareness of all internal and external factors influencing well-defined projects within known environments. He calls for new research to focus on context (the specific conditions under which the project portfolio is managed) and practice (what managers actually do). Similarly, Winch (2014) highlights the need for research on the governance interface between the owner (where ERM resides) and the project (see Figure 2.2), explicitly identifying the relationship between owners and projects as a key governance challenge.

Figure 2.2: Winch's three domains of project organisation (Winch, 2014, p.21)

From a complexity theory perspective, the gap lies in the governance structures that adequately account for the complexities of projects considering multiple stakeholders, unique activities, and dynamic timeframes. These governance structures must also recognise the interdependencies within a broader system that requires continuous *feedback loops* between elements. Risk management, one of the most critical domains in project management, is intended to support decision-making for both project managers and owners, creating and protecting the values of the organisation (PMI, 2017; ISO 31000, 2018; Coso, 2017). Recognising the complexity of *nested systems*, the PMI's Risk Management Standard improved

its second version issued in 2019, which expanded beyond the original 2009 version's focus on single projects to include programme and portfolio risks (see Figure 2.3).

Figure 2.3: Risk management domains (The Standard for Risk Management PMI, 2019)

Although PMI claims that its risk management standard can be used to harmonise practice between ERM and portfolios, programmes, and project management despite the life cycle method used, it focuses on process, technology, and information while ignoring the people involved in these activities. For example, while the standard mentions ensuring alignment between portfolio, programme, and project management risk governance models and ERM strategies, as well as promoting effective risk management throughout the enterprise through a risk management culture, it does not specify what constitutes a suitable risk management culture or how to arrive at such an appropriate risk culture. The standard states that risk management at the project level is analysed and considered based on its potential impact on the capacity to achieve a tangible outcome. As a result, project risks are evaluated and analysed at the tactical level, while additional considerations in terms of impact on expected value or benefit generation are escalated to the portfolio and programme governance levels. However, before escalating, communication between the project and higher governance levels is required to determine how project activities influence value and benefits. The standard does not clearly define when or how this communication should occur, aside from recommending escalation. Instead, it attributes risk sources to factors such as stakeholder

analysis, business cases, or enterprise environmental factors, leaving a gap in the clarity of communication loops across different governance levels.

The five remaining principles of IS0 31000 can be explored from the lens of CAS. For example, the principle of *inclusivity* stresses the importance of appropriate and timely involvement of stakeholders, whose knowledge, views, and perceptions inform the system's behaviour. In a CAS, each agent, such as PRM within the ERM system, does not have a complete view of the overall system's behaviour but reacts based on the information available in its immediate environment (Nisula, 2018). The *dynamic* principle recognises that risks can emerge, change, or disappear as an organisation's internal and external contexts evolve, reflecting the continuous adaptation inherent in a CAS. The principle of *best available information* highlights that risk management is informed by historical and current data, mirroring the *path dependency* in CAS where past actions and knowledge influence present decision-making behaviours (Nisula, 2018). *Human and cultural* factors emphasise that human behaviour and organisational culture significantly impact risk management at every level and stage. Finally, the principle of *continual improvement* aligns with the CAS concept by noting that risk management should evolve through ongoing learning and adaptation. According to Holland (1992, 1995), a CAS is "a system composed of interacting *agents*, which undergo constant change, both autonomously and in interaction with their environment to produce complex and adaptive behaviours and patterns". These patterns are aggregate behaviours and structures that are not predictable from an analysis of the system's component parts (Sweetman et al., 2014). Rather, *self-organisation* emerges as agents interact based on sometimes simple rules that can evolve with accumulated experience and changing environmental conditions (Anderson, 1999; Holland, 1995). Therefore, the second emerging research question is: how can governance, especially risk governance, influence the concept of self-organisation, a key element of CAS, in shaping the integration of PRM and ERM?

2.2.4 Examining risk culture in ERM and PRM Standards

COSO (2017) highlights the importance of governance and culture as key components of ERM (Figure 2.4). However, while these elements are recognised as critical, neither COSO nor ISO 31000 provide concrete guidance on how to establish or sustain a strong risk culture. This oversight leaves a gap in the practical application of these frameworks, particularly regarding fostering a culture that supports the integration of PRM and ERM. Without a clear direction

for building a cohesive risk culture, organisations may struggle to ensure consistent risk management practices across different levels of governance.

Figure 2.4: ERM framework (Coso, 2017 p.3)

In contrast, the Institute for Risk Management (IRM, 2012) offers a more detailed and actionable definition of risk culture, describing it as the shared values, beliefs, and understanding of risk across the organisation. IRM's ten criteria for a successful risk culture provide practical steps to build and maintain this culture, many of which align closely with CAS principles. These criteria not only address the gaps in existing standards but also provide the cultural foundation necessary for integrating PRM and ERM. PRM tends to deal with more tangible, project-specific risks, while ERM encompasses broader, strategic risks. The integration of the two requires a unified risk culture that facilitates consistent communication, shared understanding, and aligned actions. If different risk cultures exist within an organisation, it becomes more challenging to harmonise these practices, especially when moving from project-specific risks to portfolio-wide considerations. The IRM (2012) criteria offer a more concrete framework for building an adaptive and cohesive risk culture, which aligns mostly with CAS principles. Each of IRM's ten criteria provides a mechanism for fostering a culture that is capable of supporting the integration of PRM and ERM, in a way that current standards do not:

Tone at all levels: IRM stresses that both top-down leadership and bottom-up participation are needed to establish a successful risk culture, resonating with CAS's notion of adaptive systems where agents at all levels interact and contribute to system evolution.

Commitment to ethical principles: A commitment to ethical decision-making considering the views of wider stakeholders ensures that risk management is not isolated but integrated into the organisation's broader environment. CAS theory emphasises the interconnectedness of systems with their environments (Anderson, 1999), and this external alignment is key for integrating risk at the project and enterprise levels.

Continuous management of risk: Continuous risk management with clear accountability aligns with the CAS principle of constant adaptation. A culture of continuous monitoring and adjustment is essential to accommodate changing project needs and strategic objectives for PRM and ERM to be integrated.

Transparency and timely communication: A successful risk culture according to IRM, relies on open communication, especially when reporting risks. CAS is underpinned by its interactivity with the environment, drawing resources from the environment and accepting feedback from the environment, all of which characterise an open system (Cox et al., 2009). CAS stresses the importance of feedback loops for system adaptability. For PRM and ERM integration, effective communication channels between projects and enterprise governance are crucial.

Encouragement of risk reporting: The promotion of risk reporting without fear of blame creates a culture of accountability and learning, central to CAS's self-organising nature. PRM and ERM must align in how they treat risk reporting; otherwise, projects may fail to escalate critical risks to the enterprise level.

Handling complex risks: IRM stresses that no risk should be too large or complex to be understood, as even small changes can have significant, emergent consequences in a CAS, (Holland, 1995). Both PRM and ERM must share an understanding of complexity, ensuring that project risks are contextualised within the broader organisational risk framework.

Rewarding appropriate risk behaviour: IRM's focus on rewarding appropriate risk-taking and sanctioning poor risk behaviour aligns with the adaptive feedback mechanisms in CAS. Integration of PRM and ERM requires consistent behaviours and incentives across both systems to ensure that risk culture drives the desired outcomes.

Valuing risk management skills: CAS requires skilled agents to manage complexity, and IRM's emphasis on developing risk management skills is essential for PRM/ERM integration. ISO

31000 and COSO are vague about how risk management capabilities should be cultivated across the organisation. Both frameworks operate under the assumption that individuals within the organisation possess the necessary skills to effectively gather, evaluate, and apply information about risks in a rational manner. Nevertheless, these frameworks fail to adequately consider important factors such as employee engagement, the capability of organisational culture to adapt to the implementation of ERM, and the preparedness of functional departments to accommodate the necessary changes associated with ERM (Jean-Jules & Vicente, 2021).

Diversity of perspectives: IRM advocates for diversity in perspectives, which prevents rigidity and promotes adaptability—a key concept in CAS (Anderson, 1999). In the context of PRM and ERM integration, diversity ensures that project-level risks are not siloed but considered in a broader strategic framework.

Alignment with people strategy: Finally, IRM emphasises aligning risk culture with employee engagement, ensuring a balance between social support and task focus, thereby supporting the dynamic interactions that CAS requires, enabling both PRM and ERM to function as part of a cohesive, adaptable system.

The lack of explicit guidance on risk culture in ISO 31000 and COSO presents a significant challenge for integrating PRM and ERM. The IRM (2012) criteria provide a more detailed framework for fostering a successful risk culture that supports this integration as it aligns with CAS principles of adaptability, communication, and interaction. This leads to the third research question: What role does risk culture play in shaping self-organisation influencing the integration of PRM and ERM? This is crucial because risk culture influences how risks are communicated, escalated, and managed across both the project and enterprise levels. The three case studies in this research will examine how each organisation’s risk culture aligns with IRM's (2012) successful risk culture criteria and its impact on the integration of PRM and ERM.

2.2.5 Complex Adaptive System: Theoretical Framing

While there is a considerable body of research on CAS in the applied sciences (e.g., healthcare and IT) (McDaniel Jr et al., 2009; Coetzee et al., 2016; Van Beurden et al., 2013), the literature on CAS in business and organisational settings, specifically risk management, is relatively scarce. The field of risk management often remains compliance-driven and simplistic (Sachs

& Wadé, 2013), which may explain the scarcity of research in this area. Despite this, there is increasing recognition that risks are inherently complex, with calls to account for interdependencies and non-linear dynamics in risk management (Andringa et al., 2022). This recognition highlights the need to move beyond traditional approaches, which often focus on individual risks, to a more holistic understanding of the interdependencies between risks and organisational functions.

Much of the recent literature addresses risk–risk interaction networks, yet it tends to overlook the complexity emerging from interactions between risks and organisational structures (Sasaki et al., 2024). Risk management theory primarily focuses on the complexity arising from interacting risks but often underemphasises the complexities introduced by an enterprise's internal dynamics. As a result, there is a gap in understanding how risks propagate across organisational functions and how those functions themselves may contribute to risk propagation. One example of this recent focus on risk–risk interactions is the study by Andringa et al. (2022), which introduced the Complex-Based Risk Assessment Method (CBRAM). This approach integrates complexities and risks to improve risk management in complex construction projects. Andringa et al. examined how risks propagate through interrelated complexities and affect project outcomes. The study used tools such as risk registers, risk breakdown structures (RBS), and risk-influence diagrams to map cause-effect relationships between risks. However, their work focused primarily on risk–risk interactions and did not explore how these risks interact with different organisational functions, leaving gaps in understanding the full extent of risk propagation within an enterprise.

The need to examine both risk–risk and function–function interaction networks has been highlighted by van der Vegt et al. (2015), who argued that understanding how risks propagate non-linearly across organisational systems is essential for comprehensive risk management. This perspective suggests that risks do not only interact with other risks but also interact with the functions and processes of the business itself, adding another layer of complexity to risk management strategies.

Sheth & Sinfield (2024) offer a more recent contribution, taking steps toward addressing the gap by conceptualising ERM from a CAS perspective. They argue that the building blocks required for a CAS-based representation of ERM have not been systematically developed in the literature. They introduced Quantified Risk Networks (QRNs), which map the impact of

external risks on internal organisational functions. They claim that QRNs provide a more sophisticated view of risk propagation by linking external risks with the organisation's structure. They argue this approach allows companies to anticipate cascading failures and build resilience against them. By focusing on risk–function and function–function interdependencies, QRNs offer a more comprehensive approach to risk management than traditional models, which typically address risks in isolation. While their work makes significant strides in modelling these interactions, they note that the building blocks needed for a CAS representation of ERM remain underdeveloped. Their study introduces QRNs as a first step toward building a more integrated model of risk management, offering a networked understanding of how risks propagate through organisational structures. However, their focus remains largely on structural relationships, leaving other factors, such as risk governance and risk culture, less explored in terms of how they influence risk management systems' adaptability and resilience.

In this thesis, I build upon this foundation by addressing not only structural interdependencies but also the role of risk governance structure and risk culture in enabling or impeding the self-organisation necessary for effective PRM and ERM integration. Existing CAS frameworks include fundamental elements such as agents, interactions, environment, and feedback loops (Lewin, 1999; Alaa & Fitzgerald, 2013; Nan, 2011; Sweetman et al., 2014), I use these elements adding governance and culture for the purpose of this thesis (Figure 2.5). Governance, in the context of this risk management research, encompasses the structures, guidelines, roles and responsibilities that guide decision-making processes and ensure that risk management strategies and methodology are understood by employees in various departments and organisational levels, whereas culture is defined based on IRM definition, which is the shared values, beliefs, and understanding about risk among employees in an organisation (IRM, 2012, p.7). The definitions of all other elements of CAS in the reviewed literature are as follows:

An *agent* is commonly used to refer to the individual actors or simple entities that drive the actions within a complex adaptive system (Benbya & McKelvey 2006a, Nan 2011). Sweetman et al. (2014) examined projects, individuals, and teams as agents within an information systems portfolio. Likewise, I consider PRM besides other functions such as financial risk management and marketing risk management to be agents of a larger complex system, ERM, because they are governed by behavioural rules or schema (Nan, 2011; Gell-Mann, 1994) such

as norms (risk appetite and risk threshold), values (that guide decision making based on organisational priorities) and beliefs (that shape the perceptions of risk) that allow them to interpret the environment and the actions of other agents (Argyris & Schön, 1997). They are smart and can learn and adapt (Fuller & Moran 2001) by extracting input from other agents and the environment (Holland, 1995) (risk workshops), with no single agent controlling the behaviour of the system as a whole (Benbya & McKelvey, 2006a).

Interactions characterise agents' mutually adaptive conduct (Nan, 2011) and their nature rather than the agents drive the system's behaviour (Sweetman et al., 2014). Agents interact by transferring information, energy, or resources (Cilliers, 1998). In risk workshops or risk brainstorming sessions, for example, agents from the project, finance, and marketing departments are continually interacting with one another by exchanging resources and knowledge regarding interdependencies. Furthermore, interactions between agents can influence the interacting agents (Mitleton-Kelly, 2003b), and these interactions frequently cause them to alter their rules or co-evolve (Stacey, 2002; Mitleton-Kelly 2003a). PRM will co-evolve with these different functions (agents) by interacting with them and understanding how they are interdependent because even if these agents act independently, their interactions can result in aggregates that enhance the system overall (ERM) (Levin, 1998).

The *environment* represents the ever-shifting background within which agents operate and engage. In line with CAS theory, a system, as emphasised by Sweetman et al. (2014), must remain open to its environment. Consequently, a silo organisational culture is incongruent with CAS principles. PRM operates as an open system, facilitating the exchange of technical information and resources, including skills and personnel, with its environment. The condition for the occurrence of self-organisation, whereby aggregate structures enhance system order, is openness (Sweetman et al., 2014). This heightened order necessitates the importation of energy and information into the system and the exportation of disorder back into the environment, echoing Capra's (1996) insights. As noted by Benbya and McKelvey (2006a), environmental changes generate adaptive tension, driving the creation of order within the system, signifying that any achieved "fitness" is transitory. Complex adaptive systems are, therefore, viewed as sub-optimal, operating significantly "far from equilibrium" (Fuller & Moran, 2001), with a focus on improvement rather than optimisation (Holland, 1992). This aligns with ERM's objective aiming to enhance communication among relevant stakeholders,

comprehend risk interdependencies, and consequently co-evolve to enhance decision-making processes, creating and protecting organisational values.

Feedback loops manifest when elements in the output phase provide insights to elements in the input phase (Andriani 2003). An example of a PRM application is the maintenance of a repository of lessons learned, such as risk repositories and risk registers, documenting historical risks and their associated response strategies. This serves ERM, maintaining a cyclical process of feedback and improvement to evolve continuously, ensuring that risk management practices remain adaptive and responsive to the dynamic organisational environment. The emphasis is on enhancing decision-making processes by learning from past experiences and refining risk management strategies over time.

Emergence, as explained by Miller and Page (2007), refers to the occurrence where well-defined aggregate behaviour originates from the localised actions of individual entities. CAS as described by Holland (1992), exemplifies this phenomenon, showcasing aggregate behaviours that emerge from the intricate interactions among their constituent agents. In the realm of ERM, the concept of emergence is particularly relevant as it highlights that the language of risk arises from the dynamic interactions among diverse agents involved in the risk management processes. The interactions among agents within ERM give rise to novel patterns of relationships, unique system-level properties, and distinct structures. This underscores the irreducible nature of emergent properties, emphasising that the overall characteristics of the ERM system transcend the sum of its components.

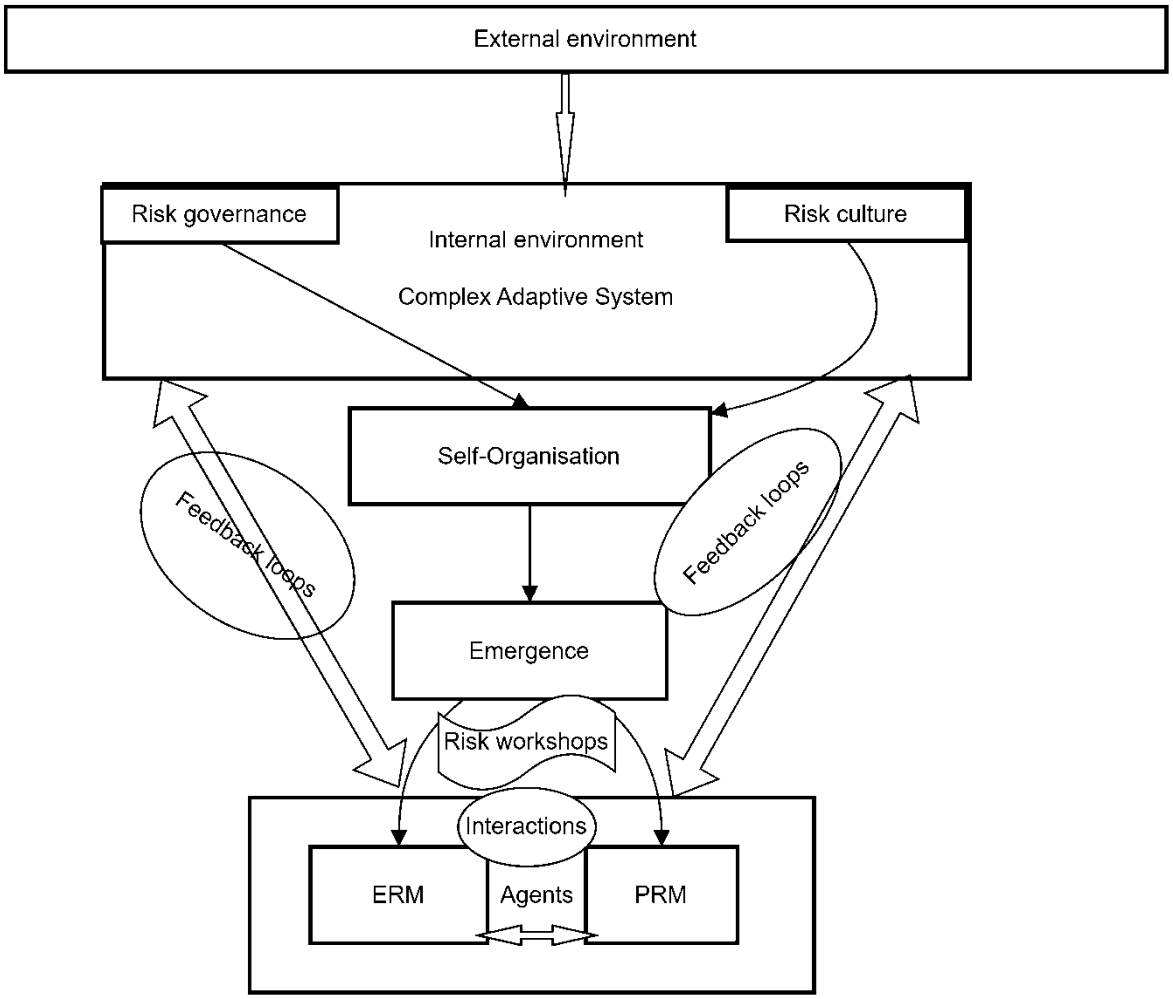


Figure 2.5: The theoretical framework for this study (Source: Author's own)

2.3 Conclusion

The literature review traced the evolution of risk management perceptions, transitioning from an objective, quantitatively focused hazard evaluation (the positivist perspective) to a more subjective, qualitative approach influenced by cultural and human values (the postmodernist perspective). It revealed that risk is now understood as a subjective phenomenon, shaped by its context and influenced by factors such as time, location, conditions, and consequences. The literature was divided into two broad categories: the objectivist perspective, exemplified by PRM, and the subjectivist perspective, exemplified by ERM. This division raises the emergent question of how companies define and accommodate different perceptions of risk. The review of the second part highlighted risk governance structures and risk culture as key gaps that this thesis aims to explore, specifically examining their influence on self-organisation—a central element of CAS and its impact on the integration of PRM and ERM. The following chapter discusses the methodological approach and methods used to explore the gap presented throughout this chapter.

Chapter Three: Methodology

3.1 Introduction

In this chapter, I outline the methodology employed in my study, structured as follows: Section 3.2 discusses the research philosophy, emphasising my rationale for adopting critical realism (CR). Section 3.3 defines the case study approach as outlined in the literature and introduces Easton's approach, including the case study design, background, and sampling strategies for each case. Section 3.4 addresses the data collection methods, which include semi-structured interviews and document analysis. Section 3.5 outlines the analysis process, focusing on template analysis, its rationale, and the process as articulated by King (2017). Section 3.6 discusses the ethical considerations underpinning my research. Finally, Section 3.7 acknowledges the methodological limitations encountered during the study.

3.2 Research philosophy

3.2.1 Overview

The complex perspective informing this research aligns with CR, a philosophy that emphasises a layered reality, as developed by Bhaskar (1975). CR posits that reality is stratified into three domains: the empirical, the actual, and the real. The empirical layer refers to what we perceive or comprehend, human experiences and observations (Vincent & O'Mahoney, 2018), or as Jones (2016) calls it, "the observable experience." For example, in my research, the empirical includes accounts of ERM/PRM integration in each case study, gathered through interviews and document analysis (3.4). However, Bhaskar (1978) highlights that reality extends beyond mere observations. The "actual" layer refers to events that occur in time and space, which may not always align with our perceptions and yet include experiences. For instance, although the Governance Risk and Compliance (GRC) model in Company B perceived the complexity of projects, increasing communication with project teams from quarterly to monthly, triangulating interviews and document analysis revealed that project managers were still not fully integrated into the GRC framework. This highlights a disconnect between the intended governance model and actual events. At the deepest level, Bhaskar's (1975) notion of the "real" refers to the underlying structures and mechanisms that generate the physical (empirical) and actual events, which often remain unseen but have an effect. In the case of

Company B, path dependency serves as one such real mechanism. Although the company is newly established, the absence of established practices and clear roles in the governance structure created challenges for integration, illustrating how unseen forces at the real level shaped the actual challenges faced by project managers.

3.2.2 Rationale for Adopting Critical Realism

Danermark et al. (1997) assert that CR is particularly suited for interdisciplinary research, making it relevant to the field of risk management which often requires the integration of various domains such as project management, IT, and marketing to fully understand the risks faced by organisations. By leveraging CR, I can uncover the underlying mechanisms that influence risk perceptions and integration between project functions (PRM) and enterprise functions (ERM).

On the other hand, positivists differ from critical realists in terms of limiting the universe to empirical observable facts, which are usually turned into quantitative and correlative measurements to create universal declarations or laws (Wynn Jr & Williams, 2012). However, when it comes to social science where human uncertainty and social inconstancy exist (such as the scope of risk management), positivism cannot explain and interpret such complexity dominating the social world. This means positivism cannot help explore the integration between ERM and PRM because it is compelled to reduce the worldliness to a series of variables where every variable represents a side of the case under study, but all it can do is relate these variables to each other in a statistical form (Paley, 1998).

Interpretivism, while useful for understanding individual perspectives, does not fully engage with the deeper structures that influence these perspectives. CR bridges this gap by considering both actors' interpretations and the broader social mechanisms that enable and constrain their actions (Wynn Jr & Williams, 2012). This makes CR more suitable for my research, which aims to uncover the mechanisms driving the integration of PRM and ERM within organisations.

Furthermore, CR aligns well with CAS theory, as both share a fundamental focus on understanding complex, dynamic systems. Both emphasise how structures and interactions shape system behaviours and outcomes, but they do so with complementary perspectives. CR digs deeper by providing a framework to explain why these emergent patterns occur through

its focus on uncovering the underlying causal mechanisms (Sayer, 1997), while CAS examines how adaptive behaviours and patterns emerge from interactions within a complex system (Sweetman et al., 2014). In this sense, CR provides the philosophical grounding to explain why the adaptive behaviours observed in CAS occur, offering insight into the underlying forces such as risk governance structures and risk cultures that shape system behaviour. Together, CR and CAS allow for a robust exploration of how risk management systems such as PRM and ERM interact and evolve in response to the internal and external environment, justifying the integration of both perspectives in analysing complex risk management practices.

3.3 Case study

3.3.1 Definitions and CR approach

Unlike other research methods that operate via a significant distance to the object of study, case studies take a close look at the phenomenon under study, to elicit in-depth analysis and continuous feedback regarding the topic under scrutiny (Flyvbjerg, 2006). Employing a case study strategy suits this research because I am addressing 'why' and 'how' questions relative to the experience in the 'social' context (Yin, 1984).

Yin (1984, p. 23) defines case study research as an "empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident." This highlights the significance of studying phenomena in the present, particularly when the boundaries of the phenomenon are ambiguous. Similarly, Eisenhardt (1989) views case study as a strategy for exploring the underlying drivers of certain phenomena by employing multiple cases, aligning with Yin's emphasis on boundary ambiguity.

However, the focus on integration between ERM and PRM in this study is better supported by definitions from Merriam (1998) and Simons (2014) due to the clarity of the boundaries (see the following section 3.3.2). Merriam (1998, p. xiii) characterises a qualitative case study as an "intensive, holistic description and analysis of a bounded phenomenon, such as a program, an institution, a person, a process, or a social unit," and Simons (2014, p. 457) describes it as "an in-depth exploration from multiple perspectives of the complexities and uniqueness of a particular project, policy, institution, or system in a real-life context." Given that this study

addresses a bounded phenomenon—the complex interplay of ERM and PRM practices within specific organisations, these definitions align well with a CR approach.

Easton's (2010) CR perspective further strengthens this study's design by emphasising the suitability of CR for exploring bounded yet complex and dynamic phenomena such as organisations and interorganisational relationships. She asserts this approach is less suited to individual behaviours or purely quantitative studies, aligning well with this research's organisational scope and its focus on the integrated governance of ERM and PRM.

3.3.2 Case study design: Easton's critical realist approach

Easton (2010) first asserts that critical realist case studies should investigate complex, dynamic, and bounded phenomena. I have already visualised PRM/ERM in the literature chapter from a complex perspective. The boundaries of this research are three organisations, with the focus on their risk management practice, where leadership at a macro level focuses on the executive roles such as ERM that lead to enhance decision making at the organisation level, and leadership at a micro level concentrate on the achievement of a specific job or task such as PRM.

Second, Easton shifts toward the issue of the nature of research questions explaining that CR has a rather clear answer. She suggests the question must be of the form "What caused the events associated with the phenomenon to occur" (Easton, 2010b, p.123). In this context, an appropriate guiding question for this research can be: What factors have driven the integration or separation of ERM and PRM practices within the three organisations under study? This question provides a pathway to uncover underlying causal mechanisms shaping the interactions between ERM and PRM across the cases.

Third, according to Easton, entities or objects should be determined. At this stage, Easton does not restrict fully determination as she believes determining causality may later necessitate moving beyond the current boundaries. Accordingly, my initial study objects were ERM, PRM as functions, and employees with risk management duties from other functions. Later, during the interviewing process, I added more objects such as heads of departments, which allowed me to draw on their insights about specific ERM integration practices that assisted my identification of the underlying causal mechanism behind ERM/PRM integration.

Once determined, Easton suggests data to be gathered by qualitative methods. While quantitative methods have been used quite widely in risk management research (e.g., Andringa et al., 2022; Sheth & Sinfield, 2024), some argue that risk management should not be left to quantitative methods because risk management involves decision-making and human judgment (Nisula, 2018). In addition, if I apply a quantitative methodology, the only thing I will be able to determine is whether the PRM is embedded beneath the ERM; however, I will not be able to determine why this is the case nor how to integrate the two systems. Therefore, following Easton's CR case study approach, I employed semi-structured interviews for their flexibility supported by documentary analysis (see Section 3.4).

Qualitative studies are often criticised in terms of their inadequacy to generalisability because they target a smaller population compared to quantitative studies that aim for generalisation to a larger population. However, a case study allows for flexibility to collect data from different sources (Eisenhardt, 1989). Having three distinct case studies allows me to draw insights from multiple contexts and sectors.

After data collection, the next step involves interpretation, acknowledging the distinctions between the empirical, the actual, and the real. Easton emphasises that data are collected from both human participants and material sources (Easton, 2010b). She employs retroduction, a type of inference that requires identifying new mechanisms, and that according to Vincent & O'Mahoney (2018) requires finding additional theories to understand. In this study, I used institutional theory as a complementary perspective to CAS (Figure 3.2) to interpret some of the findings, particularly why most participants in Company C define risk according to the ISO 31000 definition, following Musawir et al. (2024), who also utilised multiple complementary theories in their retrodictive process to understand project governance from participants' perspectives.

Finally, to explore the causal mechanisms driving PRM/ERM integration, I followed Easton's guidance on using both deductive and inductive analyses, supported by Template Analysis, the analytical approach used in this study (See section 3.5). For example, I used IRM's criteria for successful risk culture as a deductive framework, while inductive analysis of governance structures explored specific roles and practices, iteratively revealing underlying mechanisms. This retroductive approach deepened understanding of each case's unique practices and causal dynamics.

Now I turn to introduce the background of each of the three case studies and the sampling strategies used for each. A detailed presentation of each company's risk management system is provided in the Findings and Discussions chapter under the second theme.

3.3.3 Case study background and sampling strategy

The selection of case studies was guided by Easton's (2010) critical realist case study methodology, which prioritises the investigation of underlying mechanisms and causal powers that explain observable organisational phenomena. This study adopts a theoretically informed and purposive sampling strategy to explore variation in how different organisations approach the integration of ERM and PRM. The three cases were chosen because they present contrasting organisational configurations, risk governance models, and level of ERM maturity which enables a richer retroductive analysis of the mechanisms that shape risk perception, decision-making, and integration.

Company A- UK oil subsidiary

Company A is an oil subsidiary of a prominent Indian multinational conglomerate with diversified sectors including steel manufacturing, energy production, and infrastructure development. Operating within the oil and gas sector in the UK, Company A significantly contributes to the supply of transport fuels in north-west England, employing approximately 900 individuals.

Within Company A purposive sampling is well-suited for selecting cases with specific characteristics aligned with the research objectives. In particular when the goal is to gain in-depth insights into complex, contextual phenomena (Patton, 2015; Yin, 2018). By focusing on a subsidiary in the oil sector, this case provides a unique context to examine ERM and PRM integration within a high-risk industry, addressing research questions on how companies adapt risk governance across diverse sectoral contexts. The purposive strategy was facilitated by a referral from my second supervisor's colleague, who recommended it due to its recent challenges with integrating ERM practices. During initial discussions with the former ERM director in the company, he expressed a strong interest in participating in the study, recognising the research's relevance to the company's ongoing integration efforts. Hence, this purposive sampling approach was chosen to ensure that the selected case would provide unique contextual insights into the integration of ERM and PRM.

A longitudinal approach for Company A was taken, with the first interview occurring in October 2021 and the final interview occurring in July 2023. The rationale behind this approach stemmed from the recent establishment of ERM within Company A during the initial interview. At that time, only a small number of employees were familiar with risk management. As per the instructions of the previous ERM director, I was advised to conduct interviews subsequent to each ERM milestone to assess the implementation status, identify any challenges encountered, and evaluate the extent to which employees understood and acknowledged the principles of risk management in general, and ERM in particular. Prior to his departure, the previous ERM director acted as a mediator and facilitated most of the interviews. The current ERM director facilitated the last three interviews. The number of participants in this case study is nine including two ERM directors, a member of the Health and Safety Department, a member from the International Supply and Trading Department, three Project Managers, the Head of IT, and the Head of Legal Department. See Appendix A.1 for more demographical information about each participant.

Company B- project- based company (Saudi Arabia)

Company B was the last accessed company, established in 2017, stands as one of the globe's most developers, wholly owned by the Public Investment Fund (PIF) of Saudi Arabia. The company operates two groundbreaking projects within the country, both responsible and regenerative tourism destinations. These projects aspire to elevate Saudi Arabia’s luxury tourism sector and sustainability initiatives. Therefore, I was keen to explore the integration from such a unique project-based company within a dynamic sector like tourism and hospitality, offering a unique risk governance structure.

Within Company B, a similar sampling strategy was used as mentioned for Company A. Access to the company was facilitated by a colleague, a former project manager, who introduced me to a senior risk manager. The senior risk manager then arranged a formal meeting with the legal team to understand the kind of information I would need, after which I shared the research questions, and an NDA was signed.

The number of employees at the time I collected the data in 2022 ranged between 900-1000 employees. A total of twelve participants were interviewed, comprising the Risk Executive Director of Governance Risk and Compliance (GRC), the Director of Resilience, the Director of

Project Risk at the Delivery Level, the Director of Project Risk at the GRC Level, two Senior Risk Managers from GRC, the Risk Champion from the Marketing Department, the Risk Champion from the Change Management Department, three Project Managers, and a member from the Resilience Department. See Appendix A.2 for more demographical information about each participant.

Unlike Company A, in Companies B and C, the data was collected from February 2022 to May 2022. The snowball sampling technique was implemented subsequent to the utilisation of purposive sampling, which involves the selection of samples based on the researcher's discretion, owing to its prevalence in case study research and appropriateness for a limited number of samples (Neuman, 2014).

Company C- Petrochemical (Saudi Arabia)

The company functions through three Strategic Business Units – Petrochemicals, Agri-Nutrients, and Specialties – alongside a standalone organisation, Metals. The company aids its customers by recognising and cultivating opportunities in pivotal end markets, including but not limited to construction, medical devices, packaging, agri-nutrients, electrical and electronics, transportation, and clean energy. The number of employees exceeded 30 thousand by the time I conducted the interviews in 2022, operating in over 50 countries.

This company was purposively selected for its extensive experience with ERM, established in 2004. Access was obtained through a formal process initiated by an email from my primary supervisor, requesting permission for data collection on risk management. The approval process, which took approximately six months, involved reviews by the education department (responsible for research requests), risk-related departments, and senior management at the executive level. As part of this process, the research questions were reviewed, and upon approval, an NDA was signed.

As explained in the case study design, I was targeting ERM and PRM members, and employees who have risk management duties from other functions. Then, members of compliance and manufacturing functions in Company C were included through snowballing to capture their perspectives. In Company C, a total of 13 participants were interviewed, including the General Manager of risk management, two ERM Directors, two Senior Managers at ERM, six Project

Managers, an ERM specialist in PRM, and a member of the Compliance team. Appendix A.3 provides more information about the demographical information of this sample.

Now I turn to discuss the data collection methods. Table 3.1 summarises the total population of all three companies altogether, while specific details of each case study sample can be found in Appendix A. Please note that the number of interviews exceeds the number of participants because I interviewed the previous ERM director in Company A four times and the current ERM director two times to capture updates on the company's new ERM establishment. In Company C, I interviewed the previous ERM director twice- one related to his experience in the field overall and the second was for the scope of ERM/PRM integration in his company. Two experts in the field were interviewed prior to conducting the study to further formalise myself about the issue of the ERM/PRM integration. Most of the interviews lasted for about 45 minutes, although a few exceeded one hour.

Table 3.1: A Summary of the Research Population

Total Number of Participants	Total Number of Interviews	Total Number of Males	Total Number of Females	Average Work Experience in the Current Positions by Year	Number of Executives and Directors of Risk Management	Number of Participants from Different Departments other than ERM and Projects	Number of Project Professionals	Number of Senior Managers in Risk Positions
34	41	28	5	4.34	9	8	12	5

3.4 Data collection methods and analysis

In accordance with Easton case study design approach guiding this study (3.3.2) the primary data collection methods for this study are semi-structured interviews supported by documentary analysis.

3.4.1 Semi-structured interviews

Critical realists believe that other perspectives are required to understand the nature of a certain phenomenon (Sayer, 1997). A realist interview is a substantial tool for data collection in that CR is the primary source for identifying and anticipating the generative mechanisms in a particular context (Connelly, 2001). Bryman (2016) contended that one of the values of qualitative interview research is the capability to add any needed details or missing information during or even after data collection, aiding the researcher in achieving the research aim. Therefore, I use semi-structured interviews because it is flexible in that I can move from one question to another or even create new questions depending on the information given by interviewees to make sure all information needed for the issue of ERM/PRM can be covered. In addition, I build on Karim's (2015) use of semi-structured interviews to address the lack of comparative PRM research across industries, by adopting the same method with participants in the oil, petrochemical, and tourism sectors. This approach enables a contextual exploration of PRM practices, offering insights that respond directly to Karim's identified cross-industry PRM research gap.

The process can be summarised into four stages starting with effective thematising, designing, arriving at interviewing and transcribing. Each stage offers a structured, iterative method that aligns well with the study's aim of exploring the complex integration of ERM and PRM in medium, large, multi-sectoral organisations.

Thematising

This preparatory stage involves arranging interviews before they take place. This stage includes the development of interview skills, which I have acquired through the qualitative method module, which is part of the compulsory research training delivered by the Faculty of Humanities and Social Sciences at Newcastle University. In the course, I gained knowledge about the many types of interviews, one of which was the semi-structured interview, which I

ultimately decided to use as the primary technique of data collecting since it is appropriate to use while doing research that adheres to a certain research paradigm. According to Mason (1996, p.40), "You are likely to be making certain kinds of epistemological assumptions about the interaction between yourself as the researcher and those you are researching, which suggest to you that semi-structured interviewing is appropriate."

The process of thematising encompasses the objective of conducting interviews, which is to comprehend the underlying reasons and explore potential strategies for the integration between PRM and ERM. Moreover, as Brinkmann & Kvale (2018) have pointed out, acquiring familiarity with the subject matter of a research inquiry is not limited to the perusal of literature and theoretical analyses. Regarding my professional experience, I have previously been employed in the field of ERM and have engaged in communication with experts in the realm of risk management. The identification of the disparity between ERM/PRM was initiated by engaging with risk management experts who encounter this challenge in their daily professional practice. In this stage, I interviewed two ERM professionals to draw on their insights about the research problem, one of them facilitated access to company A. Subsequently, a comprehensive exploration of the gap was conducted through an extensive review of relevant literature and theoretical frameworks as per the previous chapter of literature review.

Designing

The process of designing my interviews involves the creation of an interview guide, which comprises a factsheet that provides essential details such as the date and time of the interview and some demographic information about the participants. Additionally, informed by Guion et al. (2011), my interview guide includes a set of questions, and a comment sheet that facilitates notetaking during the interview (see Appendix B). In addition, the process encompasses the preparation of both the sample and questions. Conducting interviews with all employees in each of the case studies presents a challenging task. The task at hand required me to carefully select a representative sample that accurately reflects the entire population while being mindful of potential threats to the validity and reliability of the study. To ascertain the participants, an initial meeting was conducted with the directors of ERM in companies A and C, as well as a senior manager at Governance Risk and Compliance (GRC) from company B. During the meeting, I clarified the research objectives and shared the research questions.

Following this, the attendees were convinced of the research's value and subsequently engaged in snowball sampling to identify suitable participants. Consequently, the ERM directors and the senior manager of the GRC facilitated my access to most of the participants for the interviews, while a few were contacted through recommendations from other participants. While acknowledging the potential for sample bias, the research questions serve as a valuable mechanism to mitigate the issue by asking the participants about their own perceptions and experiences. In addition, my analysis of the organisational documents aids a comparison between the participants' opinions and the content of the documents.

Interviewing

The process of interviewing includes giving a brief introduction about the topic, background about me as a researcher, obtaining permission from interviewees to do the recording, and stating the values of the research outcome to all relevant stakeholders (e.g., sharing the participants the best practices from the research findings). The interviews were conducted through a combination of in-person interviews and virtual interviews using Microsoft Teams software. In-person interviews allowed for a deeper connection through observing body language and facial expressions. However, they required more time for scheduling and travel. Virtual interviews via Microsoft Teams offered convenience and saved time but were limited by reduced ability to observe non-verbal cues. Combining both methods allowed for flexibility in participation while ensuring comprehensive data collection. Most of the participants showed a willingness to have their interviews recorded. Nevertheless, a subset of participants associated with Company C refused to record their interviews. Consequently, I took notes and encountered challenges in transcribing verbatim the statements made by those participants. To ensure comprehensive transcriptions of Company C's interviews, I conducted in-person interviews with the relevant participants during my 16-hour visits to the company, wherein I sought to clarify any ambiguities and supplement any missing details. Appendix C shows a structured approach designed to develop and align interview questions closely with the research questions, guided by Alvesson and Sandberg (2013) p.15.

After completing the interviews, the next step was transcribing, which, as per Brinkmann and Kvale (2018), involves converting recorded spoken content into written text. In this study, the transcription was initially done manually, which was although time-consuming, allowed me to closely familiarise myself with the data, informing the first process of the analysis as suggested

by King et al., (2017). This will be discussed following the data collection methods (section 3.5.3). To ensure no critical information was missed, a randomised selection of nine interviews (three from each case study) was also transcribed using the Otter.AI platform for comparison. Subsequently, I reviewed the automated transcripts and conducted another analysis to ensure accuracy. This second analysis confirmed that no new codes or themes (section 3.5) emerged beyond those already identified in the initial manual transcription.

Now, I discuss the second data collection method.

3.4.2 Documentary analysis

Documentary analysis is a systematic process for reviewing or evaluating documents, serving as a qualitative method, specifically for case study research (Bowen, 2009). It acts as significant supporting evidence for the primary research methods, improving the quality and reliability of the research (Yin, 1984; Elhoush, 2017). In other words, it is used in combination with other research methods as a means of triangulation, thereby strengthening research validity (Denzin, 2017).

Bowen (2009) suggests five specific uses for documents in research: providing contextual information, generating new questions, tracking changes, supplementing data, and finally, verifying the findings. In this thesis, I used three of such rationales, and in most cases the same document was used as contextual information and as a supplementary data for interviews. For example, I used organisational structures and risk governance structures (Document 1 in Table 3.2) to contextualise the data generated from the interviews clarifying each case's roles, responsibilities, and risk governance scope, aiding understanding the environment in which ERM/PRM operates. At the same time Document 1 was used as a supplementary data by detailing organisational risk management role, offering color-coded risk classifications (high-red, medium-yellow, green-low) that the responsible party at each level deal with. All of which were not provided by the participants.

As per Bowen (2009), the use of documents as contextual information aids in understanding interview data by situating a contextual background. On the other hand, the use of documents as a supplementary data provides extra details that support the primary research data (Bowen, 2009). In addition, the third purpose, verifying the findings is also used. For example, document 8 corroborated some participants' opinions on the current practice of risk

management in Company A, in which the document provided overreaching assessment about the existing risk management maturity.

Table 3.2 provides more information about each document, describing each document and explaining the purpose for using it. The selection of documents was based on three factors. First, the quality of the document, in which the document is assessed against subjectivity and bias. Second, the relevance of the document to the research scope. Third, the availability of the documents in the case studies.

Table 3.2: Selected Documents for Analysis

Document Number	Document Type	Description	Rationale for Use	Company
1	Organisational Structure/Risk Governance Structure	Shows how the organisation operates, outlining the reporting lines between its functions	To see where risk function is placed within the hierarchy, and explore different risk governance structures	A B C
2	Project Assurance Plan	A document that records project assurance activities to make sure doing the project right	To understand how risk is placed and managed within the project process	A
3	Risk Registers	Contain many elements including, the type of risk, risk description, its probability and impact.	To compare with the risk registers in the literature, and assess their suitability for the integration	A C
4	ERM Knowledge Sharing: Risk Management Framework	The risk management framework of Company C is very comprehensive covering risk management infrastructure (e.g., risk classifications & definitions, and risk matrix), risk management process, risk management integration including integration with projects, and risk management assessment approaches.	To understand what standard they use and how they tailor it. In addition, to understand how the company integrate projects into ERM	C
5	The Cycle of PRM and ERM Delivery	Shows how projects and ERM engage in four levels: project and program, phase, enterprise, and finally strategic	To understand the approach for integrating PRM into ERM, determining who should be engaged, defining the roles and responsibilities, outlining the purpose and the output of each level	B

6	Corporate Operational and ERM Reporting Model	Shows how different departments and ERM engage in four levels: departmental, vertical, enterprise, and finally strategic	To understand how different departments engage with projects	B
7	ERM Framework	The ERMF sets out the process for managing risks which covers Risk Identification, Risk Measurement, Risk Management, Risk Monitoring and Risk Reporting	To evaluate A set of components that provides the foundation and organisational arrangements for designing, implementing, monitoring, reviewing, and continually improving risk management throughout the organisation.	A
8	Existing Risk Communication & Reporting	Describe the current practice of risk management in terms of process and reporting	To assess the current state of the risk management practice	A
9	Annual Reports	A comprehensive document that presents in detail a company's annual performance in terms of finance operations, strategies, and other aspects including risk management	To evaluate the risk management report and understand the corporate governance guidelines	A C
10	Three lines of defence model	Illustrates the three lines of defence of an organisation. The first line is internal controls that include functions and departments on the low level of the organisational structure. Then, risk management as a supportive management in the second line, and internal audit in the third line. It also explains their reporting lines with senior managers and governing bodies	To understand how the company differentiate risk from internal audit	B

3.5 Data analysis

Following the data collection is data analysis in which I discuss next the type of analysis I used (Template analysis), the rationale for using it, the analysis steps, and the quality check I employed. The findings are presented in relation to the research questions and the relevant theoretical perspective as guided by Gioia et al. (2013) (See Figure 3.2).

3.5.1 Understanding Template Analysis

Template analysis (TA) arose as a general technique within the larger tradition of Thematic Analysis, particularly among approaches that place a high focus on research in real-world situations (Brooks & King, 2016). TA, as a type of qualitative data analysis, aims to balance flexibility with structure in how it treats textual data. The iterative process employed during the creation of the initial template involves the application, modification, and reapplication of the template (Figure 3.1). This process provides a framework for the analysis and, if executed correctly, ensures that the complexities of the data are not overlooked and that unclear themes are eliminated (Clements, 2022).

3.5.2 Consideration of Other Methods/Methodologies and Rationale for Using TA

Alternative analytical approaches were rejected for different reasons. For example, I deemed Thematic Analysis unsuitable due to its deferred identification of themes until the later stages of the analytical process (Brooks & King, 2016). However, in this study, some themes such as Bridging the Gap Between ERM and PRM Perceptions already existed prior to the analysis process. This makes grounded theory (Gioia et al., 2013) also unsuitable for this study as it is primarily intended for phenomena with limited knowledge. On the contrary, I rejected Interpretative Analysis due to its reliance on the participants' data for the development of codes, rather than pre-existing theories or literature that had been previously identified such as the identification of CAS as an explanatory theory. As a means of reaching a mutually agreeable solution, the TA has authorised the incorporation of a priori (Deductive Theme) "Bridging the Gap Between ERM and PRM Perceptions" which is established prior to the analytical process, alongside the inductive themes that are identified through the analytical process. This makes it well-suited for this thesis because it combines structure with flexibility,

allowing for initial themes based on theory, like CAS, while adapting as new insights emerge. This approach helps capture the complexities of integrating PRM and ERM for improved decision-making and value creation, accommodating diverse organisational perspectives effectively.

3.5.3 Analysis steps

The interviews were analysed according to the process outlined by (King et al., 2018), Figure 3.1 offers a visual representation diagram illustrating this process. In line with this, the interviews were transcribed verbatim. This study incorporated the definition of themes as proposed by Brooks and King (2014), wherein themes are regarded as recurring elements in the perspectives or experiences of participants that are deemed relevant to the research questions (See examples in the clustering stage). The process of identifying themes in participant data and indexing them using names is commonly referred to as coding. The themes and codes utilised in the analysis of all three case studies were determined in accordance with these respective definitions. Figure 3.1 depicts the flexible steps of TA.

Figure 3.1: Template Analysis Diagram (King et al., 2017, P.26)

As an initial step to familiarise myself with the data, I have carefully transcribed and thoroughly reviewed the first four interviews of Company A that is A1, A2, A3, and A4, and the first two interviews of Companies B and C, which are B1, B2, C1, C2 for two reasons. First, due to the longitudinal approach adopted by company A, there was a time gap between each set of interviews in that the initial six interviews were conducted between October 2021 and February 2022, while the final three interviews took place between June and July 2023 (in between, I met the previous ERM director in Company A three times to capture any update). Therefore, it was unwise not to start the analyses as PhD has a limited deadline. Second, as King et al., (2017) recommend at this early stage reading all the transcripts at once before proceeding to the subsequent step only if the number of interviews is small (ten or fewer hours). Given that this study involved more than 10 participants, I followed their suggestion

to re-read this subset of the eight transcripts. This involves a mix of roles, spanning from top management levels such as executives and ERM directors to those at micro-organisational positions such as project managers. This ensures heterogeneity among them as emphasised by King et al., (2017) to avoid challenges in applying the initial template to subsequent data.

Next, the preliminary coding phase, in which I read through the chosen subset, and took notes of what stood out to me as particularly interesting or relevant to my research questions. To facilitate the identification of preliminary coding, I used a priori themes which are according to Brooks & King (2014), typically identified when a research project is initiated with the premise that specific elements of the research questions under investigation should be the primary focus of the study. They distinguish between two kinds of a priori themes; soft and hard a priori themes, wherein the former are more loosely defined and often broader than hard ones. I sought for evidence that corresponds to tentative soft a priori themes that I had already specified in advance either theoretically or in terms of the practical implications of my research. Hence, examining the PRM and ERM risk culture from the CAS perspective and the IRM's risk culture framework generated *Risk Culture* as a tentative priori theme to investigates its role on the integration of PRM/ERM. Similarly, the literature revealed two risk perspectives: objective like PRM, and subjective such as ERM[6]. Thus, I identified *Bridging the Gap Between ERM and PRM Perceptions* as a tentative soft a priori theme to explore how project managers and ERM members conceptualise risk and whether their perceptions influence the integration. Table 3.3 below explains the two tentative themes.

Table 3.3: A Priori Themes

Tentative Themes	Description/Theory
Bridging the Gap Between ERM and PRM Perceptions	This theme explores the theoretical and practical differences between PRM and ERM, particularly their varying perceptions of risk. PRM typically emphasises the objective, quantifiable risks associated with individual projects, focusing on time, cost, and quality (Agarwal & Virine, 2019), while ERM adopts a broader, subjective view that accounts for strategic, operational, and organisational objectives (Liu et al., 2013).

[6] Both tentative themes were informed by the literature Sections: 2.1.2 and 2.2.4

	Complexity theory informs this theme by highlighting the non-linear, dynamic nature of interactions between these two risk agendas. The integration of PRM into ERM requires organisations to steer sociopolitical complexities and differing perceptions of risk (Millo & MacKenzie, 2009).
Risk Culture	CAS theory informs IRM's risk culture criteria by emphasising adaptivity, openness, and continuous learning within the organisation. This approach promotes a dynamic, flexible culture where risk knowledge is shared through both bottom-up and top-down strategies, encouraging diverse perspectives and fostering an environment where employees can continuously learn and adapt to emerging risks. This adaptive risk culture framework supports the thesis aim of integrating PRM into ERM, bridging diverse risk perceptions and practice to create a unified and adaptive risk management

During the clustering process, each cluster consists of a theme and its relevant codes supporting it. For example, the codes detected from participants' definitions of risk support the Bridging the Gap Between ERM and PRM Perceptions theme and answer the research question of how different employees define risk (Figure 3.2). Twenty-two codes arose from the analysis of the first eight interviews, integrating the priori themes with the emerging themes into seven meaningful clusters (See Appendix D). Clustering was first performed manually with "sticky notes" standing in to symbolize the participants and highlighters outlining the codes so that connections could be made by eye. Then, I transferred the clusters to a Word document, wherein I attached the quotes supporting each code before transferring them to NVivo 12 (QSR, 2022) Software for a better visual representation of the clusters, which was available for use through Newcastle University.

Subsequently, the initial template was developed using the clustering method and sent to the supervisory team for their review. I took their feedback into account when repeating the

process with new subsets. Therefore, during the subsequent stage (applying and developing the template), a comprehensive analysis of all subsets (five subsets) which were recorded for quality assurance (Section 3.5.4.2) was conducted. An iterative process was employed, involving revisions such as modifications and emergence or deletion of themes based on new data. The final template (Appendix E), which addresses all research questions (Figure 3.2), serves as the foundation for interpretation and provides a clear structure for the write-up of findings and discussion, as outlined in Chapter Four.

Following King et al., (2017) guidance on template analysis regarding ensuring the quality and rigor of this analysis was essential to maintain trustworthiness in qualitative findings.

3.5.4 Quality check

King et al., (2017) suggest four procedures for quality checking in template analysis. These include independent coding, respondent feedback, keeping an audit trail, and thick description and use of participant quotes. Two of which were used in this study as follows.

3.5.4.1 Independent coding

King et al. (2017, p. 41) recommend, “You may use fellow students, your supervisors, or a panel of people to do this.” A fellow student with experience in template analysis assisted by reviewing and confirming the process of my chosen a priori themes. Additionally, the supervisory team played a crucial role by providing feedback on the templates, asking for more clarity when naming certain codes, and requiring justification for merging or removing others.

3.5.4.2 Audit Trail

King et al. (2017) describes an audit trail as a record documenting the development of the analysis. To this end, I maintained five versions of the template throughout the process, providing a transparent record of its evolution and supporting the validity of the final template. Each version reflects the iterative adjustments made based on emerging data and supervisory feedback. This audit trail not only offers a clear timeline of the template’s progression but also ensures the traceability of decisions and refinements made during the analysis process, enhancing the study's overall credibility and rigor.

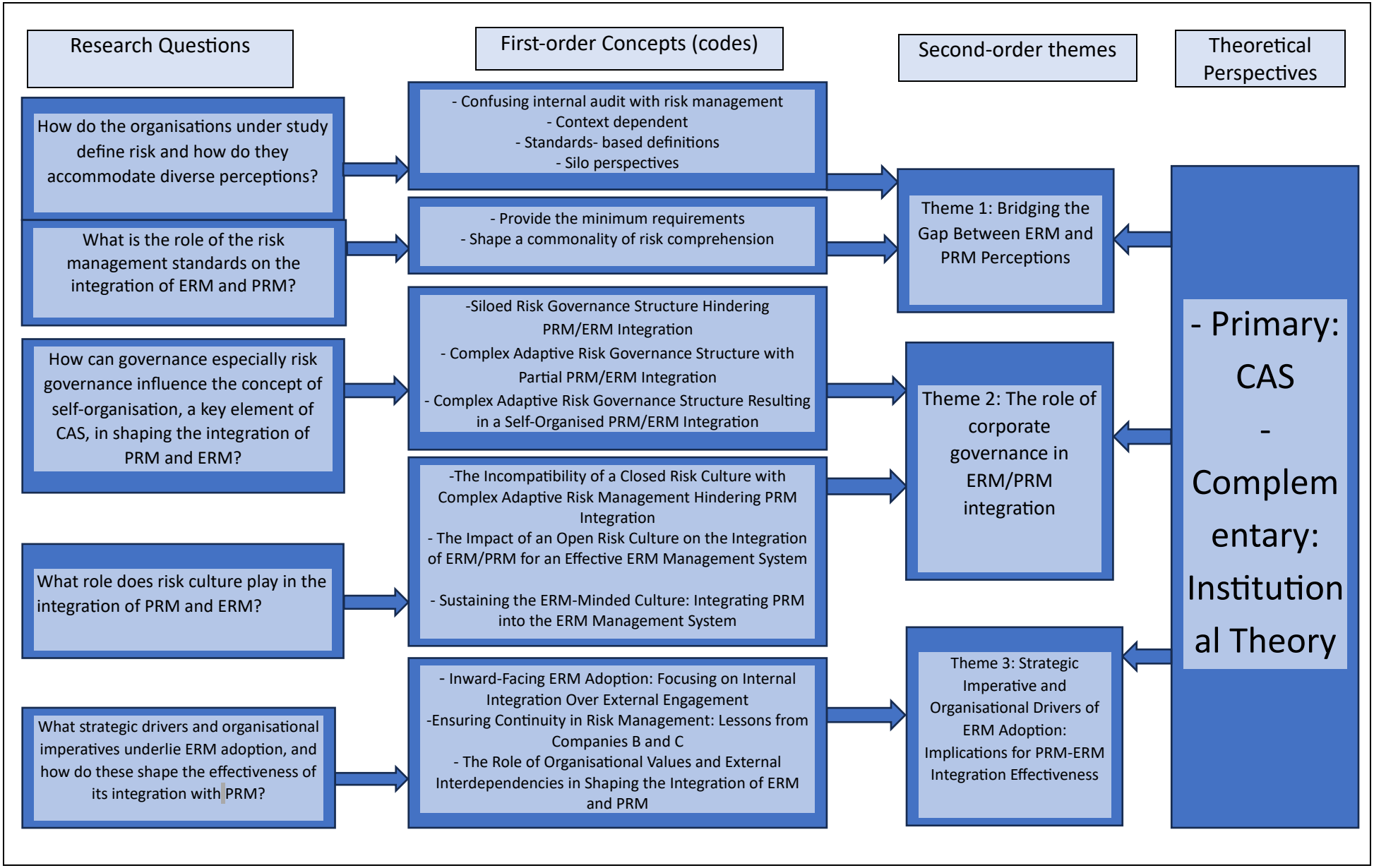


Figure 3.2: Data structure for the semi-structured interviews guided by the approach of Gioia et al. (2013)

3.6 Methodological Rigor

One of the most widely recognised criteria for establishing trustworthiness is Guba's (1981) framework, which includes credibility, transferability, dependability, and confirmability, which are applied in this qualitative study.

3.6.1 Credibility

Credibility can be viewed as the equivalent to internal validity for quantitative approaches. First, triangulation, entails collecting data from a variety of perspectives using a variety of methods (Guba, 1981). In this study, triangulation involved gathering data from multiple perspectives ranging from low-level employees to top management across various industries including oil, petrochemical, and tourism and hospitality. To meet the requirements of CR in uncovering the reality of ERM/PRM integration, I compared and contrasted the participants' perspectives with an analysis of the relevant organisational documents (Table 3.3). On some occasions, follow-up interviews with participants were necessary to ensure the accuracy and depth of understanding of the data collected. Second, TA was chosen for the analysis because it was the most appropriate method (see section 3.4.4.2). In addition, to ensure that the interview questions were aligned with current understandings of ERM/PRM, I engaged in reflexive practice by continuously reviewing the literature on ERM/PRM integration during the interview period and updating the research questions accordingly. For example, the most recent ERM literature has highlighted knowledge sharing as a fundamental building block for integrating ERM into organisational levels (See for example (Fraser et al., 2022a)). Consequently, knowledge sharing became a major focus in the subsequent interviews.

3.6.2 Transferability

Given that the study's findings are specific to certain organisational contexts, it is unwise to claim their direct applicability to other organisational settings. The three case studies were purposively selected to capture diverse ERM/PRM engagement approaches within multiple organisational contexts. This sample involves a project-based company, a subsidiary, and a large corporation, along with diverse participants' roles and experiences to maximise the findings. The thick description of each context in the findings and discussion chapter allows

the reader to assess the degree of transferability of the findings to other settings (Guba & Lincoln, 1982).

3.6.3 Dependability

To aid dependability, I used multiple case studies with different data collection methods, which allowed in depth data collection leading to triangulation and thick description. Five pilot interviews were conducted before the start of the study for different reasons. Three of them were with colleagues from different backgrounds including supply chain, corporate social responsibility, and digital economy to ensure the flow of the questions was consistent and meaningful, and to estimate the duration of each interview. The remaining two pilot interviews were conducted with risk professionals as explained in section 3.4.1 to familiarise myself with the ERM/PRM issue.

3.6.4 Confirmability

For confirmability, I use the audit trail as explained in section 3.5.4.2.

3.7 Ethical Consideration

Full ethical approval from the university to conduct the study was received in December 2020. The information provided in the interviews was held anonymously and confirmed to Newcastle's Data Management Policy to ensure no possibility to trace information or comments back to individual contributors. Pseudonyms are used to protect all identities in the study and information are stored in accordance with the current GDPR (2018) Regulations for Data Protection and the University's internal protocols: http://research.ncl.ac.uk/rdm/beforeaproject/expectations/Research%20Data%20Management%20Policy%20Principles%20Code%20of%20Good%20Practice.pdf. A formal confidentiality agreement has been signed before the study started (see Appendix F).

In accordance with Newcastle University's ethical approval, data collected from the interviews was stored securely under my student's account on the university's server. No other person apart from myself had access to the interview data. All interviews will be retained for the duration of my PhD project. After the data is transcribed, coded and analysed, data will remain on the server until after the viva and will be permanently deleted afterward. This process was clearly communicated to all participants. Furthermore, I followed data management

guidelines in accordance with Newcastle University's suggested plan for researchers. In addition, I continuously reminded the participants that participation in the study is entirely voluntary, and they are free to withdraw from the interview at any time without giving a reason. Participants were also allowed to ask questions at any time and refuse to answer any questions as they wished and discuss any concerns with me (see Appendix G). For example, some participants chose not to answer the question of risk perception as reflected in the number of participants included in the first theme as they believed the question was too simple for them (see Findings and Discussion).

Due to ethical and organisational access constraints, the study was limited to interviews and documentary analysis. The participating companies did not permit observational access to risk-related practices or workshops. This ethical boundary influenced the research design by limiting opportunities to validate cultural aspects of risk through direct observation. These limitations and their impact on the research design and findings are critically discussed in Section 5.5.

3.8 Conclusion

To conclude, this research stems from a critical realism perspective, adopting three case studies supported by semi-structured interviews and documentary analysis. Semi-structured interviews are flexible, in the sense they enable the interviewer to collect more in-depth information going back and forth to the questions or even creating new questions, which by the support of documentary analysis can delve into the three levels of reality claimed by critical realists (empirical, actual, and real). Data collected from case studies B and C were in a cross-sectional time horizon over a period of three months, while it took about two years in case study A . CR proved to be a good fit for the template analysis adopted in this study. The iterative process of TA, which involves moving back and forth through different layers of understanding, aligns well with the critical realist approach to exploring the underlying causes of ERM/PRM integration. This process began with deductive a priori themes, which were tested against data, literature and theory. Emergent themes were then identified through the analysis process, and these were revisited to determine whether there was sufficient evidence to retain, dismiss, or reclassify the original a priori themes as sub-themes.

The priori and emergent themes are presented and analysed in the next chapter.

Chapter Four: Findings and Discussion

This chapter presents and analyses the findings of the collected data. As presented in Figure 3.2, the findings are grouped into three main themes. The first theme, *Bridging the Gap between ERM and PRM Perception* addresses the first research question about how companies under study define risk, explaining the role of the risk management standards in shaping employees' perceptions of risk.

The second theme explores *the Role of Corporate Governance*, answering the second and the third research questions: (1) how can governance, especially risk governance, influence the concept of self-organisation, a key element of CAS, in shaping the integration of PRM and ERM? (2) What role does risk culture play in the integration of PRM and ERM? Finally, the last theme addresses the emergent question: What strategic drivers and organisational imperatives underlie ERM adoption, and how do these shape the effectiveness of its integration with PRM?

4.1 Bridging the Gap Between ERM and PRM Perceptions

To understand how the organisations under study define and manage risk, as well as assessing the extent to which employees in the different departments have common or varying perceptions of risk and risk management, 16 participants were asked to define risk. Although some participants as explained in Section 3.4.5 (Methodology Chapter) chose not to answer due to the simplicity of the question, I concentrated on a sample of employees from different departments (11 participants) to check if there is a commonality between their definitions as this is key for the ERM integration through the lens of CAS theory. In complex systems, everything is interconnected and interdependent, failure to see the interconnectedness can cause ignorance and linear thinking (Emblemsvåg, 2020). The remaining five participants were from top risk management positions such as ERM directors and Executive Directors to ensure top-level perceptions are not missed.

Starting with the confusion between risk and internal audit which according to Participants B1 (a senior manager at GRC) and B2 (The Executive Risk Director) already exists in company B. This forms the first sub-theme, which was only experienced in Company B.

4.1.1 Distinguishing Internal Audit from Risk Management

When Company B started its risk management journey in 2020, it struggled with some employees confusing the perception of internal audit with risk management. In the following two quotations, Participant B2 highlights the issue of such perception and explains how providing risk awareness sessions, trust and understanding risk management through The Three Lines of Defence Model (See Figure 4.1) as a supportive function helped differentiate the two functions.

> *"Despite all the awareness and the risk culture enhancement that we have been working on, some departments still think risks are related to an internal audit, while others think you will report them to the boards. Some departments think you are the resilience function. It is all about perception and the solution is first, to keep delivering the awareness and remind them that this is our structure, and this this how we do it, today I am a management function. Second, which is the most important thing is trust, and by this I mean if the department trusts that you are not going to take their risks and disseminate them in front of the boards, they will start to be more transparent with you…"* (Participant B2).

> *"So you have to make a balance between aligning with management because by the definition of The Three Lines of Defence (Figure 4.1), you are a management function meaning you are supposed to support management, align with these departments, and agree with them on what to share with the internal audit and the boards without making risk misreport. This is the most difficult piece of work in risk management. And from my long experience in risk management, I can tell you that the thing that can make them trust you is that you help them solve their issues. So, risk management is now advisory for the business, it is not just going to these departments and asking them what risks are you having and then registering them and reporting them. Instead, we work with them to reduce their risks by providing our experiences"* (Participant B2).

The participant proposed two approaches to address the confusion between risk management and internal audit. The first involves sociopolitical solutions, which focus on engaging and interacting with employees. A large complex system such as risk management is governed by behavioural rules such as norms, values, and beliefs (Argyris and Schön 1997) that shape the perception of risk. A CAS posits it is through the nature of interaction that these

behavioural rules can be transferred to different agents (e.g., the departments in which those employees work).

Another sociopolitical strategy suggested by the participant to enhance risk perception and further distinguish it from internal audit is through trust. The literature on trust in risk perception and risk management explores its critical role in shaping risk perception (Siegrist, 2021; Earle, 2010). In particular, the development of the Trust Confidence Cooperation (TCC Model) which these two authors developed is relevant to this context. According to the authors, trust is related to social relations or shared values that represent good intentions to the trusting person. In the context of Company B as explained by Participant B2, trust in risk perception is gained when employees trust that the risk management function will not report their risks to the board; instead helping them to identify and manage their risks. The same perception is adopted in Company C; for example, the previous ERM director when explaining the role of the ERM department states:

> "*It is wrong to think that your job is facilitating only, you need to study their objectives (referring to functions and departments) and due diligence. Get them to see the value of ERM, otherwise it will be a burden"* (Participant C1).

While trust is concerned with intention, confidence is concerned with the ability related to past performance, factual knowledge, and established rules and regulations (Siegrist, 2021; Earle, 2010). This suggests a more structural rather than a relational strategy to increase employees' confidence in the risk management system. In the context of Company B, the structural strategy raised by Participant B2 is to distinguish risk management from internal audit through the Three Lines of Defence. The Organisational Governance Document (Document 1) provided by Company B shows the different roles of the two functions adopted from The Institute of Internal Auditors, IIA (2013) (See Figure 4.1).

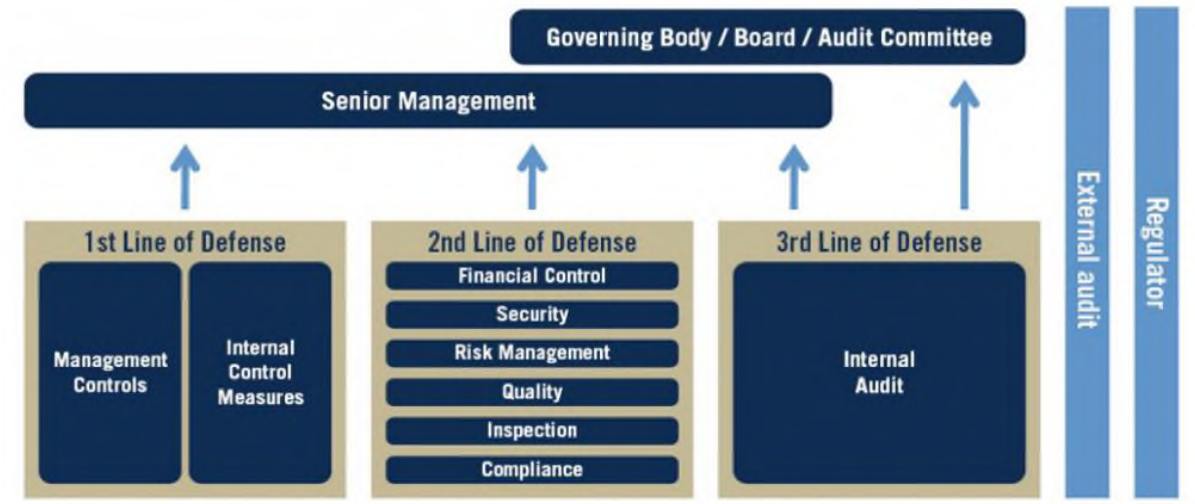


Figure 4.1: The Original Three Lines of Defence Model (IIA, 2013)

According to the model, risk management serves as the second line of defence for any organisation after operations, the first line of defence which implement controls and suggested treatment plans, and before the internal audit, the third line of defence which periodically reviews controls, procedures, and the outcome of the risk management activities to provide objective and independent confirmation of the effectiveness of the procedures and controls applied in the organisation. It should be noted that the IIA updated the model in 2020 to reproduce the evolving role of risk management and to foster better collaboration between corporate functions (See Figure 4.2). The original model shows only the internal audit can report directly to the company's governing body, board, or audit committee, while in the new model both management and internal audit report to and receive oversight from the organisation's governing body.

A close look at the three lines of defence adopted by Company B reveals that the model was tailored to combine the two versions (See Appendix H). For example, the directions of the arrows follow the updated version in that both management and internal audit can report and receive insight from the governing body and the board, while the actors under each line of defence shadow the original version except risk management which is modified to ERM. However, the company's model shows the internal audit reports to the senior management but not vice versa. This suggests the internal audit is less complex than risk management as it serves as a reactive process, providing an independent and objective assurance about the effectiveness of risk management and internal controls (Institute of Internal Auditors, 2020). On the other hand, risk management is a proactive process that engages in daily adaptive

iterations of controlling and monitoring aligned with CAS where feedback loops occur when components in the output stage inform the components in the input stage (Sweetman et al., 2014). For example, the organisation's strategy, values, vision, and mission determined at the board level can inform the risk policies and appetite at the management level (ERM), influencing the risk practices at the first- line departments including projects and vice versa.

Risk management operates in a dynamic and interconnected environment where small changes can lead to significant and unpredictable outcomes, embodying the principles of nonlinearity and complex adaptive systems. As Emblemsvåg (2020) reminds us about this interconnectivity in complex systems small changes in one area can lead to significant disruptions in another. This keeps the system far from equilibrium, making risk management is a continuous process of flux and change. Internal audit, while crucial, operates with more predictable and linear interactions, focusing on assessment and assurance rather than continuous, adaptive management of risks. Most importantly as shown in the updated model and outlined by Participant B2 at the beginning of this subtheme, risk management (ERM) now acts as advisory management, providing expertise to help solve departments' issues. This will not occur without activating feedback loops to understand the needs of the first-line departments and the expectations that ERM management has for those departments, including projects.

According to Fraser et al (2022), the role of internal audit functions as an assurance department responsible for raising identified inefficiencies to the board, whereas risk management acts as a supportive function aimed at assisting management in comprehending risks and prioritising actions. This was further emphasised by Participant B1, who concurs with Participant B2 that some employees still confuse risk management with internal audit while observing a gradual improvement in the perception of risk management over the years, as employees increasingly place their trust in the process.

> *"Aside from everyone wanting to help, but there's always because it's a risk, sometimes it does get confused with internal audit. Differentiating yourself from trying to support the department, we're trying to find whatever issues that you have as a department and trying to fix it for the better of the organisation rather than us just writing a report and saying you did something bad. This is like an audit review. This is one of the biggest challenges we have had. And in the last few years when we first started the*

department, our Risk Culture Survey was horrible to be honest. People did not trust because it was the first time doing this thing. We had a lot of people who would push back on the information that we're providing. We had to show them in the next two years that the more information that you give us and the more honest you are with what is happening within your departments, the more we can support you…" (Participant B1).

"So, now we do actual projects when we put mitigations, we are putting very valuable mitigations at a much higher level where we are connecting the department not only within our company to try to fix an actual risk, but we've been going out to actual PIF[7] *and different types of ministries to try to solve a problem that we have internally. So, once we started doing that and departments started noticing that this is what we can do, they felt much more comfortable starting to be highlighting risks. So, within 2022, the way people identify risks to us now is completely different than in 2020"* (Participant B1).

Participant B1 concurs with Participant B2, emphasising that the GRC team continuously motivates employees to share accurate work-related information to help solve their issues and foster trust and transparency. Hence, the company must possess both trust and confidence to influence employee cooperation. Since confidence relates to ability, agents such as Participants B1 and B2 must continuously enhance their knowledge and skills to enhance their ability to assist the first-line departments such as projects in identifying and managing their risks.

[7] PIF stands for the Public Investment Fund which owns Company B

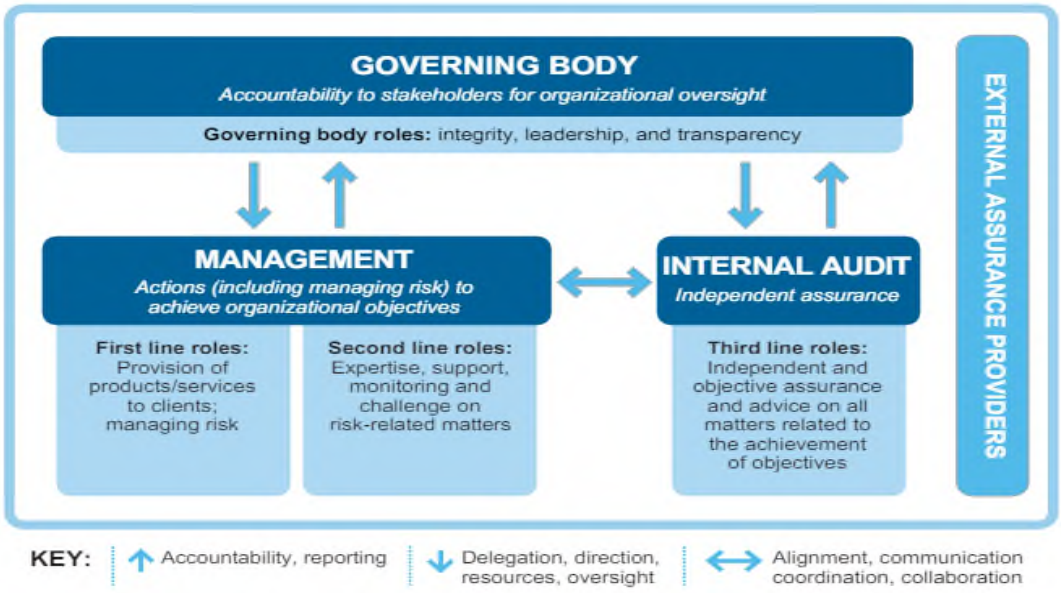


Figure 4.2: The Updated Three Lines of Defence Model (Institute of Internal Auditors, 2020)

This is why Schuett (2023) criticises the updated model (Figure 4.2) for assuming the second line of defence has the required skills and expertise to challenge the practice and controls in the first line. In the second theme, I present the three various risk governance structures of the three case studies, explaining how each company ensures having these necessary skills and expertise in the second line (e.g., ERM) to support the first line (e.g., PRM). For now, it appears that the new risk management perspective as a supportive function to the first-line functions is the causal mechanism that has helped place trust in the employees to distinguish risk management from internal audit because none of the participants I asked experienced confusion between the perceptions of the two functions. Thereby, the findings conceptualising risk management as a supportive role align with the current ERM literature (Qazi & Simsekler, 2021; Fraser et al., 2022).

Participant B6 acknowledges the value of The Three Lines of Defence.

> *"The role of the governance as they (The GRC teams) taught us is the first line of defence, so this is what I teach each function within my department. Specifically, in marketing, we deal with external, we are the image of this company, we deal with the sentiment, so our department is in the face front of any potential risks"* (Participant B6)**.**

Hence, the abductive process employed to investigate the empirical observation, which is the confusion between risk management and internal audit that is observed by Participants B1

and B2 concludes at this level. Now, I move toward presenting the perceptions of risk considering contextual factors that were defined by most participants.

4.1.2 Context- Dependent Definition of Risk

Most participants (10) defined risk in line with the postmodern (see Section 2.1.1) subjective perspective, viewing it as a perception dependent on the specific context of a particular place, time, and conditions. For instance, Participant C4, an ERM senior risk manager with prior experience as a project manager, stated:

> *"One of the beauties of approaching ERM is it is not science, it is a conceptual understanding of the concept of risk, and a lot of human translation of the concept along two main things; time and location determine your definition of risk. I believe that risk is extremely dynamic, we should monitor risk because what is a risk today might not be a risk tomorrow, and a current risk plan might not mitigate the risk in the future but can mitigate it today"* (Participant C4).

Similarly, Participant C7 agrees:

> *"You cannot define risks in one category- we look for the project as a case that depends on the risk category (technology, cost, schedule, marketing, operation, or integral category) so, we set plans accordingly. Some risks we identify during the project life are calculated, you live with, or they can be continued live with you after the project is completed but they are registered and known, and their mitigation strategies are known. So, for us ERM is just one source of risk identification although we look for ERM as an integrated party identifying and keeping monitoring the identified risks"* (Participant C7).

The participants' consideration of time and space when defining risk leans toward openness, co-evolving processes, and emergence, implying that change is always possible. For example, according to Participant C8,

> *"In our risk assessment of a project in Africa, we identified risks related to the location, leading us to change the location of the project. We faced two issues related to building and operation associated with regulations of that government and facilitation with the operations"* (Participant C8).

Therefore, some project managers appreciate the value of ERM input, as it enables them to conduct proper risk assessments. ERM engages with the external environment, gathers relevant knowledge, and integrates it internally. For example, Participant C6 states, “If a project is operating in Africa, ERM involvement is very important to ensure proper mitigation for corruption” (Participant C6). This underscores the perception of risk as context-dependent, implying that if the same project were to operate in a different country, the risk assessment might not necessarily flag corruption as a high concern. Thus, changing the location could significantly alter the project's risk profile and its impact on reputation. This reinforces the view of risk as a complex concept that necessitates interaction across various levels and networks within loosely nested open systems, where outcomes are never predetermined but can be actively influenced (Byrne & Callaghan, 2013). For instance, Participant B5 when asked about his perception of risk explained the layers that risks in his company undergo, which matches the document, Corporate Operational and ERM Reporting Model (Document 6) provided to me by Participant B2 (See Appendix I).

> *“We can divide risks into 3 layers: 1) enterprise-wide risks, the risks which need to be mitigated on priority because they have an impact on the overall enterprise-level organisation; 2) risks that have to be treated at a departmental level, so if I am in the IT department, there is a list of maybe thousands of operations are being executed or monitoring or incident management, service request management, change management, or problem management, or a system development lifecycle or so many other perspectives, so this is our portfolio or technology change management; 3) to manage our risks internally even the risk department is already asking us to provide the risks, which we have identified but on the other side we also try to gather our own input; for example, how we normally do that”* (Participant B5).

Participant B5 demonstrates a comprehensive understanding of risk as a context-dependent concept, perceiving the company as a nested system (Byrne & Callaghan, 2013). This is evident in the way he categorises risks into three distinct levels: enterprise-wide risks, department-level risks, and internal risks. He prioritises enterprise-wide risks, showcasing his grasp of the broader risk landscape. Subsequently, he delves into department-level risks, those associated with agents at the same level, followed by internal risks. Then, he went on to explain the risks from his context as a change manager in more detail.

> *"As a change manager, one of the sources is the change which is going to be implemented into the live environment. So, we identify if we are going to implement a new service, what the lists of the services which are going to be impacted and is it a single point failure solution which we are going to, or you can say is it going to impact what kind of business user? There are 2 types of solutions: 1) the management side; 2) the ones that the business users are using. If the business users are uploading their production data, it's a critical system, but if it is a solution just for the sake of IT department, it's not that critical."* (Participant B5).

Thus, the four participants while carrying different positions, agree on the context-dependent definition of risk. In the context of projects, risks are identified concerning project objectives and the contextual elements that might impact those objectives (Mabelo, 2023). Consequently, brainstorming about threats and opportunities relevant to the current project should stem from its objectives and the factors that could influence them, rather than merely focusing on what could potentially go wrong. Figure 4.3 demonstrates the essential components of the ISO 31000 Risk Management framework, with a notable improvement between the 2009 (the left side) and 2018 (the right side) editions of the standard. In the 2009 edition, the endorsement was for Risk Identification to stalk from the "Base Risk Register" and/or "Specific Contingency," inferring that risk practitioners must obtain risk elements from previous identification attempts as if the present project automatically shared identical or similar objectives and contexts (Mabelo, 2023). However, the example of the project conducted in Africa highlights the limitations of this approach. If the project managers had not engaged with ERM to understand the local regulations and instead relied solely on previous similar project risk assessments, they could have jeopardized one of the company's critical risk thresholds.

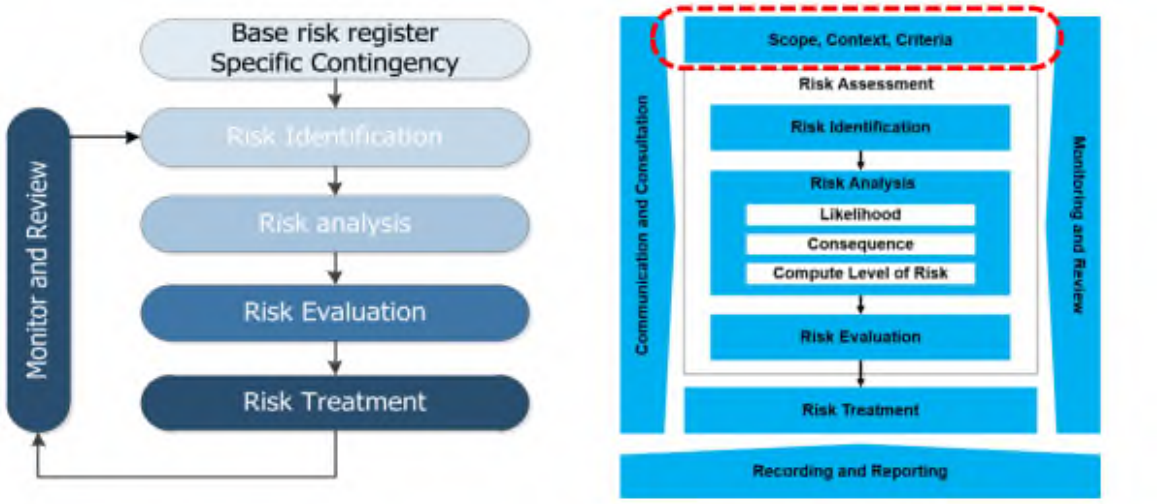


Figure 4.3: ISO 31000, 2009 Version Versus 2018 Version

However, this limitation has been remedied in the 2018 version by introducing considerations such as "Scope and Context" before beginning the Risk Identification Process. In company C, according to document 4, ERM knowledge Sharing, the process that is based on ISO 31000, the company divides the context into external context and internal context. The former is considered based on the PESTL framework, that is Political, Economical, Social, Technological, Environmental, and legal/ Regulatory. The latter is considered based on People, Equipment, Process/Systems. However, the key lies on finding a suitable approach to ensure that risk elements are brainstormed in association with the present scope and context of the event to avoid the inclusion of irrelevant risks (Mabelo, 2023).

Therefore, in the second theme, I discuss in detail the approaches that each of the three case studies applies to brainstorming risks. For now, the participants' perspectives (C4,C6,C7,C8,B5) align with the perspective presented by Alberts (2006), who emphasises the significance of context in explaining the fundamental circumstances, environment, or background in which risk is evaluated, including factors such as time and location. Such a dynamic risk perception is reinforced by the current literature such as Sheth & Sinfield (2024), Andronache et al. (2018), and previously Kerstin et al. (2014). In complexity theory, context is key when defining a risk because it depends on knowledge. And knowledge by definition is information combined with experience, context, interpretation, and reflection (Davenport et al., 1998). Employees with experience in projects such as these participants, possess a unique blend of professional risk management knowledge and personal skills developed from their work in

various functions. As a result, they became familiar with different risk perspectives, so now they can put risk into different contexts.

Because of continuous interactions between different agents such as these project managers, employees in different departments, and ERM members through different feedback loops that include risk workshops, new patterns of relationships and structures emerge. This new emergent structure "risk based on context" is the collective result of the local interactions between those agents, making them self-organised systems. For example, four of the 16 participants defined risk based on their experiences from working in different functions in the company, which included working on projects. The first participant A3 defined risk based on her current role as a Chemical Engineer from Health and Safety Department and from her former position as a project manager:

> *"My perception stands from the process that we have outside that poses to personnel- first of all, people working here and then society. In the UK, the HSE (Health Safety Environment) has a price on life and as our duty of care permits your requirements demonstrate that we have done everything reasonably practicable. It is unacceptable for someone to come to work with a likelihood of becoming injured or dying as a result of their workplace. So, our risk management is more structured around demonstrating to ourselves ethically and morally that we are happy with the place of work, that we are doing everything possible to minimize risk to people and the environment and there is an obligation from governing bodies such as the HSE. But, from my background in projects, I will always do sensitivity analysis in my project development role, especially if it was margin driven if it was growth projects around when a project is not going to payback. So, I think we should look at both perspectives, especially at a high level, it is important for senior management and boards to understand both so they can sort of assess both and prioritize accordingly. Whilst safety should come first"* (Participant A3).

For ERM to identify those different risk perceptions in an integrated way, the company must have previously identified a common language to define risks. Carlile & Rebentisch (2003) call it the syntactic stage, in which the focus is on recognising and classifying risks in a way that the various functions and departments can comprehend and agree upon. Applying Alberts's (2006) elements of risk as discussed in the literature chapter (Section 2.1.3), the context in which risk is identified plays an important role. For example, the context of HSE includes

regulatory and ethical considerations toward people and the environment, while in PRM, it is more about project-specific constraints. The syntactic boundary demands that a shared risk definition, methodology, and terminology are created to ensure all organisational functions and departments can contribute to a coherent risk identification process (Jean-Jules & Vicente, 2021). This means establishing a common language to define risk among the various organisational functions and departments regardless their specific focus. Prior to conducting the study, I have interviewed two risk management professionals to capture their insights about ERM/PRM integration. One of them with over 20 years of experience in ERM, emphases the importance of identifying common aspects of risk within different contexts.

> *"It can work with a common denominator, understanding your dimensions of risks. The risks of a project might be quite different to the other elements of risks across the business. So, unless that denominator of risk is common then it is going to be very difficult for that level of risk to be appreciated"* (Participant RP1).

As Emblemsvåg (2020) highlights, complex systems are characterised by interconnectedness, making it crucial to understand the big picture to maintain the system's interconnectivity. "Thinking about the big picture is therefore to pay great attention to the right details that shape the big picture" (Emblemsvåg, 2020, p.47). Participant C10 who shares a similar role to participant A3, an engineer in one of the factories explained the link between risks coming from his department and their interconnectedness with projects.

> *"When it comes to risk, anything that can affect our objectives, we work interdependently with other departments. Let me give you an example, imagine the thickness of the pipe is 6mm, after 10 years it is reduced to 4mm, I know if it gets to 3mm it will not work. So, I am reaching out to a replacement team, which is a project in this case"* (Participant C10).

The participant first associated risk with the objectives and accordingly, acknowledged the interrelatedness between risk coming from his department and projects impacting the overall objectives. Thereby, it is the understanding of the company's overarching objectives at the enterprise level that allows agents in different departments and functions to visualise interconnected risks. This understanding enables them to identify risks in an integrated manner, taking into account their potential impact on the organisation's objectives. Most of

the participants (A3, B1, B12, B5, C2, C5, C6, C8, C10) defined risk based on objectives, and a close look at these definitions reveals the closeness of their definitions with risk management standards' definitions. I discuss these definitions in the next sub-them.

4.1.2.1. The Role of Standards in Unifying Risk Language

The risk management standards appear to play a crucial role in the syntactic stage, contributing to common dimensions of risk definition which employees from different departments and functions understand and agree upon. Given the significant number of similar definitions related to this subtheme, I will first present all the participants' definitions collectively and then discuss them, rather than citing and analysing each one individually.

Some participants when asked about their perceptions of risk, provided very short definitions. For example, Participant B1 defined risk as "*Any event that can take place and stop you from achieving your goal or objective",* and for Participant B12 risk is: *"Any event if they happen could impact the overall objectives negatively or positively"*. Other participants defined risk in relation to uncertainty; for example, for Participant C2:

> "*Risk is an effect of uncertainty on the objectives. Risk is about threat and opportunity that we have to capture. Risk management is a systematic process of identifying, assisting, managing, and monitoring, as well as reporting risks to top management and board of directors"* (Participant C2).

Another participant (C5) defines risk in general, and then differentiates project risks from organisational risks.

> *"Any uncertainty in your objectives then it becomes a risk. If you look at PMI it is a governing risk management structure; they are not related to organisational risks. They are highlighting how to identify risks related to your projects, how to treat them and how to ensure that your risk is in an acceptable level. Organisational risks management is risk assessment more than project risk management. It is about identifying risks related to your organisation to achieve the objectives. You don't have cost and time to control"* (Participant C5).

Participant C6 thoroughly addresses aspects of risk integration, defining risk and outlining the role of the risk management framework in integrating PRM and ERM as follows:

> *"Any threats or opportunities for any project from achieving objectives. But because the name is PRM does that mean we should have the power to treat risks differently? I think No, we have uniqueness as operational risks (unlike ERM), so we have the right to use specific techniques like PMI methodology (qualitative then quantitative ..etc) no contradiction with ERM or ISO or even COSO, but the intervention occurs in identifying the risk through the framework, the risk register through the framework, reporting through ERM framework, and escalation and closure of the risks are done with coordination with ERM acceptance to see the justification"* (Participant C6).

Looking at these definitions associated with uncertainty matches the ISO 31000's definition, which is "The effect of uncertainty on objectives" (ISO, 2018, p.2). Participant C8 has stated clearly that his definition is based on ISO 31000.

> *"My definition stems from our risk management standards, we use ISO 31000 definition that is uncertainty on objectives. In PRM, we have time and cost, you may have external impacts from regulation, taxation...etc. Once I create the context then I become acquainted with my risk assessment"* (Participant C8).

Company B, according to Participants B2, B1, B12, and B5, is ISO 31000 Risk Management certified, and the company is ISO-certified in other areas, such as IT ISO 28000 and ISO 27001 Information Security Management. For Participant B2,

> *"It's not about a standard; it's about the tailored framework you can implement and utilise. The idea is that you find something that your organisation can utilise. The standard describes the minimum requirement and the required process, but tailoring determines how to report and how to identify the values. However, you wanted certification, so we chose ISO"* (Participant B2).

Participant B12 concurs with Participant B2 that ISO provides minimum requirements, but ultimately the process is similar. He continues, "The quantitative aspect of projects can be incorporated into ISO, such as Quantitative Schedule Risk Assessment or Quantitative Cost Risk Assessment." Hence, Company B does not rely completely on ISO 31000, instead, the company adjusts this standard to fit their organisational structure but adopts this standard only to achieve the minimum requirements for managing risks. Company C is ISO certified, so risk management adopts ISO 31000, but PRM adopts the PMI's Risk Standard, which

Participant C5 praised stating: “It fits the purpose and is clear for everybody especially after they added escalation and communication”. Participant C4 believes ISO is good as a guide overall, but the problem for him it is not updated,

> *“It is rigid, it is about best practices; the question is do we apply everything in the standard? The difficulty with it is nothing wrong you can also get to this point”* (Participant C4).

From the above-presented definitions, the participants of Company C and the majority of participants in Company B appeared influenced by the ISO 31000 definition and principles. From a CAS perspective, professionals in companies C and B while aligned on fundamental aspects of risk, acknowledging elements such as uncertainty and their impact on objectives, both project managers and members of ERM recognise that the perception of risk is context-dependent. In this dynamic environment, PRM views ERM as a valuable source for identifying risks, implying that ERM holds a nuanced understanding of risks that may not be immediately apparent to PRM. Despite this, both entities strive to communicate effectively, appreciating each other's perspectives as part of “a co-evolutionary potential” (Rammel et al., 2007, p.3), which ruminates the ability to sense and react to feedback in terms of setting mutual and dynamic interactions among the agents (ERM and PRM).

Company C's long journey with ERM, which began in 2004, reflects the role of path dependency in complex systems. Agents within this system have learned from past experiences, shaping the system's behaviour over time. Employees who have been involved since the establishment of ERM have observed changes in the company’s risk management behaviour. For instance, Participant 11 notes:

> *“Their role (ERM) appears when associating project risks to strategy because we don’t have a full vision about the link to strategy. We were speaking a different language with ERM, but after embedment and change management, we started to see the value”* (Participant C11).

The influence of ISO 31000 is evident in the way most participants define risk, reflecting the definition adopted by ERM, as noted in the ERM Knowledge Sharing Document (Document 4). Therefore, the ISO 31000 standard appeared to serve as common definition that most of the participants comprehend. From another lens, normative isomorphism in institutional theory

refers to pressures from professional standards, education, and training, which shape organisational behaviour (DiMaggio & Powell, 1983). In the context of Company C, the adoption of ISO 31000 can be explained through this lens. Jepson et al. (2022) note that normative pressures emerge when organisations adopt standardised risk management practices through professional associations or training, often using generic templates and tools like ISO frameworks. This explains how ISO 31000 serves as a shared language for risk management in Company C, helping to align practices across departments based on professional norms.

When it comes to the risk management standards adopted by Company A, the current ERM director (Participant A9) provided several documents that have been utilised during risk workshops with each department (Confidential Documents). These documents include the ERM framework and the risk register, as detailed in the methodology chapter (see Table 3.3, documents 3 and 7). The documents adhere to standard practices available in the grey literature, especially the adoption of ISO 31000 which was essential for ensuring compliance with other ISO standards implemented across the entire organisation, including those related to environmental, health, and safety. For example, the ERM Framework, which sets out the key components that provide the foundation for designing, implementing, monitoring, reviewing and continually improving risk management throughout the company was based on the risk management principles and guidelines developed by both ISO 31000 and the practice recommended by COSO.

The company performance against these components will be evaluated throughout the next two themes. However, in the context of PRM/ERM integration and risk perception across the organisation, Company A appears to lag behind Companies B and C in terms of fostering a shared understanding of risk. Although ISO 31000 and COSO provide structured frameworks for managing risk, they did not contribute to unifying risk perceptions among employees in Company A at the time of data collection. Most participants in Company A framed risk within the narrow scope of their immediate work, leading to siloed perspectives, which is one of the main challenges of ERM implementation (Qazi & Simsekler, 2021; Fraser et al., 2022). Only Participant A3 showed a broader understanding by defining risk across multiple contexts, including project-related risks. This siloed approach to risk perception illustrates a significant

barrier to the effective integration of PRM and ERM, as discussed further in the following sub-theme.

The disconnect between the standardised risk management frameworks and the everyday risk perceptions among employees suggests that the formal adoption of ISO 31000 and COSO alone is insufficient to foster a unified risk culture across different functions and levels within the organisation.

4.1.3 A Silo Risk Perspective

As explained in the methodology chapter (section 3.3.1), Company A in the UK is a subsidiary of the Indian multinational conglomerate group. The conglomerate in India funds projects operating by Company A using a General Fixed Contract, which is the type of contract the conglomerate uses for funding all its projects regardless of their geographical location as one size fits all. This type of contract according to Participant A6 is not suitable to the UK, as the British market differs significantly from other markets such as the Indian market.

> *"The risk in the UK market lies in the construction side rather than in engineering and design or materials. The UK has a relatively small and ageing workforce and from an industrial relations standpoint, it can be prone to militancy. In India, it is possible to have a General Construction Contract with a fixed price. However, in the UK, there is a tendency to apply these fixed price contracts, but many companies are unwilling to do so"* (Participant A6).

Thus, the risk for him pertains to the possibility of top management lacking comprehension of its operations in the UK. In India, the workforce in the construction industry is high reaching 36.12 million (Dhal, 2020), while the workforce in the UK is estimated to be around 2.2 million (ONS, 2023). Since the CAS is full of independent agents with unique interests and experiences (Freeburg, 2020) such as projects, leadership (the boards in this case) must be involved in a bottom-up process to understand the local context (Freeburg, 2020). This means the boards must be aware of the labours' conditions in the UK, including the suitable project contracts. The efficacy of such engagement hinges on the nature of interactions whether by a direct involvement of the boards in India in the UK's local context or through feedback loops from the escalation process in the UK to the boards in India. These interactions determine the effectiveness of emergence, which is well-defined aggregate behaviour originating from

localised actions of individual entities (Miller, 2007) (See section 2.2.5 in the Literature Review).

Other participants could only define risk concerning their specific roles. For example, participant A4:

> *"So, at every point, there is a price that is at risk, you know, when I buy the crude oil, the price could be X, by the time that crude arrives to my refinery, the price could be Y. And by the time I process that crude, and I sell the products, the price could be different... I only look at price risk. So for me, anything that I'm buying or selling, I look at that and find out you know, what risk is involved because, you know in the oil business, nothing is sold on a fixed price, everything is sold on a basis floating, like a month average or, five days after a certain event date. So, we only hedge, our purpose is not to take any trading positions, we only take positions to hedge our price risk. So, any money that I may lose on paper, that money I will gain on the physical and vice versa if I make money on the paper, my physical is going to lose money"* (Participant A4).

Another example was from a project manager who defined risk based on the project constraints.

> *"Everything that affects time, schedule, cost, safety, or quality of the project in delivering the project. Risk management is a very important part of the project assurance process, it's part of the value improvements of the project, and it's a key task that needs to be completed before you move on to the next stage of a project. So, it's one of those tasks that you have to complete to meet your assurance criteria and get approval to move from scouting into what we call, you might call it pre-feasibility, and then into engineering, and then into execution. You'd have to complete risks review, as you move through the phases"* (Participant A5).

These silo perceptions show a lack of awareness regarding the potential risks that may impact the overall organisation's strategic objectives. Thus, a consensus on the perception of risk among the various interviewees in Company A could not be identified. One of the challenges facing PRM/ERM integration is the different perceptions and risk languages used by project managers in identifying and defining risk (Agarwal & Virine, 2019). This disparity complicates

collaboration across departments and undermines efforts to align risk management with broader strategic objectives. However, it's important to recognise that the ERM implementation within Company A is relatively new. As a result, employees have not yet had adequate time to develop a shared risk language and framework. This gap in understanding likely contributes to the different perceptions observed. While this challenge may be attributed to the nascent stage of the ERM system, it also raises questions about the company's risk culture prior to ERM adoption. Despite being established in the industry for a long time, Company A did not adopt ERM until the last three years, which suggests that risk governance may have been somewhat fragmented or reactive before ERM was introduced.

To conclude answering the first research question—how do the organisations under study define risk? Participants from Company A presented siloed risk perspectives. Some participants from Company B defined risks based on objectives as a common denominator. Most participants from Company C associated risk with objectives and/or threats and opportunities, and then put the concept into context. Accordingly, Company A shows no general unified risk language as a first step toward the integration between ERM's elements, particularly projects. Company B shows a partly unified risk language. Company C stands as a self-organised system having common elements of risk influenced by the adopted risk management standard as a first step toward a general unified risk language. It recognises the dynamism of risk, particularly in terms of time and space, requiring openness, co-evolution, and emergence. This moves beyond determinism, suggesting that while having general common aspects of risk such as the impact on objectives as influenced by the normative isomorphism from an institutional theory perspective (Jepson et al., 2022), changes in perception are always possible as the agents are continually adapting in a nested system which is the norm of CAS.

The next theme will delve into the underlying reasons for these varying perceptions, particularly focusing on corporate governance. This exploration will examine how the governance structures and risk cultures within these organisations shape the integration of PRM and ERM. To do so, I will apply Winch's three domains of project organisation (Figure 4.4), contributing to his call for research into the governance interface between owners and projects. This exploration will also address the role of corporate governance—the system through which companies are directed and controlled (Corporate Governance Institute,

2022)—as a key influence on the integration process (Kerstin et al., 2014; Andronache et al., 2018), which will be analysed further in the next main theme.

Figure 4.4: Winch's Three Domains of Project Organisation (Winch, 2014, p.21)

4.2 The Role of Corporate Governance in ERM/PRM Integration

As discussed in the literature, the study of corporate governance examines how companies are directed and controlled to ensure accountability and alignment of interests among shareholders, managers, and other stakeholders (Jensen & Meckling, 1976; Freeman, 1984; Corporate Governance institute, 2022). By analysing the governance structures of the three companies, this research contributes to both project management and corporate governance literature. Specifically, it extends Winch's (2014) framework by exploring how risk governance structures are embedded within broader corporate governance systems (the owners), aligning project-level risk management with strategic corporate objectives, which is a main focus of (Winch et al., 2022) . This addresses the authors' call for more research on the governance interface between owners and projects and offers insights into how corporate governance practices influence project outcomes. Additionally, this research highlights the importance of stakeholder management in project decision-making, contributing to a deeper understanding

of the dynamic between corporate oversight and project delivery (Killen et al., 2012; Donaldson & Davis, 1991).

The findings on the risk governance structures and their relationship with the companies' risk culture are presented as follow.

4.2.1 A Siloed Risk Governance Structure Hindering PRM/ERM Integration

Company A operates within the energy sector in the United Kingdom, with headquarters situated in India.

> *"The company has established a risk management committee and an internal Audit Committee, both of which adhere to the company's corporate governance guidelines. Both Committees are chaired by a non-executive Director, ensuring a direct reporting line to the board. As the ERM director, in conjunction with the Chief Risk Officer (CRO) and a representative from internal audit, I regularly participate in sessions to deliver a comprehensive report to top management, including the CEO and legal counsel. This report provides updates on internal audit and risk management activities"* (Participant A9).

Looking at the company's risk management annual report (Document 9, P.37) in the methodology chapter, primarily focuses on financial and commodity risks, which, while important, do not cover the full spectrum of risks that a comprehensive ERM framework should address. For example, there is no mention of operational, strategic, or project-specific risks that could impact the organisation's overall performance (Hunziker, 2021; Andronache et al., 2018; Jiang et al., 2023).

Fraser et al. (2022) found that in small-to-medium enterprises (SMEs) like Company A, the co-location of ERM with internal audit is more practical because it allows for more efficient use of resources, streamlined communication, and better coordination between risk management functions. The authors explain that in smaller organisations, where resources and staff might be limited, combining ERM and internal audit can prevent redundancy and ensure that both functions work cohesively towards the organisation's overall risk management goals. However, it remains important for both internal audit and ERM units to maintain functional separation and uphold internal audit's independence as distinguished by the three lines of defence model, while concurrently nurturing the trust-based relationship between ERM and

management. In this context, Fraser et al. (2022) suggest the ERM director to have direct access to the executive team, including a seat at the executive committee table, not for the sake of asserting authority but to ensure close alignment with the organisation's strategic decision-making processes and to provide effective advisory and support to the CEO.

However, no visual representation of this risk governance structure could be found on the company's website, nor could the participants provide. Instead, the participants provided verbal explanations about the risk governance structure. Specifically, Participant A9 and A1 elaborated on the framework, supported by documents such as the ERM framework and the risk register, as shown in Table 3.3 in the methodology chapter, and the overall organisational governance structure, as depicted in Figure 4.5 below.

Projects sit under Chief Operating Officer (COO) along with engineering, which is the technical assurance side of operating the refinery, operations, which are responsible for the day-to-day operation of the plant, the process safety group, which looks after site process safety, regulatory commitments, and maintenance as well. In projects, risk management is integrated into the project management process rather than being segregated into a distinct PRM function and standard. The Project Assurance Plan (Document 2) describes a four-stage project cycle—idea generation, framing, scouting, and execution.

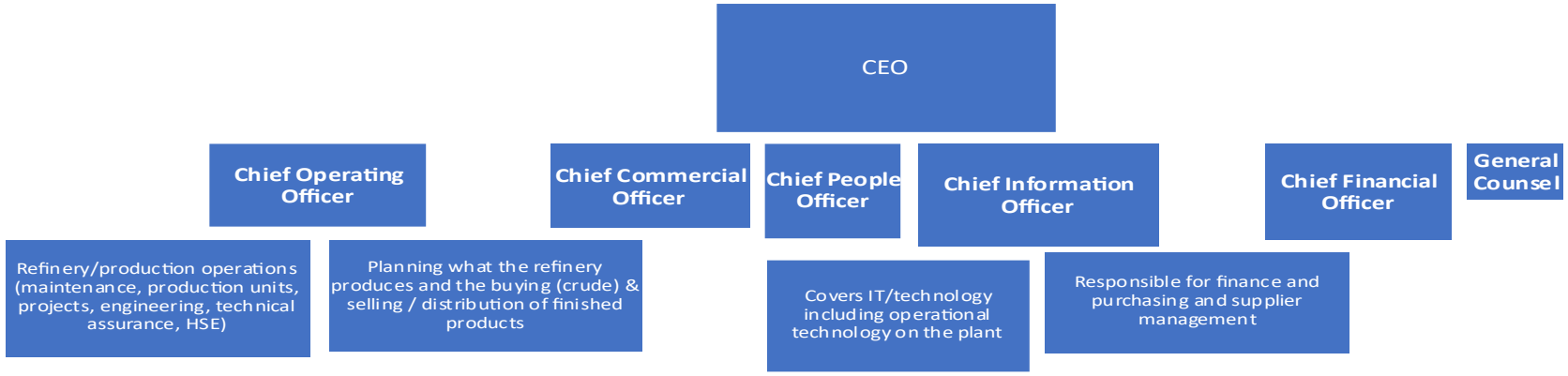


Figure 4.5: Company A's Organisational Hierarchy

During the framing stage, risks are identified, but the effectiveness of this process is hindered by a gap in risk perception between project managers and the boards in India as cited by Participant A6. An explanation could be that the four-stage project cycle described in the Project Assurance Plan (Document 2) while addressing who makes decisions, when, and based on what information (Winch et al., 2022) complemented by the three lines of defence model, appeared to treat PRM independently rather than in portfolio governance that links projects with the strategic objectives. However, Martinsuo (2013) criticised the empirical literature of portfolio management for conceptualising project portfolio management as a rational decision process assuming that companies possess full awareness of all internal and external factors affecting well-defined projects in predictable environments. Therefore, Martinsuo calls for further research to examine contextual factors—the specific conditions in which project portfolios operate—and managerial practices, i.e., the real-world actions that managers take when dealing with portfolios.

The context of Company A shows that despite the reporting line that extends to the board as explained by the current ERM director (A9), the former ERM director (A1) has provided clarification that ERM is exclusively focused on a single site (UK Oil Refinery) whereas audit encompasses multiple sites. Consequently, the implementation of ERM was undertaken to ensure the establishment of consistent and integrated risk management processes solely at this specific UK site. As such, the practice of Company A places its parent company resides on the owners category as the key financial and strategic stakeholder, while Company A along with its ERM reside on the project side as the delivery vehicle of the parent company (Figure 4.6).

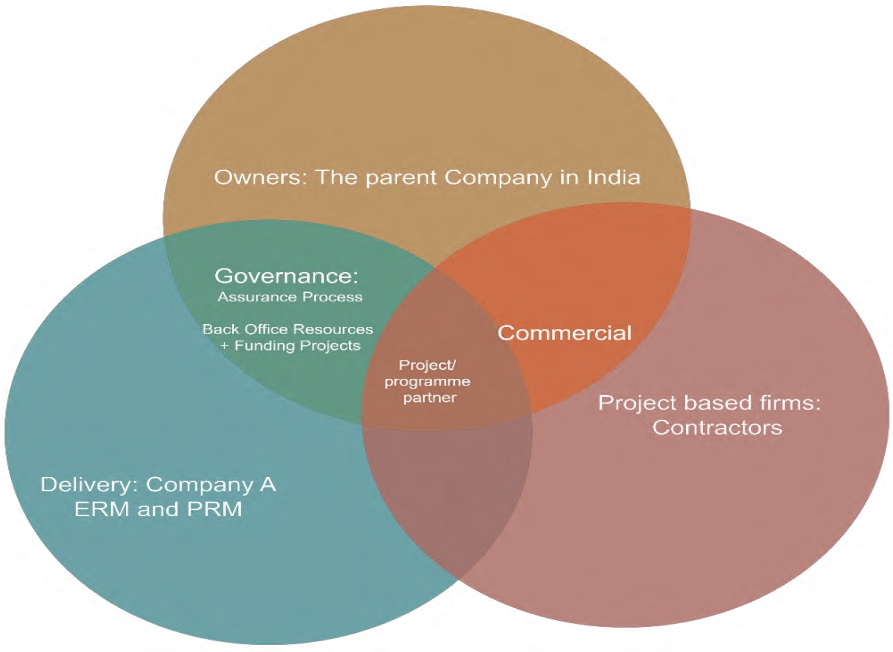


Figure 4.6: Company A's ERM, Projects, and the Parent Company Organisation

This raise concerns regarding ERM coverage to key shareholders and stakeholders in relation to the parent company in India. Hence, discussing consideration of this risk, with the former ERM director responded as follows:

> *"I think the only real consideration of a risk from a company level is, is really, from a funding perspective, we are very much a standalone business, although we're part of a bigger group. This is a business on its own, it doesn't really have any links to look to other companies and doesn't have any relationships in terms of, we're not trading with any other than the UK market. You know, we're purely just a UK refiner that is selling fuel into the UK market and buy-in from, we're not buying oil from our parent company or anything"* (Participant A1).

Unfortunately, none of the risk management standards adopted by the company, whether ISO 31000 or COSO, provide guidance or advice on how to achieve the integration of a standalone subsidiary with a funding relationship with its conglomerate group. Instead, COSO explicitly states its framework is meant to be for the boards and management in entities of all sizes. Similarly, ISO 31000 states that the guidelines are applicable to all types and sizes of organisations. This is reflected in the recent literature which highlights the need for studies on ERM that focus on the implementation of ERM within conglomerate groups with diverse subsidiaries, as noted by Makmor et al. (2023).

Nevertheless, from a theoretical perspective, complex adaptive systems (e.g., ERM) are nested within larger systems (Meadows & Wright, 2008). The interaction of the system within the larger one leads to co-evolutionary dialogue involving the wider situation (Allen, 2012). Even if the company is operating independently, its funding relationship with the owners in India nests it into a broader, interconnected system that is the parent company in India. Ignorance of ERM as a nested system can result in a siloed structure that fails to integrate these complex systems presenting risks from various functional standpoints.

One piece of evidence raised in the previous theme by Participant A6 pertains to the possibility of top management lacking comprehension of project funding in the UK context. As a result, the General Fixed Contract, which the board in India takes as the single type of contract for funding all projects appeared not suitable for the UK market. Martinsuo (2013) criticises project portfolio management for assuming that projects are obedient servants, fulfilling the parent company strategy, rather than purposely used to question the strategy (Artto et.al 2008). This critique aligns with Participant A6's observation, which highlights the rigid and inflexible strategy adopted by the owners.

> *This pattern of delayed decision-making and insufficient project funding leads to the misallocation of resources, particularly a fixation on fixed-price contracts that do not align with the realities of the UK construction market. The constant pressure to operate within tight constraints forces us to compromise on project quality and overall cost efficiency. In practice, this means that we may secure approvals on incomplete designs or mismanaged risk assessments, and we are left struggling with increased costs and extended timelines as the projects progress. Our insistence on applying rigid contract structures, similar to those used in the Middle East, without adapting to local conditions only exacerbates these issues. If we continue down this path, we risk repeating the same mistakes and failing to learn from past experiences, leading to a cycle of inefficiency and waste that affects both our bottom line and our reputation in the industry"* (Participant A6).

In Company A's case, the imposition of fixed-price contracts, which are misaligned with the realities of the UK market, results in resource misallocation, incomplete designs, and mismanaged risks as cited by Participant A6. The resulting inefficiencies and delays highlight the governance gap: projects are treated as isolated entities rather than as interconnected

elements within a broader system, failing to integrate with both strategic objectives and local market conditions. Hence, the governance failure in this case is twofold: (1) The strategic misalignment between the parent company and UK operations, where projects are expected to follow an outdated governance model echoing Martinsuo's (2013) critique of the rational approach, which wrongly assumes projects are "obedient servants" meant solely to fulfil the parent company's strategy, rather than being used to question and adapt the strategy to local conditions., and (2) the insufficient resource and contractor management, leading to project cost overruns and delays in execution. This dual failure reinforces the need for integrated portfolio governance that links projects to the broader strategic objectives of the parent company while considering local contexts and the role of suppliers in the project ecosystem. Such failure resulted in failure of ERM as a Management System as in the next sub-theme.

4.2.1.1 Failure of ERM as a Management System

Building on Participant A6's observation of risk misconceptions between the Indian owners and the UK project teams in Company A, Participant A8 notes that since the company relies on services from the Indian owners, differences in location may result in the Indian team developing practices that don't fully align with UK business requirements and preferences, potentially leading to misalignment. Following this, I evaluate Company A's ERM against the ISO Management System Standard (2019).

> "We *take some services from the subsidiary in India, but provide services back to the UK. In theory, they should be aligned with the UK requirements, and business practices because they're effectively a subsidiary that does provide back-office owner services. So, from that perspective, the resources in India should all be aligned with our processes and risk sites, and the like, I suppose in practice because there's a time difference and a physical location difference, I suppose there is a risk that culturally they'll develop in their own processes and procedures that don't necessarily align. An example is the international spline trading. They are the guys that buy the big bulk cargoes of crude. So the team in the UK has shrunk quite significantly, the people that buy and sell the crude back office admin function that does all the paperwork for that does the shipping etc, is got a lot bigger in India. I could see a theoretical risk that if they don't speak regularly, they're not aligned with business practices or requirements in the UK, they can be doing over what works in India, or whether people are doing*

wherever they're not necessarily quite aligned, or quite right with the UK business. What's the word understandings or preferences just based on locality, I guess, because it's because of this from doing things in different jurisdictions" (Participant A8).

Despite the possibility of a lack of support for risk management from top management, the decision made by the previous ERM director to implement ERM separately from the parent company also shows a failure to consider the broader system's influence on the company as evidenced by Participants A8 and A6. This raises questions regarding the efficiency of ERM as a management system. The Institute of Risk Management IRM (2022) identifies ERM as a management system, which is defined as the framework of policies, processes, and procedures employed by an organisation to ensure that it can fulfil the tasks required to achieve its purposes and objectives (Annex, 2019). Aligned with the ISO Management System Standard (2019), ERM under Annex SL requires adherence to ten essential components. These include defining the scope, referencing normative standards, establishing terms and definitions, understanding the organisational context, providing strong leadership, engaging in strategic planning, ensuring adequate support structures, conducting operational activities, evaluating performance, and fostering continuous improvement. IRM (2022) further categorises these components into two distinct groups within the ERM framework. Group A focuses on defining the scope and designing the system, while Group B emphasises controlling operations and fostering development (See Figure 4.7).

Figure 4.7: Components of Management Systems Based on Annex SL Format (IRM, 2022)

According to (IRM, 2022), an effective ERM plan should include three key steps. First, it involves identifying the intended benefits of the ERM initiative and gaining board support. Second, it requires planning the scope of the ERM initiative and developing a common language of risk. Third, it entails establishing the ERM strategy, framework, roles, and responsibilities. Company A seems to face challenges in the planning phase, particularly in the second step. The company did not recognize ERM as a nested system within the conglomerate group in India, resulting in a siloed structure. Additionally, the lack of a common risk language is evident from the varying perceptions of risk among different participants in the previous theme. In the next sub-theme, I assess Company A's risk culture to gauge its influence on siloed ERM practices that impede integration with projects.

4.2.1.1.1 The Incompatibility of a Closed Risk Culture with Complex Adaptive Risk Management Hindering PRM Integration

As stated in the literature section 2.3.5, given the absence of risk culture guidelines in ISO 31000 and COSO, evaluating the risk culture in this study is based on the ten criteria of a successful risk culture suggested by the Institute of Risk Management (IRM, 2012). Starting with the first criterion, the tone from the top, while the establishment of ERM in Company A follows a bottom-up approach due to its status as a subsidiary, the approach to ERM knowledge sharing in this company takes a top-down approach.

> *"I think if we started looking for these champions now, which was my initial thought, all that will happen is they'll be doing all the work and then the wider team are not going to be engaged and sort of understand the framework. So anyway, I mean, with the size of this organisation, that's the approach. I mean, I think, obviously, for larger organisations that are more complex, you know, we could maybe follow a different approach, but here dealing with heads off, and their direct senior leadership teams is the approach that I'm taking. And I think it seems the feedback really good"* (Participant A9).

The second point, relating to ethical principles, is supported by the company's establishment of a Risk Management Committee and an Internal Audit Committee, both of which adhere to the company's corporate governance guidelines, which is embedded according to The Wates Corporate Governance Principles for Private Companies in the UK (Document 9, P. 35). Thirdly, there is still no common acceptance throughout the organisation of the importance of continuous risk management.

> *"I had a lot of discussions with heads of departments and bought, again, because the business has gone through a bit of a sort of transition phase. Maybe 30, 40, 50% of those heads of departments whom I'm having discussions with two years ago, have now left, and there are new heads of departments. And so there will be a process to go through again. This has resulted in a lack of resources dedicated to risk management"* (Participant A1).

Such limitations as stated by Participants A1 and A3 have negatively affected the way risk is communicated and understood among the different functions and departments in the

company. This aligns with the findings of Qazi & Simsekler's (2021), who identify unifying risk language among the main challenges hindering ERM implementation. Hence, it was unsurprising to find the company struggles in setting timely risk information flowing up and down the organisational communication channels (Fourth criterion).

> *"I suppose at my level, I don't necessarily see what happens to those reports. Once you identify a risk, and it goes up into other committees, it's sort of I input into it, and then it disappears. That's not to say that a subtle level above me sits in the Risk and Audit Committee meetings, and they discuss some of these risks but don't necessarily have a loop where it comes back round*" (Participant A8).

Fifth, Participant A3's insight supports event risk reporting, but only in terms of risks related to health and safety.

> *"It's part of our culture to think about, before you start a task, what are the risks that you're going to be introducing yourself to assessing them, and what controls you have in place, whether it's Perimetry controls that someone authorised, you know, of a particular competency level as specified in a permit, that you're following them correctly, that you're aware, what you're putting yourself in the situation that you're putting yourself into, and therefore you if something starts to go wrong, you can recognise how it's going wrong, how it may affect you, and whether you should stop the job. And then like recovery, like control measures, if it starts to go wrong, do you know for example, where you need to go with the site alarm goes off, things like that. So on an individual level, we encourage people, as a safety culture as like a risk culture, a risk management culture to flag to bring awareness to the management of unsafe conditions or concerns. We track these as key performance indicators one of our KPIs where we love we call it safety noise. So when people have brought something to the attention of management that they feel is unsafe or could be improved"* (Participant A3).

Criteria six, which states that no process or activity should be too large, complex, or obscure for the risks to be readily understood is not met by Company A. According to the Existing Risk Communication & Reporting (Document 8), Company A exhibits a diluted view of risk due to a lack of clear cross-silo interaction. In projects, risk management is integrated into the project

management process rather than being segregated into a distinct PRM function and standard. The Project Assurance Plan (Document 2) describes a four-stage project cycle—idea generation, framing, scouting, and execution. During the framing stage, risks are identified, but the effectiveness of this process is hindered by a gap in risk perception between project managers and the boards in India. In addition, Participant A2 highlights that recent changes in senior management have led to the removal of key scrutiny and readiness reviews. This reduction in oversight has resulted in some risks being inadequately addressed, undermining the effectiveness of the integrated PRM-ERM approach. This issue often manifests when employees or ERM members consider ERM a strategic task while the senior and top management view ERM as merely a compliance requirement (Andronache et al., 2018; Hunziker, 2021).

> *"We used to have a more rigorous scrutiny process, which included a readiness stage and a challenge review before proceeding to Investment Proposal (IP). However, this level of oversight has been removed. Previously, each large project was accompanied by a summary review, but this practice has been discontinued due to changes in senior management. It seems that the new leadership may not see these steps as necessary, leading to important checks being overlooked"* (Participant A2).

Seventh, the participants did not reference supporting appropriate risk-taking behaviours be rewarded and encouraged, while inappropriate behaviours are challenged and sanctioned. At this point, I do not assume this criterion does not exist within the company but simply remain unsubstantiated by the provided evidence. The absence of criteria 7 is highlighted within the limitations and future research section in the conclusion chapter. For criterion eight, while risk management skills and knowledge are encouraged, there is no properly resourced risk management function, instead Participant A9 is the only member in the ERM. This shortage of top management support for the ERM project, along with the differences in the use of risk terminologies reduce the acceptance level of risk management among the employees (Qazi & Simsekler, 2021).

For criterion nine, the conglomerate group does not accommodate diversity of perspectives, instead treating all subsidiaries as one-size-fits-all. Criterion ten emphasises the importance of aligning culture management with employee engagement and people strategy to ensure social support and a strong focus on tasks. However, Company A shows clear misalignment in

this area. For example, Participant A6 highlights that last-minute decision-making by the owners and people operating at the high level often results in inadequate project funding. This reactive culture pressures employees to work under tight constraints, compromising project quality and cost efficiency. This indicates a disconnect between the company's culture and its people strategy, where employees are not adequately engaged or supported to focus on their tasks effectively. This is further captured in Document 8 which show the principles risks are based on executives' personal opinions but no consensus across departments/functions. This suggests that ERM in Company A is not integrated into all decision-making processes across the top management and the different functions and departments. Such integration is a key element of " a positive risk culture" (Hunziker, 2021, p.116).

> *"The biggest problem you will always find with our company is that the royals, and people operating at that top level, invariably leave decisions to the last minute, resulting in inadequate funding for projects, which ultimately costs the business money. This pattern of delayed decision-making and insufficient project funding leads to the misallocation of resources, particularly a fixation on fixed-price contracts that do not align with the realities of the UK construction market. The constant pressure to operate within tight constraints forces us to compromise on project quality and overall cost efficiency. In practice, this means that we may secure approvals on incomplete designs or mismanaged risk assessments, and we are left struggling with increased costs and extended timelines as the projects progress. Our insistence on applying rigid contract structures, similar to those used in the Middle East, without adapting to local conditions only exacerbates these issues. If we continue down this path, we risk repeating the same mistakes and failing to learn from past experiences, leading to a cycle of inefficiency and waste that affects both our bottom line and our reputation in the industry"* (Participant A6).

The evaluated summary of Company A's risk culture is provided in Table 4.1.

Table 4.1: Company A's Risk Culture according to (IRM,2012)

Criteria	Status	Evidence/ Comments
1. Distinct and consistent tone from the top, from the board and senior management in respect of risk-taking and avoidance (and also consideration of tone at all levels)	Partially Met	ERM follows a bottom-up approach as a subsidiary, but ERM knowledge sharing is top-down. "Dealing with heads off and their senior leadership teams is the approach" (Participant A9).
2. A commitment to ethical principles reflected in a concern with the ethical profile of individuals and the application of ethics and the consideration of wider stakeholder positions in decision making	Met	The establishment of a Risk Management Committee and Internal Audit Committee aligns with corporate governance guidelines.
3. A common acceptance through the organisation of the importance of continuous management of risk, including clear accountability for and ownership of specific risks and risk areas	Not Met	Lack of consistent commitment to risk management due to frequent changes in department heads. "30-50% of heads of departments have changed, leading to a lack of resources dedicated to risk management" (Participant A1).
4. Transparent and timely risk information flowing up and down the organisation with bad news rapidly communicated without fear of blame	Not Met	Struggles with communication channels; reports disappear after submission, with no feedback loop. "Once you identify a risk, it goes up and then disappears; there's no loop where it comes back" (Participant A8).
5. Encouragement of risk event reporting and whistle blowing actively seeking to learn from mistakes and near misses	Partially Met	Risk reporting exists but is focused mainly on health and safety issues. "We encourage people to flag unsafe conditions, and we track these as key performance indicators" (Participant A3).
6. No process or activity too large or too complex or too obscure for the risks to be readily understood	Not Met	Lack of clear cross-silo interaction dilutes risk understanding. PRM is integrated into project management, but gaps exist in risk perception and recent scrutiny removal has undermined effectiveness (Document 8, Participant A2).
7. Appropriate risk-taking behaviours rewarded and encouraged and inappropriate behaviours challenged and sanctioned	Unsubstantiated	No evidence provided supporting the reward or sanctioning of risk-taking behaviours. The absence of criteria 7 is highlighted in the conclusion chapter.
8. Risk management skills and knowledge valued, encouraged and developed with a properly resourced risk management function	Partially Met	No properly resourced risk management function; only one member in the ERM team (Participant A9).
9. Sufficient diversity of perspectives, values and beliefs to ensure that the status quo is consistently and rigorously challenged	Not Met	The owner does not accommodate diversity of perspectives; all subsidiaries are treated uniformly, without adapting to local conditions.
10. Alignment of culture management with employee engagement and people strategy to ensure that people are supportive socially but also strongly focused on the task in hand	Not Met	Disconnect between culture management and people strategy. Last-minute decisions and inadequate project funding compromise quality and efficiency. (Participant A9) "Last-minute decisions lead to misallocation of resources."

The closed risk culture in Company A contradicts the principles of CAS by limiting interactions between agents, disrupting effective feedback loops, stifling emergence, and hindering self-organisation. This restrictive environment prevents the free flow of information and collaboration between the parent company and local project managers in the UK, reducing the diversity of perspectives. Therefore, risk assessments should remain flexible and open to new sources of information (Hunziker, 2021) to adapt to the ever-changing environment. The current risk culture of company A shows ineffective feedback loops between the top, middle, and low-level management, resulting in a lack of continuous emergence of new patterns of risk management behaviours that can accommodate and interconnect diverse risk perspectives. This deficiency hinders projects to be a self-organising system capable of adaptively responding to evolving risks. As per Boulton (2012), evolution starts locally and collectively, and variation leads to self-organised forms but this is missing in Company A. As a result, the complex nature of projects in Company A fails to align with the rigid practices of governance enforced by the parent company.

As we shift our focus to Companies B and C, it becomes important to explore whether their risk governance structures can overcome these challenges. Does Company B's structure allow for greater flexibility, interaction, and the free flow of information? Can it adapt to evolving risks more effectively than Company A? The answers to these questions will provide deeper insights into what constitutes successful PRM/ERM in dynamic and complex environments. By contrasting Company A's failures with Company B's practices, we can better understand the critical elements necessary for an effective and adaptive risk management culture. As such, I now shift to Company B to explore its risk governance structure.

4.2.2 A Complex Adaptive Risk Governance Structure with Partial PRM/ERM Integration

The risk function in Company B falls under Governance Risk and Compliance (GRC) (See Figure 4.8). GRC constitutes an integrated and comprehensive approach to corporate management, emphasising an organisation's adherence to its self-defined regulations, risk tolerance, and external mandates (Racz et al., 2010). This approach achieves this alignment by harmonising an organisation's strategy, processes, technology, and human resources, thereby capitalising on synergies and enhancing overall performance (Racz et al., 2010). Therefore, GRC is perceived as the umbrella of ERM (Andronache et al., 2018). Under this structure in Company B, there are three types of risk management structure: "ERM which includes development and

operations departments and anything that has been identified by the CEO or anyone of C-Suite as a very important risk or something that the GRC team sees happening within the market, PRM, and Resilience" (Participant B1).

> *"There are two levels of risk management in projects: one on the project ground (delivery) which communicates with the project directors to gather risks related to the actual scope of the project in terms of cost, quality, health and safety, time, and any factors that touch the scope of the project and completing it on time, then discussing mitigation plans. The second is the role of GRC which looks at how information is collected and assesses how well risk management has been conducted within these various projects altogether. Resilience is a tenet of risk management protocols that are concerned with risk mitigations for identified risks, and evaluate if such risks cannot be mitigated for whatever reason and become realised risks; for example, the implications emerging from the global pandemic"* (Participant B2).

Resilience is defined as a system's ability to absorb disturbances and reorganize during change, thereby retaining its essential functions, structure, identity, and feedback mechanisms—remaining within the same regime (Norberg et al., 2008). Therefore, resilience indicates the degree to which a complex adaptive system can self-organise and sustain its capacity for learning and adaptation (Norberg et al., 2008). One of the GRC teams Participant B3 who is a member of the ERM team explains:

> *"The three GRC teams (ERM, Projects, and Resilience) meet regularly to assess where we are and what risks need to be highlighted to the champions. We have 17 champions that gather data for us in a risk register and then the champions meet GRC teams on a quarterly basis with ERM and Resilience teams but on a monthly basis with projects because the frequency of change on projects is much higher than on the corporate level. We (the GRC teams) put all the information together then it goes up to the Executive Risk Director (ERD), who oversees all three GRC teams. The ERD drafts the enterprise risk register and reports the high-level risks to the audit committee and then the very important strategic level risks get reported to the board"* (Participant B3).

This, along with the company's risk governance structure (Figure 4.8), supports the implementation of the three lines of defence as discussed in the first theme in several ways.

First, ERM, as part of the GRC framework, aids various functions through appointed champions. Second, due to feedback loops between agents in the GRC and project members, the GRC teams recognise the unique features and durations of projects, increasing interaction on a monthly basis. Third, although the audit committee operates independently from risk management, it continuously provides feedback on the effectiveness of the GRC's performance. Fourth, the board demands reports from the risk management function led by the ERD to ensure alignment with the company's risk appetite and to understand strategic risks that might affect the organisation's strategy. This approach aligns with the principles of complex systems, which emphasise applying both bottom-up and top-down approaches (Boulton, 2012). The former empowers local agents, i.e., those working on the project ground, to make local decisions and adapt to project-specific challenges, while the latter ensures that the overall strategic direction and oversight are maintained by the leadership. In addition, Company B by appointing the two PRM directors indicates a portfolio management strategy, which is a project governance structure that oversees the sum of individual projects of an organisation (Winch et al., 2022). By balancing these approaches, the company can effectively manage and align individual projects with broader strategic goals, fostering a more resilient and responsive organisation.

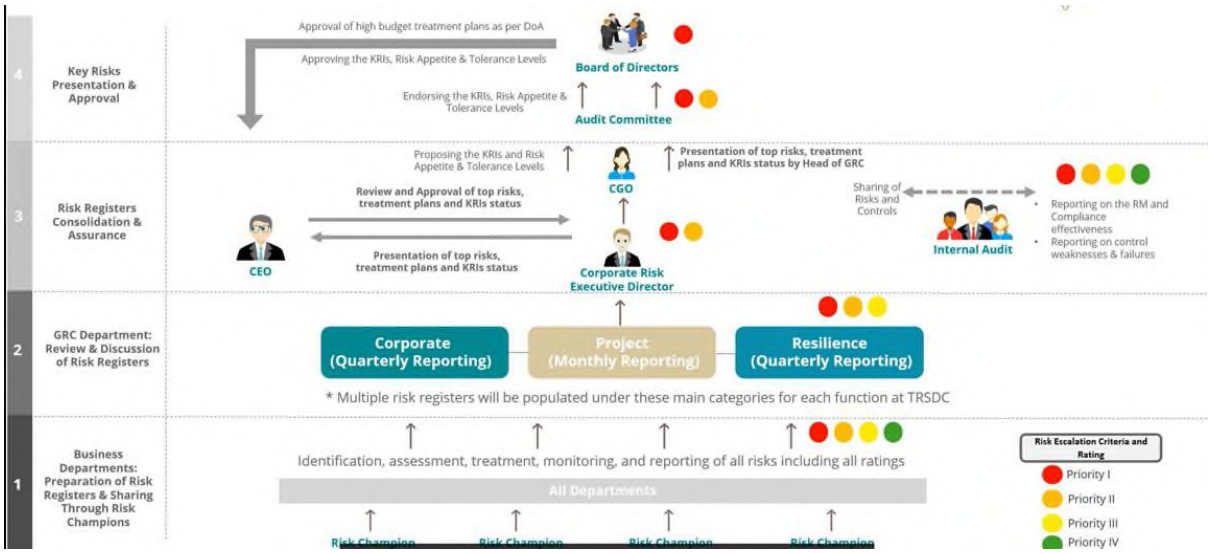


Figure 4.8: Company B's Risk Governance Structure (Document 1)

With regard to how governance structures impact on the interaction of risk management, some participants, specifically the risk champion for the change management department found the risk governance structure illustrated above is working efficiently.

> *"I have seen many companies treating the identified key risks at the departmental level. Here, I notice the risk management team communicates with me on the agreed time frame, if there is a lack of response they always make sure to communicate with my backup, and if my backup is also not there, they escalate to the top management straight away…etc so, here is a proactive approach, we gathered all the input, share it with our top management, and based on their approval we get it to the risk team"* (Participant B5).

These clear timelines and escalation processes were lacking in Company A as evidenced by Company A's Existing Risk Communication and Reporting Process (Document 8) and participants A1, A2, A6, A8. For example, according to participant A2,

> *"There is a time issue, senior management has limited availability (solution having a follow-up discussion, having a much smaller meeting with fewer parties). We used to have some scrutiny that has been removed whereby you had more readiness stage and a challenge review before going to implementation to make sure your project receives everything needed before implementation. So, things like these are now missed… Sometimes some business risks are obvious, but sometimes the business is sensitive and don't share anything with everyone, so you must have someone from the business (board) to know about them. There are unclear/ inconsistent risk monitoring & reporting processes from departments/ functions to senior management and the board will not be improved until you stabilize your structure. There are some risks that do not exist in risk registers (not big risks but they may cause major issues). There is self-censorship, the new managers change the structure every 5 minutes, sometimes you don't report all risks, but the major risks because you know the top managers will not take all the risks, so some risks remain invisible. Then, you are surprised terrible things happen because those risks were lingering for a while"* (Participant A2).

Therefore, the findings on Company B's risk governance structure contribute to the recognition of the need for an overreaching portfolio governance structure that effectively integrates projects with the enterprise strategic level. This governance structure, with its dual

PRM directors; one overseeing integration with GRC requirements and the other managing individual project risks acknowledges the intricacies of coordinating multiple projects while aligning with strategic objectives. By balancing centralised oversight with project-specific risk management, Company B's model addresses Martinsuo's (2013) critique of traditional, overly rational project portfolio management that assume predictable environments. Instead, it reflects an adaptive and dynamic governance approach that accounts for the evolving nature of projects. This approach enables PRM and ERM to interact, exchange feedback, and maintain alignment with broader organisational goals. As illustrated in Figure 4.9, which presents the actors in Winch's Three Domains of Project Organisation Venn diagram, the PRM and ERM agents in Company B unlike those in Company A, are positioned at the governance intersection between owners and project delivery. This positioning results in more integrated PRM/ERM governance, characterised by a clearer risk escalation process and well-defined roles and responsibilities, as evidenced by Participants B1, B2, and B5.

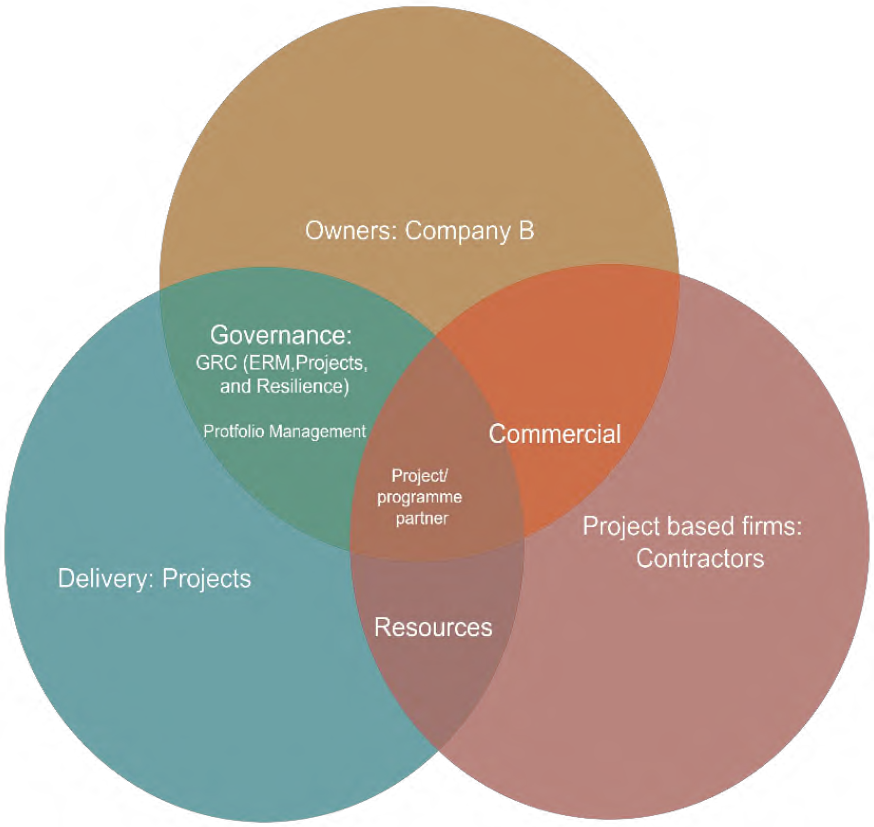


Figure 4.9: Company B's ERM and PRM Governance within Winch's Three Domains Venn Diagram

However, although the GRC teams in Company B communicate with projects members on a monthly basis, the project risk director at the delivery level, thinks this is still not enough communication to address the fast-track nature of projects, he adds:

> *"ERM frameworks while they are good for steady-state organisations where you have gone with organisations or banks they are very useful, but in the case of projects, projects are way too fast in terms of their evolution. So, you can have a project that starts today and in six months the project will be over. By the time you have your monthly risk review, you will only have 6 risks reviews if you go with the ERM model. That's one of the biggest challenges; by the time you even raise a risk, record it, and report it the risk could have been mitigated because that is the urgency at which and the fast-track nature of projects. ERM is just not going to be adaptable to that fast-paced nature of the project. You got a project in one hand, things need to be decided very soon, but then you have other departments where there is no such urgency for that matter…. ERM frequency is completely mismatched with the projects reporting framework. ERM tends to have*

quarterly and monthly sessions, but in projects, we need to have daily and weekly sessions, so the timeline doesn't align well" (Participant B8).

The governance framework implemented by Company B facilitated risk communication and escalation, as evidenced by the involvement of champions. However, despite the company's endeavour to address the fast-paced and frequent project activities by increasing the frequency of communication from quarterly to monthly intervals, the project director's feedback indicated that projects continued to face challenges in aligning with this governance framework. The fact that Company B is newly established suggests that path dependency played a role in its development, as the company lacks the accumulated experience (Holland, 2006) needed for its GRC and project teams to become fully self-organised. Despite the complexity of Company B's risk governance structure, which takes into account the challenging environment in which it operates and results in a clearer escalation process with defined roles and responsibilities, self-organisation is still maturing.

In contrast, as will be discussed in sub-theme 4.2.3, the risk governance structure of Company C exhibits a more adaptive and self-organised approach. Evidence from Participants C6 and C9 indicates that agents, such as project teams, exhibit greater agility in knowing when and how to interact with the ERM framework. The long-standing experience of Company C in launching ERM reflects the influence of path dependency, where past practices and accumulated knowledge shape current decision-making behaviours (Nisula, 2018). Path dependency in this context contributes to the agility of project teams, as they have internalised risk management practices that align with both organisational strategy and the realities of project execution.

> *"It is about balancing agility with compliance, and this requires wisdom. To achieve this, we need to view decision-making holistically, ensuring that authority and empowerment are matched with accountability. It's about maintaining a dynamic system that supports flexibility while keeping a close eye on compliance. By updating and adapting our processes, we can empower leaders to make swift decisions without compromising on regulatory standards." (Participant C6).*

This insight underlines the critical role of leadership in balancing agility and compliance. Leaders with this balance can enhance the organisation's adaptability, which is hard to exist

in a closed risk culture as seen in Company A. As will be discussed next Company B's risk culture is more open and adaptive to various stakeholders than Company A's risk culture.

4.2.2.1 The Impact of an Open Risk Culture on the Integration of ERM/PRM for an Effective ERM Management System

Applying IRM's Successful Risk Culture Criteria, the below evidence from the participants supports a consistent tone from the top ensuring risk management skills and knowledge are valued, encouraged, and developed with a properly resourced risk management function led by the GRC teams.

> *"First, we meet with the C suite, and then we meet with heads of departments and give them a crash course on risk management every year, thus, it is two-way communication, top-down and bottom-up approaches. We do like a quick little follow-up, and then we obviously tell them what our risk appetite is for the year, what the levels are, and all that stuff. So, there's a really quick session that we do for the heads of the department. You know risk management is a group thinking environment, so we conduct risk workshops in which we share our experience. "We do the champions themselves; we train them twice a year. So, we do a really quick crash course, depending on the level of information. So, we have really good champions who understand risk and really do support us, but then some need a little bit of work. So, depending on where they stand, we provide them with actual training, and we are the ones who provide them with that training"* (Participant B1).

The evidence provided by Participant B1 supports Fraser & Simkins' (2016) emphasis on promoting a culture of willingness to open, to share, and to create teamwork across boards, senior managers, and employees as the key factors for ERM success. In addition, Company B's Code of Conduct (Document 10) aligns with the second criterion of the IRM's Successful Risk Culture, which emphasises a commitment to ethical principles, including concern for the ethical profile of individuals and the application of ethics in decision-making. The section on "Business Partners and Suppliers" (Document 10, p.12) exemplifies the company's dedication to fairness, integrity, and transparency in its dealings, all of which must be embedded in an organisation's risk culture (Hunziker, 2021). In the context of risk management, I found the risk awareness survey allows the GRC department to evaluate its effectiveness since it measures

how well employees understand GRC work and gives them a chance to reflect on it. The survey ensures transparency and reinforces the company's dedication to ethical risk management.

> *"On an annual basis, we do awareness sessions where we specify to all employees, if you do see a risk, if you do identify something, these are your risk champions, and we split this awareness session into departments so that we can actually provide these departments with the information required for them. And then at the end of that, at the end of every year on about q4, we do like a risk awareness survey, and we provide that information to the audit committee"* (Participant B1).

Drawing from Participant B1's insights, which highlight the encouragement of risk reporting and transparency in the work of the GRC teams, I triangulate this with the experience of Participant B6, who received the risk awareness survey.

> *"I have done it once, it is probably they want to know about our experience, is there anything that can be improved, the way they contact us, how was the champion, where the champions clear? Were the questions clear? Was the process easy? So, I think it is a general survey to evaluate their work and see the importance of their work to other stakeholders, which I think this is very positive when it comes to measuring your own tools and their effectiveness to ensure transparency"* (Participant B6).

The participant further elaborates on the company's extensive range of tools designed to encourage risk reporting, emphasising that such proactive approaches place the company at the top in risk management compared to others he has worked for.

> *"I think what sits this company above a lot of companies I have worked with is that the company has so many tools open to all its employees. First of all, to report any suspicious anything, we have a whistle-blowing website, hotline, and even emails, so employees can send while their identity protected, and the GRC is always available to answer any questions and receive any risk. When it comes to knowledge sharing, we circulate all this knowledge within our internal communication emails and then the team ensures that whenever this critical documentation exists within our intranet, …., where people can see policies, guidelines, and other relevant information that could be beneficial not only for the champions but also for the rest of the employees"* (Participant B6).

Recalling Participants' B5, B6, and B9 insights in the previous theme, which support the common acceptance in the company about the continuous management of risk including clear accountability and ownership of risks and timely risk information following up and down the organisation. Despite being from different departments, these participants recognise the critical importance of managing risks and clearly understand their responsibilities in this process.

> *"The risk management team communicates with me on the agreed time frame, if there is a lack of response they always make sure to communicate with my backup, and if my backup is also not there, they escalate to the top management straight away…etc so, here is a proactive approach, we gathered all the input, share it with our top management, and based on their approval we get it to the risk team"* (Participant B5).

> *"The role of the governance as they (The GRC teams) taught us is the first line of defence, so this is what I teach each function within my department. Specifically, in marketing, we deal with external, we are the image of this company, we deal with the sentiment, so our department is in the face front of any potential risks"* (Participant B6)**.**

The company has structured its risk management system to ensure that no process or activity is too large or too complex or too obscure for the risks to be readily understood in different ways. The creation of GRC as explained earlier, which consists of three functions ERM, projects, and resilience. Participant B9 adds the company's way of unifying the risk language is through three ways; First, risk appetite, second, risk assessment criteria through a shared probability and impact matrix, and third, awareness sessions to all employees. These approaches particularly the development of a risk glossary as part of the risk appetite are necessary "to keep everyone on the same page" (Kerstin et al., 2014, p.9).

> *"We have three ways for unifying the risk language, first risk appetite, and second risk assessment criteria through a shared probability and impact matrix. Finally, the GRC teams hold awareness sessions. Withing our policy document which obviously is kind of the top level in terms of governance of our programs, we would have a defined common understanding of terms, so we have a list of all of the terms we use and a definition that is accepted across the organisation. However, the informal way of*

unifying risk language is a bit challenging for example, how do we classify disruptive events (we call it distributive events, it could be emergency, it could be an IT failure)" (Participant B9).

These structures and approaches demonstrate an alignment between culture management, employee engagement, and people strategy, ensuring that employees are both socially supportive and highly focused on their tasks.

"The interaction with the GRC teams has broadened my knowledge about risks, which I believe will help me in future careers, it is also helpful in my own life because if you take something to that extent, it helps you to always plan ahead. At the department level, it gives you a sense of responsibility towards the brand, towards your work, and your colleagues. So being responsible gives you ownership and elevates you as a professional to think beyond your scope. So, exposure, knowledge, ownership, and competency" (Participant B6).

"They give us a big responsibility in terms of owning that document and identifying the risks, not only reading what it is, also they open the channel to discuss new risks even if we don't know if they are risks or not, so they can shape our ideas better and walk us to that, and then come back to us with new risks added with suggested treatments, so they literally want us to be part of their team as champions to represent them, and there is empowerment to that" (Participant B5).

However, despite these positive outcomes, insights from Participant B10, who oversees the interdependence of project risks with organisational objectives, suggest that some project members still struggle to understand his role fully. "My role is constantly confused with the project delivery risk director role. I'm frequently asked why we need so many levels in risk management, and it's an easy question to answer because we are a large organisation dealing with various external parties, ministries, and macroeconomic factors," he explains. This challenge can be understood through the lens of CAS, particularly by Sheth & Sinfield's (2024) explanation of ERM as CAS through four features: parallelism, conditional action, modularity, adaption and evolution. *Parallelism* means multiple risks happening in parallel and impacting multiple business functions at the same time (Sheth & Sinfield, 2024). The risk governance structure of Company B shows a recognition from the top management that project risks are

complex emerging from different projects simultaneously requiring a suitable governance structure with clearly defined rules to manage such complex conditional action. The authors define *conditional action* as the programmatic governance rules in an organisation that warrant action or engagement based on managers' threat perceptions and evaluation. As these top managers including Participant B10 engage with these various external parties, they understand the mechanism of the risk impact on business functions (such as the project function). Hence, they can create risk responses to alleviate risk propagation "*modularity*" (Sheth & Sinfield, 2024). Therefore, it is through communication and learning *"adaption and evolution"* that these top managers can proact risk impact by identifying a centralised function (Sheth & Sinfield, 2024) such as ERM, projects, and resilience in the case of company B. However, as a relatively new company, the company is still in the early stages of developing and solidifying its structures, roles, and communication channels. This indicates that while progress has been made, there is still work to be done in refining these systems and ensuring all employees understand and accept their roles within the broader organisational context.

Having said that, more relevant to the context of PRM/ERM, the cycle of the integration of project risks into program and enterprise levels, as well as the detailed aggregation process (Figure 4.10), have been understood by many participants for example (Participants B10, B2).

> *"We have specific risk functions that aid in delivering objectives of other departments namely projects (they have their own project risk director), safety that is part of Hazzard logs, and environmental that is part of environmental assessment, and IT that is precisely linked to cyber security…Level 1 is tactical risks (asset project specific); level 2: aggregation in a program level where you repeat risks try to deal with them in a program level; then look at these different program risks in Level 3"* (Participant B10).

> *"We have assets (e.g. projects) and 13 programs (13 risk registers) then we make aggregation on the phase level, then we take the phase corporate risk register+ business continuity (threat risk analysis TRA) = Enterprise, then a copy of enterprise to strategy. The audience of the enterprise is the CEO and audit committee, and the audience of strategy is the boards"* (Participant B2).

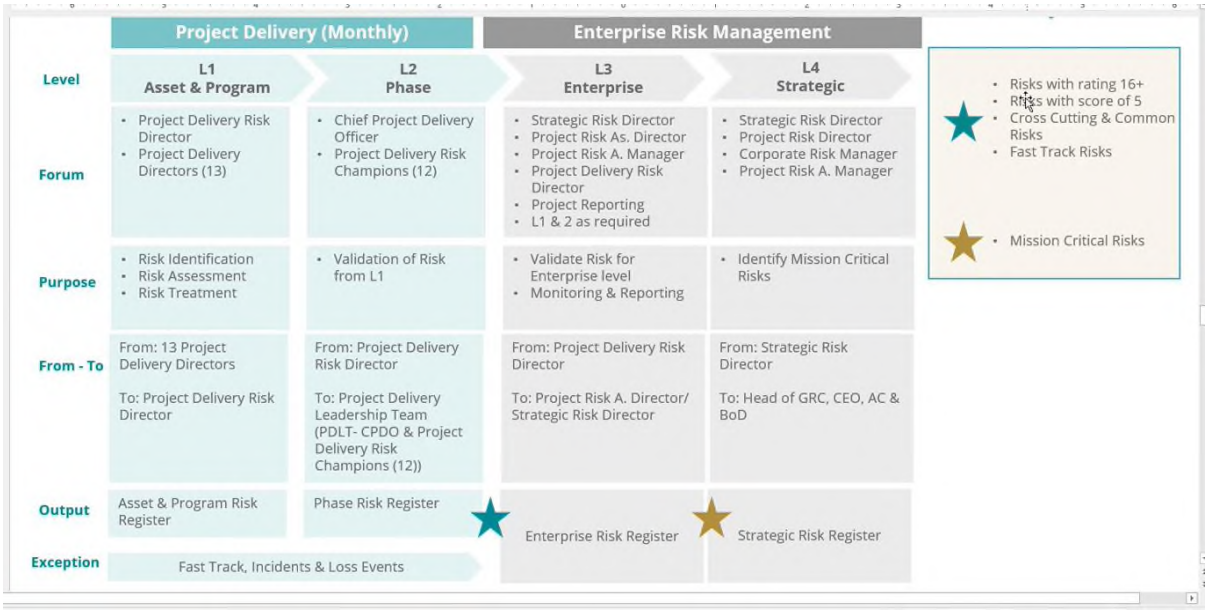


Figure 4.10: The Cycle of Delivery (Projects) (Document 5)

This demonstrates while some employees struggle with understanding some risk managers' roles, there is some level of consistency in understanding risk management practices among different employees, which aligns with the company's risk management documentation. The evidence found in Andromache et al (2018) further supports the risk governance structure of Company B, highlighting the importance of centralised risk management roles such as the role of the PRM director at the GRC level to continuously update the risk status based on the feedback loops. Table 4.2 summarises Company B's risk culture against IRM's criteria of successful risk culture.

Table 4.2: Company B's Risk Culture according to (IRM,2012)

Criteria	Status	Evidence/ Comments
1. Distinct and consistent tone from the top, from the board and senior management in respect of risk-taking and avoidance (and also consideration of tone at all levels)	Met	C-suite involvement in annual training sessions and communication of risk appetite reflects a clear and consistent tone from the top (Participant B1). (*First of all, to report any suspicious anything, we have a whistle-blowing website, hotline, and even emails, so employees can send while their identity protected, and the GRC is always available to answer any questions and receive any risk. When it comes to knowledge sharing, we circulate all this knowledge within our internal communication emails and then the team ensures that whenever this critical documentation exists within our intranet, …., where people can see policies, guidelines, and other relevant information that could be beneficial not only for the champions but also for the rest of the employees"* (Participant B6).
2. A commitment to ethical principles reflected in a concern with the ethical profile of individuals and the application of ethics and the consideration of wider stakeholder positions in decision making	Met	The company's Code of Conduct reflects a commitment to ethical principles, especially in dealings with business partners and suppliers, emphasising fairness, integrity, and transparency (Document 10, p.12). Additionally, the risk awareness survey reinforces ethical risk management by promoting transparency (Participant B6).
3. A common acceptance through the organisation of the importance of continuous management of risk, including clear accountability for and ownership of specific risks and risk areas	Partially Met	Despite being from different departments, Participants B5, B6, and B9 recognize the critical importance of managing risks and clearly understand their responsibilities in this process. Notwithstanding, these positive outcomes, insights from Participant B10, who oversees the interdependence of project risks with organisational objectives, suggest that some project members still struggle to understand his role fully
4. Transparent and timely risk information flowing up and down the organisation with bad news rapidly communicated without fear of blame	Met	*"The risk management team communicates with me on the agreed time frame, if there is a lack of response they always make sure to communicate with my backup, and if my backup is also not there, they escalate to the top management straight away…"* (Participant B5). *"First of all, to report any suspicious anything, we have a whistle-blowing website, hotline, and even emails, so employees can send while their identity protected, and the GRC is always available to answer any questions and receive any risk."* (Participant B6).
5. Encouragement of risk event reporting and whistle blowing actively seeking to learn from mistakes and near misses	Met	The use of various tools for risk reporting, including whistle-blowing channels and risk workshops, encourages employees to report risks. Participant B6 highlights the range of tools available for risk reporting, confirming with Participant B1.
6. No process or activity too large or too complex or too obscure for the risks to be readily understood	Met	The company has structured its risk management system to make risks more understandable. Participant B9 notes efforts to unify risk language through a common risk appetite, assessment

		criteria, and awareness sessions. Additionally, the GRC's creation, including ERM, projects, and resilience, aims to improve risk comprehension across the organisation.
7. Appropriate risk-taking behaviours rewarded and encouraged and inappropriate behaviours challenged and sanctioned	◯ Unsubstantiated	No evidence provided supporting the reward or sanctioning of risk-taking behaviours. The absence of criteria 7 is highlighted in the conclusion chapter.
8. Risk management skills and knowledge valued, encouraged and developed with a properly resourced risk management function	🟢 Met	The company conducts regular workshops, training, and follow-ups to ensure continuous risk management (Participant B1, B9). The GRC teams are dedicated for risk management
9. Sufficient diversity of perspectives, values and beliefs to ensure that the status quo is consistently and rigorously challenged	🟢 Met	To me, at the enterprise level, I learned the depth of the company and the know-how of risk overall. But, the challenge I have is distinguishing project risks from enterprise risks and resilience" (Participant B6).
10. Alignment of culture management with employee engagement and people strategy to ensure that people are supportive socially but also strongly focused on the task in hand	🟢 Met	The alignment is evident through the active involvement of employees in risk management processes, which enhances both social support and task focus. Participants B5 and B6 describe how their engagement in risk management has elevated their sense of responsibility and professionalism.

Company B meets most of the successful risk culture criteria outlined by the IRM (2012). It also demonstrates adherence to the ISO Management System Standard (Annex, 2019), with ERM as part of GRC being driven from the top, ensuring leadership commitment and continuous support while promoting risk reporting and engagement from the bottom level. Company B's risk governance structure emphasises a proper plan, implementation, and measurement criteria. The company should use insights from these measurements to continuously improve communication with projects so that PRM co-evolves with ERM to become a self-organised system. This goal seems achievable and is likely a matter of time, given the company's recent establishment and its conducive risk culture for integration.

The findings offer a theoretical contribution to CAS by demonstrating how the structure of risk governance can influence the adaptability and evolution of risk culture within organisations. In CAS literature, organisations are understood as dynamic, interdependent systems that adapt based on interactions and feedback loops between their components (Sheth & Sinfield, 2024; Andringa et al., 2022). Company B's integrated governance structure, where PRM intersects with ERM, enables the company to establish multiple feedback mechanisms, promoting continuous learning and interaction across different levels. This integration aligns with CAS principles, where systems are most adaptive when they can exchange information freely and respond to changing conditions (Kurtz & Snowden, 2003). By fostering these feedback loops, Company B not only enhances its risk culture, ensuring that risk is managed holistically rather than in isolated silos, but also improves its capacity to evolve and respond to complexity (Sheth & Sinfield, 2024). In contrast, Company A's siloed governance structure limits these interactions, reflecting a more rigid, less adaptive system where risk management remains localised within project assurance processes. This distinction contributes to CAS by showing how risk governance structures that promote information flow and interaction are essential for creating adaptive, resilient systems, thereby strengthening the link between risk governance and culture in complex environments.

Moving on to explore the risk governance structure of Company C.

4.2.3 A Complex Adaptive Risk Governance Structure Resulting in a Self-Organised PRM/ERM Integration

Company C principal corporate offices and headquarters are in Riyadh, Saudi Arabia with major industrial operations in different industrial cites of the country. The company's manufacturing, sales, technology and innovation facilities are located throughout the globe and are managed by four regional offices: the Middle East and Africa, Asia, the Americas and Europe. ERM is an integral component of the risk management framework, alongside Business Continuity Management and Enterprise Data Management (See Figure 4.11). These three functions are accountable to the general manager of risk management. The general manager serves as a secretary in two committees: the Board Risk & Sustainability Committee (BRSC) and the Risk Management Sub-Committee (RMC). The BRSC is comprised of three boards of directors, one of whom serves as the chairman, and their primary responsibility is to ensure the independence of the ERM function. More importantly, BRSC according to the ERM Knowledge Sharing Document (Document 4) reviews the corporate risk management policy periodically to ensure consistency with the change that may occur in the internal or external environment in which the company operates, the legislation governing its business or strategic objectives or otherwise and recommending proposed changes to the board. The RMC, on the other hand, consists of executives charged by the CEO. This shows much larger allocation of resources for risk management in Company C compared to Company A, as well as a greater emphasis on adapting to the ever-changing environment. The general manager holds the belief that:

> *"This risk governance structure demonstrates the entire management team convening in a dedicated session to address risk management, although it is not a mandatory requirement. We enjoy great support from our executives and boards. ERM is a successful journey in our company, yet our ambitions go far beyond where we are now"* (Participant C3).

The company focuses on risk management and business continuity. Unlike Company A which has only one member working in ERM, Company C according to Participants C4, C7 has one director and two senior managers, each overseeing a team of four specialists. Additionally, two advisors focus on higher-level tasks, such as analysing intelligence reports, beyond the day-to-day operations.

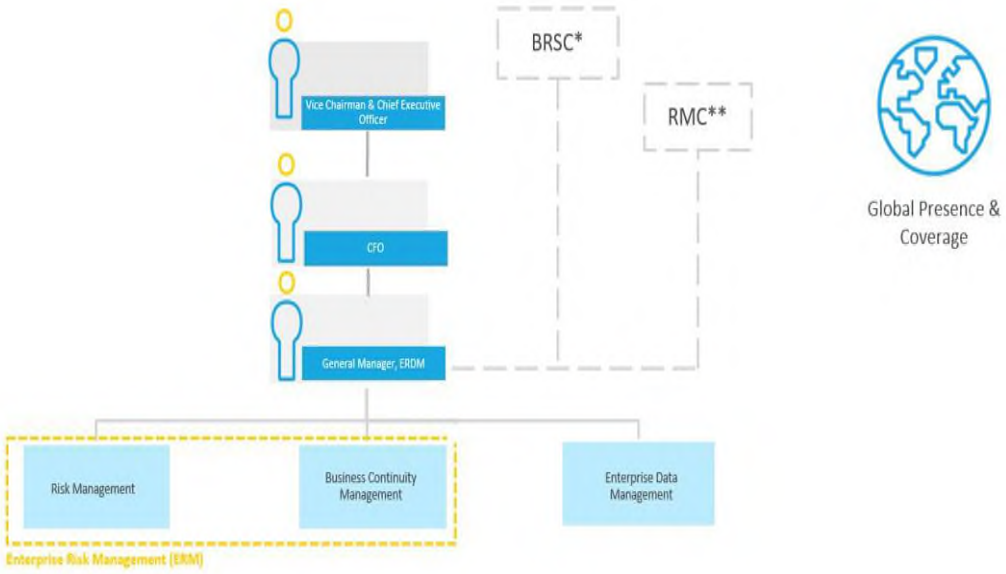


Figure 4.11: Company C's Risk Governance Structure (Document 1)

The risk governance structure accommodates the global presence and coverage as shown in the top right corner of Figure 4.11. The ERM Knowledge Sharing Document contains the ERM Governance Structure (Figure 4.12), which identifies the ERM key stakeholders, including all subsidiaries, projects, sales offices, and global manufacturing sites. It explains the operating rhythm with these stakeholders. Figure 4.13 further details that the identification of these stakeholders follows the first process in ISO 31000, specifically the scope, context, and criteria as part of defining the scope. The communication strategy between ERM and offices located outside of Riyadh, unlike Company A, for Company C it is necessary for manufacturing sites to adhere to the ERM procedure as stipulated in their joint venture agreement. In the case of sales offices, they conduct regular risk assessments, taking into account factors such as revenue, location, capacity, and the unique challenges posed by each country.

> *"It is important to note that different countries, such as China and the USA, present varying risks. Regardless of whether it is a sales office or a manufacturing site, standardised approaches are in place to guide the interaction and determine the appropriate timing for engagement. Clear expectations are established for these engagements. ERM conducts a comprehensive review of the risk register for both manufacturing sites and sales offices every three years, ensuring its renewal. The risk*

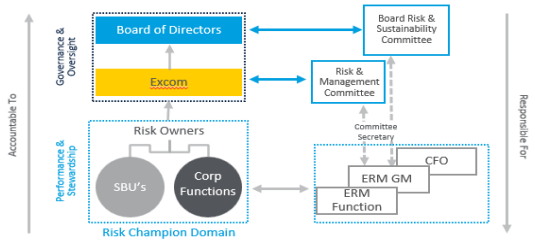
registers are either a historical base generation or a zero-base generation. The latter is used when they go from scratch where they bring the sales office objectives, what are business challenges or uncertainty that will impact achieving the objectives. The former is used when they look to their previous exercise if they have previous risks that are still active, and then reassess. Regardless, the company adheres to a standardised approach regarding writing style, content selection, formatting guidelines, colour usage, and representation methods" (Participant C4).

Company C, listed on the Saudi Exchange Market, adheres to the Corporate Governance Regulations (CGR) (CMA, 2006) (Section 1.1.1 in the introduction chapter), which mandate the establishment of a committee and naming it a "Risk Management Committee" with a majority of non-executive members (CMA, 2006, P. 41). By maintaining a centralised risk management function, Company C aligns with ERM literature that emphasises the importance of centralised oversight for risk management (Andronache et al., 2018; Kerstin et al., 2014).

At the same time, the company grants autonomy to its various functions and subsidiaries, allowing them to manage risks using their own tools while following established guidelines. This approach reflects a CAS perspective of ERM, where the interdependencies between the functions or as Sheth and Sinfield (2024) describe as “function-function interaction networks” (the parent company's ERM function and its subsidiaries in this case) are acknowledged, preparing the company to address cascading risks across the enterprise (Sheth & Sinfield, 2024). The importance of addressing risks arising from the enterprise’s organisational structure is highlighted by Sheth and Sinfield (2024), and Company C demonstrates this understanding by implementing dual approaches: top-down guidelines from the parent company and bottom-up practices tailored to the local operating contexts of its subsidiaries and functions.

By combining a centralised oversight guided by the ERM guidelines with decentralised autonomy, Company C integrates insights from two key streams of literature: those advocating for a centralised risk function (Andronache et al., 2018; Kerstin et al., 2014) and those emphasising the importance of decentralised organisational structures (van der Vegt et al., 2015). This complex ERM governance structure addresses the recent literature calling for integrated ERM frameworks that bridge the governance gap between parent groups and their subsidiaries (Makmor et al., 2023).

Governance Structure



Operating Rhythm

Activities	Monthly	Quarterly
RM Deployment at [redacted] Affiliates/Subsidiaries	• ERM LT	• BRSC • RMC
SBUs/CFs Risk Assessments Progress & Outputs	• SBUs/CFs • ERM LT	• BRSC • RMC • SBUs/CFs • RDN
Risk Management Strategic Objectives & Initiatives	• ERM LT	• BRSC • RMC • QPR

*BRSC: 3 times per year; RDN: twice a year

BRSC: Board **R**isk & **S**ustainability **C**ommittee

RMC: Risk **M**anagement Sub-**C**ommittee (EXCOM)

QRR: Quarterly **R**isk **R**eview

RDN: Risk champion Domain Network

ERM Key Stakeholders

- BRSC
- RMC
- ALL SBU's and Corporate Functions
- All Sales offices/Projects/ Major Initiatives/L&D
- Global Manufacturing sites

Figure 4.12: Company C's ERM Governance Structure (Document 4)

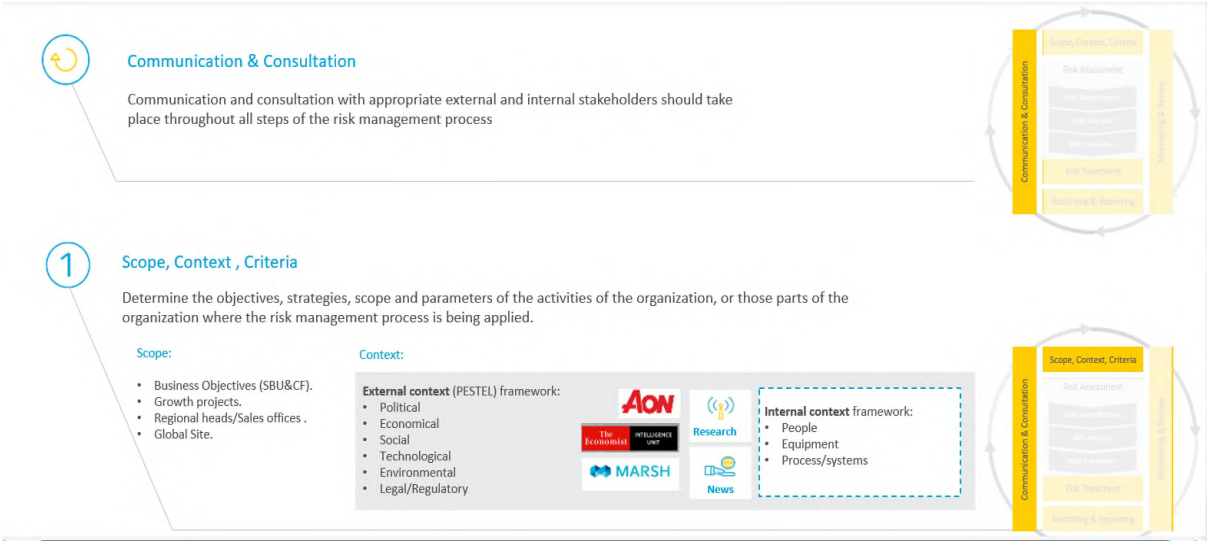


Figure 4.13: Company C Scope, Context, Criteria process based on IS0 31000 (Document 4)

In relation to projects, according to participants C4 and C6 the project function includes a dedicated risk office comprising four members and one senior manager responsible for overseeing project risks. ERM team conducts a thorough risk assessment prior to granting approval for projects. Following this assessment, the project department employs a comprehensive system consisting of five gating stages. ERM is involved by its members in gates 1 and 2 (qualitative risk assessment) to give their input. Therefore, *"during the initiation phase, PRM is responsible for engaging ERM"* (Participant C6). The rationale behind ERM's decision to not participate in all project gating systems is attributed to the significant volume of projects initiated by the company annually. During this particular incident, a project manager expressed the following views,

> *"We have annually more than 1000 projects, so there is no way ERM can be involved in each stage. Therefore, the operating model was adjusted for ERM to engage in only specific phases of the project. When we move from initiation (qualitative) and receive ERM input to calculate cost we engage with different stakeholders (corporate finance, procurement…etc) we have standards and processes mandating who should be engaged. There is a risk workshop within projects and communication between the risk office within projects and ERM. We have monthly and quarterly meetings to review risk status. So it is two ways communication, also lessons learned are shared and distributed with similar projects"* (Participant C6).

Figure 4.14 illustrates Company C's actors in Winch's Venn diagram, placing the BRSC and RMC in the owner domain, while ERM occupies the governance intersection with PRM, which has a dedicated risk office. Feedback flows between ERM and PRM, highlighting their interaction. Compared to Companies A and B, Company C emphasises institutionalised guidelines and structures while allowing autonomy for projects to use their preferred risk management tools. From an institutional theory perspective, as explained by DiMaggio and Powell (1983), organisational behaviour is shaped by external pressures, norms, and mimetic tendencies. In addition, the authors explain that coercive isomorphism occurs due to regulatory pressures or resource dependencies, which is evident in both Companies A and C. In Company A, coercive pressures from the parent company in India enforce a rigid governance model, limiting alignment with the UK market's needs. Company C, however, balances top-down

guidelines with local autonomy, recognising the complexity of the environment and giving teams discretion within standardised frameworks.

ERM's involvement in only two of the project gating stages while still receiving praise from project participants for its valuable input demonstrates the system's agility and adaptability, which is the result of accumulated practice and experience as the role of path dependency explains. This interaction reflects a mature risk management system where self-organisation emerges as agents interact based on simple rules that can evolve with accumulated experience (Anderson, 1999; Holland,1995). Projects and other functions know when and how to engage ERM within ERM general rules. The continuous role of the BRSC, reviewing and updating risk policies, acknowledges the evolving risk landscape, ensuring the governance structure adapts accordingly.

This analysis shows how institutional theory (coercive and normative pressures) complements CAS. Both perspectives help explain how Company C's governance structure, despite formal guidelines, allows flexibility and self-organisation in managing risk across its complex, global operations.

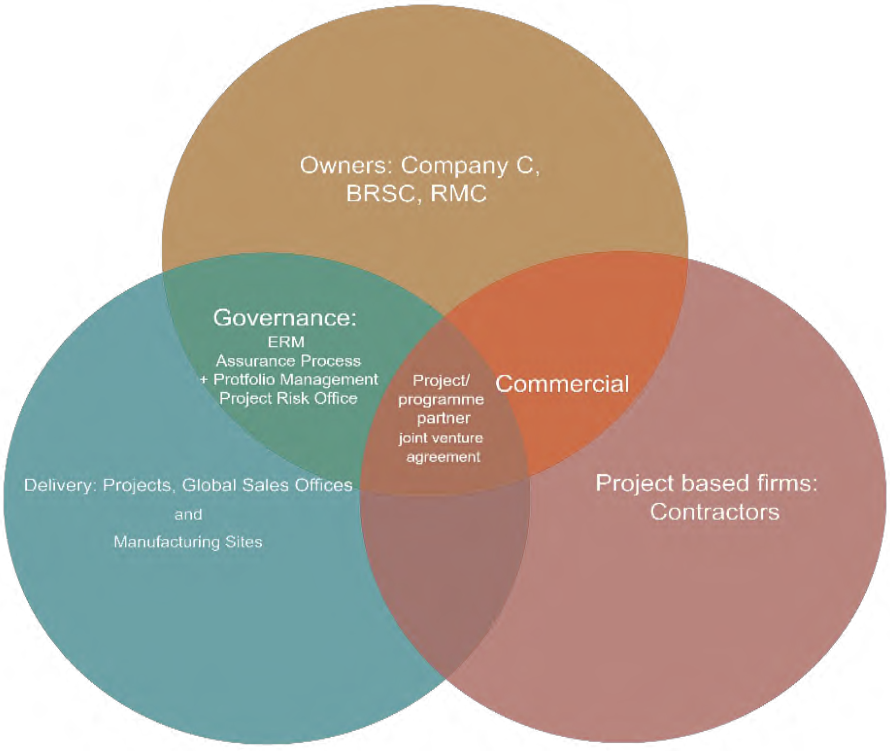


Figure 4.14: Company C's ERM and PRM Governance within Winch's Three Domains Venn Diagram

In comparison, Company A relies heavily on a siloed assurance-based PRM system, limiting integration and adaptive capacity, while Company B employs a more comprehensive portfolio management approach that integrates PRM and ERM, supporting escalation and strategic alignment (Martinsuo, 2013; Svejvig & Andersen, 2015). In contrast, Company C's long-established centralised ERM and PRM systems that use different risk management tools but aligning with ERM guidelines, fostered an adaptive, agile and at the same time institutionalised governance model. In line with CAS theory, a system consisting of all these agents, as emphasised by Sweetman et al. (2014), must remain open to its environment, as it does in Company C as in the next sub-theme.

4.2.3.1 Sustaining the ERM-Minded Culture: Integrating PRM into the ERM Management System

Participant C4 explains that the company adopts an "ERM-minded culture" that he believes is essential for effective risk management. In practice this means, appointing risk coordinators within functions and embedding ERM into management systems, therefore, the company ensures compliance through standardised procedures, ongoing engagement, and regular audits, reinforcing the importance of culture alongside formal strategies and systems.

> *"Culture easts the strategy for breakfast. The company built a strategy at the beginning of 2004 to start the ERM concept. At that time, ERM was under the umbrella of finance. With time we started growing to reach projects, manufactories, safety and environment, opportunity and so on. You grow, in large companies like ours, you cannot handle everything, you will depend on risk owners for each function to drive the ERM concept. So, first, you have to have the right culture, I would call it the ERM-minded culture; for example, if you want to start any meeting at a manufacturing site, you start with a safety moment. This requires the right level of information awareness education for other functions, and this is achieved in two different ways. First, we have a risk champion, we request each function to have one, and we call them risk coordinators, those are the ambassadors of ERM within each function. Those ambassadors we always capitalise on them where we convey to them the main messages, keeping them informed, keeping theme part of our integration strategy. We usually meet with them twice a year. We have continued engagement every quarter. The second part of having the right culture is to translate your procedures, policies, understanding, and concepts*

of ERM into a management system not only to enforce the ERM culture but also to force the organisation to comply. And how you comply is by having the standard ERM procedure that has to be implemented with frequent auditing models" (Participant C4).

The participant's quote provides further evidence of Company C's institutionalised approach to risk management, this time through the lens of ERM culture. As previously discussed in the context of Institutional Theory (DiMaggio & Powell, 1983), organisations tend to conform to institutional pressures through standardisation and formalised procedures. In this case, the ERM culture is institutionalised through the appointment of "risk coordinators" or champions in each function, which disseminates the ERM agenda and reinforces organisational consistency. The participant highlights the significance of formalised structures (ERM procedures and auditing models) that ensure compliance and embed risk management deeply within daily operations. This mirrors earlier evidence about Company C's emphasis on structured and standardised approaches, further solidifying the institutionalisation of risk practices across, subsidiaries, branches, and functions. Additionally, the focus on culture complements these institutional frameworks by ensuring that employees at all levels are engaged and empowered to act as risk owners. This evidence, viewed alongside previous discussions of institutional theory in Company C's risk management, showcases the importance of an embedded risk culture to sustain the organisation's ERM journey. Furthermore, it suggests that while formal structures are necessary, a culture fostering ongoing education and engagement is critical for long-term success (Fraser et al., 2022; Hunziker, 2021). As such Participant C4's insight can be analysed in two aspects, risk management culture and ERM as a management system.

Upon my 16-hour visit to the company, conducted over two separate visits, one notable observation which I recorded was the multiple emphases on the importance of fostering a risk management culture raised by various employees. For example, participant C6 highlighted the significance of enhancing the risk management culture while explaining the number and role of the risk management team in project management.

"The risk management team in project management conducts comprehensive training to maximize the risk management culture and facilitate knowledge sharing. They ensure everyone is updated about new risks, processes, or practices. For instance, following the Russian/Ukrainian war, the team in coordination with ERM initiated risk

*assessments related to Ukraine. These risks would have been difficult to assess accurately without the input of ERM because they provided a broader understanding beyond the project's scope, they gave us insights into the overall situation in the country. Based on their input, we could estimate the impact on wheat production and its effects on specific locations, and the implications for steel production" (*Participant C6).

Another example emphasising the importance of a risk management culture was raised, highlighting that this culture should be driven from the top.

"The tone at the top is very important. Culture is really important, and embedding it within the process is crucial. One of the things that our CEO mandates before making decisions is the risk register. And he has made it clear that if anyone is not adhering to our risk management practices, it should be brought to us as a compliance issue" (Participant C3).

Applying the successful risk culture criteria (IRM, 2012), along with a consistent tone from the top, adherence to the corporate risk management policy, and a widespread acceptance (CEO, project managers, and employees from other functions such as manufacturing sites and compliance) of the importance of continuous risk management, the company has established sanctions for inappropriate behaviour that does not comply with risk management policy and standards, as evidenced by the GM of risk management. This was farther emphasised by the compliance member:

"The compliance have Code of Professional Ethics, zero tolerance, any non-compliance risk saver, like corruption (Nzaha), they have 16 polices including conflict of interest, we have online training every year for every employee takes time and a lot of modules like chapters every month they send 2 so you don't finish it at once , with examples and illustrations not difficult but take time. This is kind of awareness session anyone don't follow get punishment. So there is no risk management practice but ethical business (conflict of interests) for example, you cannot sign up contract with a company owned by your brother, also if you are going to have interview with relatives you need to declare it, I work with my brother in a project I need to declare it, any decision you are going to take that include relationship you have to declare it. Every company has its

own code of ethical practice, and compliance management acts as the police who make sure they are enforcing the code of compliance" (Participant C9).

Additionally, granting global branches and subsidiaries the autonomy to manage their risks based on local perceptions, while adhering to ERM guidelines, and allowing projects to manage risks according to their own risk management standards while engaging in specific gating reviews for ERM input, demonstrates the enablement of diverse risk perspectives to continuously challenge the system's status quo. This approach allows various agents including projects to operate as self-organised systems, understanding when, who, and how to engage with these nested systems, including ERM. As per Byrne & Callaghan (2013), the conception of systems as self-organising under conditions of co-evolution allows us to understand governance in terms of processes that do not function merely under command and control. Company C illustrates how empowering different parts of the organisation to self-organise and adapt fosters a more resilient and responsive governance structure. An additional example that shows projects in company C functioning as self-organised systems can be drawn from a project manager's perspective about ERM describing ERM as one of the stakeholders that need to be engaged:

"Organisational risk involves the risk assessments identified by ERM to achieve our objectives. ERM is just one stakeholder among many that we need to engage; they do not have the upper hand over us" (Participant C5).

The last example of capturing risk culture emerged during an informal conversation over lunch break with four employees. One participant while discussing transparency as a key element for knowledge sharing, associated it with the company's ERM culture.

"Sometimes I find project teams are not transparent, and sometimes I find other project teams are transparent. Overall, the ERM culture in this company has a good level of transparency, which is important as we continuously work on improving the integration of ERM with growth projects" (Participant C8).

Looking at the Enhancing Risk Management Capabilities, part of document 4, it shows not only risk management skills and knowledge valued, encouraged, and supported, but also an alignment of culture management with employee engagement. Participant C1 explains:

"First, the Risk Management Competency Development Programme (this is in line with HR to see where the employees are and where they need to be, what is the minimum requirement in the current position for risk management). Second, instructor-led classroom training delivered by the organisation's risk management team (2-4 training sessions, physical attendance at the company academy). Third, specialised focused workshops in various sectors: petrochemicals, human resources, etc., and for this, risk assessment and awareness sessions are supplied in advance. Fourth, there are rotational engagements. Finally, engaging with/hosting external parties (between the company and various consultants)" (Participant C1).

In the context of ERM, every ERM member is expected to run at least four awareness sessions a year at different levels and functions.

Last year (2021) we conducted eighty risk workshops. The content of these awareness sessions includes what does risk means what is the difference between risk and issue, why do you need ERM and then we give them highlight how to conduct risk assessment at a high level. Every three years, ERM conducts a risk maturity model assessment. This assessment follows a bottom-up approach, starting from individual departments. It involves identifying and evaluating all potential threats and opportunities within each department, followed by a filtering process as we move up the organisational hierarchy" (Participant C4).

Table 4.3: Company C's Risk Culture according to (IRM,2012)

Criteria	Status	Evidence/ Comments
1. Distinct and consistent tone from the top, from the board and senior management in respect of risk-taking and avoidance (and also consideration of tone at all levels)	Met	*"The tone at the top is very important. Culture is really important, and embedding it within the process is crucial. One of the things that our CEO mandates before making decisions is the risk register. And he has made it clear that if anyone is not adhering to our risk management practices, it should be brought to us as a compliance issue"* (Participant C3).
2. A commitment to ethical principles reflected in a concern with the ethical profile of individuals and the application of ethics and the consideration of wider stakeholder positions in decision making	Met	*"The compliance have Code of Professional Ethics, zero tolerance, any noncompliance risk saver, like corruption (Nzaha), they have 16 polices including conflict of interest, we have online training every year for every employee takes time and a lot of modules like chapters every month they send 2 so you don't finish it at once , with examples and illustrations not difficult but take time. This is kind of awareness session anyone don't follow get punishment. So there is no risk management practice but ethical business (conflict of interests) for example, you can't sign up contract with a company owned by your brother, also if you are going to have interview with relatives you need to declare it, I work with my brother in a project I need to declare it, any decision you are going to take that include relationship you have to declare it. Every company has its own code of ethical practice, and compliance management acts as the police who make sure they are enforcing the code of compliance" (Participant C9).*
3. A common acceptance through the organisation of the importance of continuous management of risk, including clear accountability for and ownership of specific risks and risk areas	Met	*"Organisational risk involves the risk assessments identified by ERM to achieve our objectives. ERM is just one stakeholder among many that we need to engage; they do not have the upper hand over us"* (Participant C5).
4. Transparent and timely risk information flowing up and down the organisation with bad news rapidly communicated without fear of blame	Met	*"So there is no risk management practice but ethical business (conflict of interests) for example, you cant sign up contract with a company owned by your brother, also if you are going to have interview with relatives you need to declare it, I work with my brother in a project I need to declare it, any decision you are going to take that include relationship you have to declare it. Every company has its own code of ethical practice, and compliance management acts as the police who make sure they are enforcing the code of compliance"* (Participant C9).
5. Encouragement of risk event reporting and whistle blowing actively seeking to learn from mistakes and near misses	Met	*"If you want to start any meeting at a manufacturing site, you start with a safety moment. This requires the right level of information awareness education for other functions"* (Participant C4).

6. No process or activity too large or too complex or too obscure for the risks to be readily understood	Met	*"This risk governance structure demonstrates the entire management team convening in a dedicated session to address risk management, although it is not a mandatory requirement. We enjoy great support from our executives and boards. ERM is a successful journey in our company, yet our ambitions go far beyond where we are now"* (Participant C3).
7. Appropriate risk-taking behaviours rewarded and encouraged and inappropriate behaviours challenged and sanctioned	Met	*"The tone at the top is very important. Culture is really important, and embedding it within the process is crucial. One of the things that our CEO mandates before making decisions is the risk register. And he has made it clear that if anyone is not adhering to our risk management practices, it should be brought to us as a compliance issue"* (Participant C3). *"The Compliance have Code of Professional Ethics, zero tolerance, any non compliance risk saver, like corruption (nzaha), they have 16 polices including conflict of interest, we have online training every year for every employee takes time and a lot of modules like chapters every month they send 2 so you don't finish it at once , with examples and illustrations not difficult but take time. This is kind of awareness session anyone don't follow get punishment. So there is no risk management practice but ethical business (conflict of interests) for example, you cant sign up contract with a company owned by your brother, also if you are going to have interview with relatives you need to declare it, I work with my brother in a project I need to declare it, any decision you are going to take that include relationship you have to declare it. Every company has its own code of ethical practice, and compliance management acts as the police who make sure they are enforcing the code of compliance" (Participant C9).*
8. Risk management skills and knowledge valued, encouraged and developed with a properly resourced risk management function	Met	*"First, the Risk Management Competency Development Programme (this is in line with HR to see where the employees are and where they need to be, what is the minimum requirement in the current position for risk management). Second, instructor-led classroom training delivered by the organisation's risk management team (2-4 training sessions, physical attendance at the company academy). Third, specialised focused workshops in various sectors: petrochemicals, human resources, etc., and for this, risk assessment and awareness sessions are supplied in advance. Fourth, there are rotational engagements. Finally, engaging with/hosting external parties (between the company and various consultants)"* (Participant C1).
9. Sufficient diversity of perspectives, values and beliefs to ensure that the status quo is consistently and rigorously challenged	Met	Granting global branches and subsidiaries the autonomy to manage their risks based on local perceptions, while adhering to ERM guidelines, and allowing projects to manage risks according to their own risk management standards while engaging in specific gating reviews for ERM input, demonstrates the enablement of diverse risk perspectives to continuously challenge the system's status quo.

		"Organisational risk involves the risk assessments identified by ERM to achieve our objectives. ERM is just one stakeholder among many that we need to engage; they do not have the upper hand over us" (Participant C5).
10. Alignment of culture management with employee engagement and people strategy to ensure that people are supportive socially but also strongly focused on the task in hand	Met	The Enhancing Risk Management Capabilities, part of document 4 shows not only risk management skills and knowledge valued, encouraged, and supported, but also an alignment of culture management with employee engagement.

Thus, Company C places a strong emphasis on fostering a culture centred around compliance, transparency, adaptability, learning, and resilience when dealing with risks. According to Boulton (2012), adaptability in self-organised systems is enhanced through diversity and interconnectivity. For example, PRM in Company C is empowered to have its own risk management standards while adhering to ERM guidelines. This adherence facilitates interconnectivity among various agents, including projects and finance, which Participant RP1 refers to as “the common denominators”. This approach strikes a balance between laissez-faire and strict control modes of operating (Boulton, 2012). This balance differentiates Company C from Company A. While Company A has diverse risk perspectives across functions, the lack of top-level guidelines that unify common terminology and understanding leaves the agents working in different directions and hinders top-level making the right decisions.

In short, to answer How are ERM and PRM adopted in the organisations' understudy? And how can governance especially risk governance influences the concept of self-organisation, a key element of CAS, in shaping the integration of PRM and ERM? And What role does risk culture play in the integration of PRM and ERM?

The integration of ERM and PRM in the organisations under study reflects distinct governance approaches and risk cultures that influence their integrated and adaptive capacity. Company A’s siloed PRM system, guided by top-down, rigid governance, shows how a lack of complex yet interconnected risk governance structures hinders adaptability—a key feature of CAS (Holland, 1995). The closed risk culture further restricts interactions between different levels of the organisation, thereby weakening the emergence of new structure and adaptive behaviours (Hunziker, 2021) that integrate PRM with the strategic objectives.

Although Company B’s governance acknowledges the complexity of managing multiple projects with dual PRM oversight—balancing GRC integration with individual project risks, the system has not yet achieved full self-organisation. Path dependency plays a significant role in this lag, as Company B is newly established, and historical decisions and structural constraints still influence its progression towards a self-organised system. The governance structure, while enabling adaptability (Martinsuo, 2013), is still evolving. The challenge in Company B lies in the alignment between PRM and ERM, where governance fosters adaptability but the

interactions and feedback loops required to fully integrate these systems are still maturing. Despite Company B's generally open culture and alignment with most of the IRM's criteria for a successful risk culture, certain cultural factors still contribute to ongoing challenges. Specifically, some project members still struggle to understand the role of the PRM director at the GRC level, who manages the interdependence between project risks and broader organisational objectives and how PRM connects with ERM. This indicates that, while the governance framework is well-established, the risk culture has not yet fully matured to support a self-organising system as per CAS principles.

Company C, on the other hand, exhibits a governance structure that allows both decentralisation and clear tone from the top, aligning PRM and ERM through consistent engagement. Here, risk governance plays a significant role in fostering self-organisation by enabling various agents within the organisation to adapt while maintaining alignment with ERM (Boulton, 2012). The strong risk culture of openness, compliance, learning, and adaptability enables this alignment, supporting the CAS principle that interconnected systems are more resilient and capable of responding to emerging risks (Kurtz & Snowden, 2003). Risk governance in Company C enhances inter-agent communication and feedback loops, facilitating continuous learning and integration.

Given the different risk governance structures—one establishing ERM independently of the parent company, another adopting a GRC model, and the third emphasising risk management and business continuity—a key question arises: What strategic drivers and organisational imperatives underlie ERM adoption, and how do these shape the effectiveness of its integration with PRM? This leads to the third emergent theme: Strategic Imperatives and Organisational Drivers of ERM Adoption: Implications for PRM-ERM Integration Effectiveness, which is discussed next.

4.3 Strategic Imperative and Organisational Drivers of ERM Adoption: Implications for PRM-ERM Integration Effectiveness

4.3.1 Inward-Facing ERM Adoption: Focusing on Internal Integration Over External Engagement

In the case of Company A, the impetus behind establishing ERM reflects an inward–facing goal to integrate the risk management process across the various departments in the UK site.

> *"I think the reason why I was put in the role was when I was working in internal audit, we had some risk registers with each function. So each function had a risk register, and every quarter we would meet those functions, we would go through the risk register and say, you know, is anything still changed, and then that risk register would get put back away for a quarter, it wouldn't get reported anywhere within the business. And I was asking them, what do you get out of this process? Do you get anything? And they would basically say No, we just do it, because you've asked us to do it, we don't really get anything out of it. So if nobody really knows what's on it, it's not reported to anybody within the business, it doesn't add any value, then it's almost a waste of time…Our company's middle management level manages risk effectively, and they make risk management decisions. However, neither the C-suite nor the board receives any information that would allow them to see. You can think of a piece of equipment that, for whatever reason, is not in excellent condition on the construction site. If someone in the business's middle management were to make a decision to continue using the equipment, it would continue to function normally. This increases the likelihood that it will break down at some point, but nobody is aware of this. So, I merely desired a procedure that alerts the senior management to such occurrences, so they could decide whether or not to take action, but at least they had the necessary information to do so rather than being in the dark."* (Participant A1).

The participant perceived that the company's risk management practices were not adding value, which is the ultimate objective of risk management (ISO 31000, COSO, 2017; PMI, 2017). This was attributed to each department managing risks in isolation, leading to a fragmented, siloed approach rather than an integrated system that could effectively support the organisation's broader strategic objectives. Byrne & Callaghan (2013) describe an isolated system as one that does not exchange energy nor matter with its environment. Such a system is reflected in Company A, which as noted by Participants A1 and A3, possesses too many risk management processes because some employees who have joined the company have

brought with them processes they have observed at other companies, which they have subsequently implemented for their own departments. As a result, the company ends up with many distinct ways of conducting risks. Although diversity is what makes complex systems creative, such systems should not operate randomly (Boulton, 2012). Therefore to address this fragmented risk management practice, ERM was proposed by Participant A1, aiming to bring the company to the edge of chaos, where systems are more adaptive and capable of self-organising (Cox et al., 2009). The ultimate objective was to have a standardised framework and procedure throughout the company so that various employees from different departments could fit into different roles. As explained in the first theme, the Document, Enterprise Risk Management Framework of Company A (Document 7) sets out the key components that provide the foundation for designing, implementing, monitoring, reviewing, and continually improving risk management throughout the company. I have already criticised the designing phase for excluding the parent company. Additionally, evidence showed most of the participants were defining risk in silos without any interrelated elements exhibiting a fragmented and chaotic system. To assess the implementation component, I explained in the second theme that the company's approach to implementing ERM is through delivering risk workshops to senior managers, including heads of departments. Therefore, I present insights from two such heads of departments (Participants A7 and A8) who were involved in these workshops.

> *"We have actually made the risk management more mature. So, we have a Chief growth officer, so we've got an individual responsible for risk sitting at the board level, that's good, but that's not always been the case in the past. It gave me more encouragement to manage risk because there is somebody in the central location of our organisation looking at this from the business perspective. It's always better for us, particularly for the senior stakeholders in the business that the message does not always come from one individual, but it's a consistent message from various functions in the business. But more dedicated resources are needed to enforce the process especially, in current times when organisations face financial challenges. Often organisations forget about resources, they just go after tools, because they believe that tools can do everything. So, the challenge for many organisations is the continuity of that process. We're talking about a department or individual managers managing*

enterprise risk, but how do we manage the risk of that individual not being able to manage that risk? Will we have continuity of that process going forward? This company like other companies does not look at the process itself, they consider having a risk management process in the organisation, but there are risks involving the risk management process. So, how do organisations manage the risk of managing the risk in the business?" (Participant A7).

The head of IT Department (Participant A7) was delighted that there is now a central function looking at all the company's risks and potentially attempting to identify any connections between the risks identified by his department and those identified by other functions. Since information and knowledge are dispersed throughout the complex system (including IT risks, project risks, legal risks, etc.), it is essential to gather these different perspectives to understand the situation fully (Nisula, 2018). As these elements are interconnected, the associated risks also become interconnected, forming complex problems that should not be managed in a fragmented manner. For example, the participant provided the example of a disaster recovery system that not only mitigates risks from a cybersecurity standpoint, but also from an IT infrastructure standpoint. Thus, for him, it is reassuring that somebody is looking at those duplicated risks across the business that refer to the same root cause, which encouraged him to continue working on the risks. Therefore, introducing ERM as a systematic umbrella to serve as a comprehensive framework that looks at the complex interconnected relationships of risks. This was echoed by the other participant, the head of the Legal Department (Participant A8) who mentioned that risk management became more comprehensive and structured than before, resulting in a greater number of risks being identified in the department than before.

"We went through some of the processes and some of the key risks. And we updated our risk register to capture things that were a concern. That resulted in more, I suppose more risks are identified than we had previously. I suppose my observation is it seems quite well structured. It's a bit clearer, and probably a little bit less cumbersome than I've seen in previous iterations, quite focused..." (Participant A8).

This means these systemic risks are intertwined with different organisational processes, extending beyond the realm of IT and Legal to encompass project management. As per Joubert & Snyman (2021), the proactive handling of systemic risks holds the potential to

significantly enhance the integration of PRM and ERM, delivering benefits to both ongoing and future projects. But the current ERM implementation approach centres on senior managers only, revealing several drawbacks. First, as reported by the project lead (A2) in the second theme the senior managers have limited time to discuss risk management, representing a sociopolitical issue related to their commitment to it. Furthermore, those who showed encouragement such as Participants A7 and A8 struggled to sustain the process with top managers given their high turnover rate, as noted by Participant A1 in the previous theme. This supports Participant A7's concerns about the continuity of the risk management process. In contrast, in the next sub-theme, I will discuss how Companies B and C ensure continuity in their risk management practices, contrasting their approaches with the challenges faced by Company A.

To analyse the driver and the adoption of ERM in Company A, institutional theory offers a clear perspective. Mimetic isomorphism, as described by DiMaggio and Powell (1983), occurs when organisations imitate practices from others perceived as successful or credible to reduce uncertainty. In Company A employees introduced risk management practices from previous employers reflects this mimetic dynamic. Miterev et al.(2017) and He et al.(2016) highlight how organisations often adopt proven practices from other firms, but in Company A, this led to the implementation of various processes without strategic coherence. This issue was compounded by coercive pressures from the parent company in India, which imposed a rigid governance model that treats UK projects similarly to those across other global subsidiaries. This approach limits the UK site's ability to adapt to local market conditions, resulting in inefficiencies and strategic misalignment. This supports the findings of Miterev et al.(2017) and He et al.(2016) that mimicry can perpetuate inefficiencies when practices are not contextually adapted.

4.3.2 Ensuring Continuity in Risk Management: Lessons from Companies B and C

In comparison with Company A, resilience as in Company B and business continuity as in Company C were proven to be essential when planning an ERM governance structure. In particular, the two structures preserve the core functions, structure, and feedback mechanisms of the risk management system, ensuring it remains within a stable regime. Business continuity addresses how long a company can operate without disruptions (Assibi, 2022). Thus, both resilience and business continuity reflect the extent to which a CAS can self-

organise and maintain its ability for learning and adaptation (Norberg et al., 2008). However, Company A remains in a chaotic state, in contrast to the adaptive capability demonstrated by Company B and the adaptive and self-organised capabilities demonstrated by Company C. These companies' resilience and business continuity allowed them to recover and thrive in the aftermath of major crises.

> *"I can give you an example today you have a project and because of COVID (resilience), the manpower number got reduced due to the number of positive cases (project risk on schedule), so you have to talk to recruitment and board to help you get an exemption to talk to other ministries to get employees from other countries outside the covid travel ban. Since it links resilience, projects, and enterprises to provide you the whole picture, this demonstrates the suitability of our model*" (Participant B2).

The participant provides an example of how Company B's risk governance structure helped maintain resilience during the COVID-19 pandemic. This was achieved by implementing a resilience-focused risk response, which involved coordinating with recruitment teams and government ministries to secure resources from countries not affected by the travel ban. Similarly, the examples from Company C highlighted how its robust business continuity plan, as an integral part of its risk management governance structure, allowed the company to remain unaffected during crises such as the Russian/ Ukraine War, demonstrating the effectiveness of its approach to sustaining operations in the face of disruptions.

> *"We have employees in Russia we cannot pay them, but because we have a document in our business continuity telling you what to do if banks collabs or something like that, we have some financial channels to pay them if Swift is collabs (confidential information), so no effects on their payment. Another example, some customers could not pay during the pandemic, but because we had about 10-20 response plans helped us to keep our liquidity (confidential information). Another example, we were working from home before the pandemic and we have already a good infrastructure, so our business never stopped even during the pandemic".*

However, Company A should not expect to achieve strong resilience simply by adding resilience or continuity measures to its current risk governance structure in response to this structural complexity. The company is facing deeper, more fundamental issues that must be

addressed. For example, Participant A8 adds uncertainty regarding the subsequent handling of reports once risks have been identified and escalated to other committees. Specifically, he observed that after providing his input, these reports disappear without any clear feedback loop, thereby lacking a fundamental element of CAS for the follow-up process with ERM. In addition, he was unsure whether the identified risks were targeted and specific enough to make management aware of clear and present risks that were going on within the business.

> *I suppose at my level, I don't necessarily see what happens to those reports. Once you identify a risk, and it goes up into other committees, it's sort of I input into it, and then it disappears. That's not to say that a subtle level above me sits in the Risk and Audit Committee meetings, and they discuss some of these risks but don't necessarily have a loop where it comes back round. I also fear it gets into a theoretical view of risk management in the sense that some of the risks that we have now are a little bit too generic. For example, if someone initiates a claim procedure against us it doesn't feed through to legal quickly enough for us to react to it, or people don't recognize that it's a legal issue that needs to be dealt with, or they try to manage it themselves, and it blows up. And we end up with a high court writ against us for winding up before we even know about it before it reaches us. And I think of projects that are ongoing, that if we don't resolve them quickly, they would, present a clear and present threat to our current needs of trading. I won't go into any detail on them. But they're almost like BAU items that just need to be handled and managed through BAU's day-to-day work process, but they should also be maybe tracked as a key risk to the business and then managed that way. And I don't know theoretically, whether the two need to be theoretical, process-driven risks that we need to track at a higher level and fix those systemically so that they don't go awry, or whether we ought to be tracking to the risk management process specific ongoing projects that need to be resolved, because I perceive those as an equal or actually more present danger than some of the theoretical risks"* (Participant A8).

The participants' concern regarding the uncertainty surrounding what happens to reported risks after escalating to higher committees is captured in the Document, Existing Risk Communication & Reporting (Document 8), which highlights unclear and inconsistent risk monitoring and reporting processes from Departments/Functions to Senior Management and

the Boards. In projects, the deficiency in monitoring and reporting has reduced the number of project risks reported from the project level to the senior management as project managers recognise that the senior management and the boards will not consider all identified risks.

> "*The risk register might have 100 items on it, and the Chief Operating Officer will report the 4-5 issues from the risks particularly those associated with technology, cost, and schedule, usually cost and schedule are the big issues"* (Participant A6).

While it is not uncommon for top management to prioritise specific risks associated with the company's risk appetite, the boards according to Document 8 prioritise the principles risks based on executives' personal opinions but no consensus across departments/functions. This lack of alignment contradicts a key criterion of the IRM (2012) framework for a successful risk culture, which emphasises the importance of aligning culture management with employee engagement and people strategy. As a result, the less visible risks that were overlooked knowing that top management would not consider became issues for the company.

> *"We don't report all risks, but the major risks because we know the top managers will not take all the risks, so some risks remain invisible. Then, you are surprised terrible things happen because those risks were lingering for a while"* (Participant A2).

The focus on identifying only technical risks is evident in Participant's A5 definition of risk: **"**Everything that affects time, schedule, cost, safety, or quality of the project in delivering the project". This focus has led some project managers to become inflexible when dealing with risks that could impact these specific project constraints, while being more cooperative in addressing risks related to areas like health and safety. For instance, Participant A3 observed that project managers tend to be less cooperative when it comes to risks that might affect their project's scope, time, and budget.

> "*I think in terms of process safety, and health and environment, project managers are very cooperative because that's what will drive whether a project meets the objective or not, it has to comply with regulations. But in terms of risk register, like wide project risk register, we're talking now and things that might affect the schedule or things that might affect delivery on budget, maybe less so because as a project sort of grows or progresses, if something is identified later down the line, that means a scope change as a result of a safety issue or an environmental issue. In terms of the project*

management side, they're not as receptive to that change because it's going to affect their scope growth, budget, and the do delivery on time" (Participant A3).

However, according to Hillson (2006), the main reason organisations fail to achieve the business objectives is the tendency to focus more on tactical rather than strategic objectives. Previous studies show that business objectives and clear vision are critical factors for the successful implementation of ERM (Jean-Jules & Vicente, 2021). In particular, the organisational values serve as attractors governing complex systems (Cox et al., 2009). Ironically, the organisational values of Company A stand in stark contrast to its risk management practices. The company claims three core values: sustainability, governance, and avid learning. However, these values are undermined by its risk management actions. First, while sustainability is a stated value, it is contradicted by the company's unsustainable risk management processes, which lack long-term focus and effective follow-up. Second, the value of governance is intended to improve risk management by consolidating processes, yet the exclusion of key stakeholders from the ERM framework directly conflicts with this goal. Lastly, despite promoting avid learning, the company's siloed approach to risk management hinders cross-functional learning and integration resulting in siloed risk perspectives and practices, further contradicting this core value.

Therefore, the effectiveness of ERM integration with PRM in Company A was constrained by an inward-facing goal that drove its implementation. The initiative primarily led by middle management, aimed to address the issue of silo risk practices but failed to fully engage senior leadership. This limited buy-in from top management hindered the deep integration of ERM with PRM, as senior managers are crucial to driving this integration, but they often lacked the time and commitment to fully engage with ERM processes. Consequently, there was a gap between the strategic intent of ERM and its operational execution in projects. While the inward focus on standardising risk management across departments contributed to greater organisational cohesion in Company C, it overlooked the distinct and dynamic requirements of PRM in Company A. This gap arose from the lack of a dual top-down and bottom-up approach, which, as demonstrated by Company C, allows for greater autonomy and adaptability to the specific context of projects. Moreover, the lack of a robust feedback mechanism further weakened this integration. Risks that were escalated to higher committees often disappeared from the view of those who initially identified them, creating uncertainty

about their management. This disconnect underscores a critical flaw in Company A's ERM approach while it focused on internal standardising processes, it neglected the adaptive feedback loops essential for effective PRM integration, as emphasised by CAS theory. In contrast, the next sub-theme will explore how external factors, such as market growth pressures and reliance on external parties, influenced the ERM implementation in Companies B and C.

4.3.3 The Role of Organisational Values and External Interdependencies in Shaping the Integration of ERM and PRM

In contrast to Company A, where inward goal primarily drove ERM implementation, Companies B and C demonstrate a connection between their organisational values and the external drivers of their ERM initiatives. For example, Company B's values are responsibility, collaboration, passion, and respect. Collaboration in particular is linked to the company's main motivator for designing the GRC model which is according to Participant B1 “to enhance its relationships with outside parties”. The GRC senior manager (Participant B1), when asked about the motivation for implementing the GRC model states that "We heavily depend on experts outside Saudi so some processes are taking longer than they should be”, and the project risk director at the GRC level (Participant B8), states that "We are a very large company dealing with external parties various ministries, macroeconomics”. Therefore, for company B, there was much more recognition of the complexity of the environment in which the company operates leading the company establishing a unique risk management system. In other words, there was much more recognition of the structural complexity involved in the company's scope of work.

> *“We are spearheading a new model of development, putting people and planet first and leveraging the most innovative concepts and technologies to deliver projects that actively enhance the well-being of customers, communities and environments. We take a comprehensive approach to setting new standards in good governance, compliance, and risk management. We have embedded a holistic approach to structural governance into the business at every level, from construction through to hospitality operations.” (Company B’s Corporate Governance Overview).*

The company’s corporate governance statement aligns with its value of collaboration, reflecting the complexity highlighted in tourism and hospitality literature due to the

coordination required among various internal and external parties (Elshaer et al., 2023). Participant B2 provided context by discussing the impact of COVID-19, which led to a reduction in project manpower and prompted top managers to use the GRC model to engage with ministries and secure resources from countries outside the travel ban. This response illustrates the actions mentioned by Participant B1 in the first theme, where the company works with the PIF and various ministries to address internal issues. Therefore, top managers are responsible for importing external knowledge and integrating internal knowledge (Mitchell, 2006) and are the main agents responsible for developing and changing organisational structures and policies, including the values and culture within an organisation (Liang et al., 2007). Since all these changes are needed for successful ERM implementation (Jean-Jules & Vicente, 2021), how do top managers ensure these strategic objectives and values are integrated at the project level?

> *"There was recognition with ERM that there was insufficient project experience to deal with what you said especially in the early days of a project organisation. So, I was put to look at any strategic risks that impact projects and also to assure what project risk teams do, so there is a project risk director that sits inside the delivery team and they do all the review and workshops and I attend them sometimes and I would check they are accurate and meet our standard and the mitigation actions are closed on times. So from that perspective, I appreciate that we cover any gaps that are missed and also they appreciate that we deal with high-level impactful risks that they themselves cannot because project delivery is just one department and there are 20 of them between legal, safety, environment…etc. so from that perspective, they are very grateful, but it is foolish to think that there are no clashes, my role is constantly confused with the project delivery project risk director role and you know I am always having to answer why we need that many levels in risk management. That's an easy question because we are basically a very large dealing with external parties various ministries, macroeconomics"* (Participant B10).

Therefore, the appointment of project risk director at the GRC level (B10) is crucial in aligning project risks with GRC guidelines, highlighting the importance of external relationships in managing interdependencies among project risks. This complexity illustrates the organisation's need to balance internal capabilities with external interactions, which is vital

for effective risk management. By fostering communication across organisational levels and external entities as advised by the IRM's risk culture criteria and CAS principles, the project risk director at the GRC level exemplifies an adaptive response to the complex risk landscape. This approach acknowledges that risk management is a dynamic system, not a linear process, enhancing the organisation's resilience and adaptability.

A more integrated approach is found in Company C, which established ERM for two main reasons: first reason related to business requirement that is to increase the level of assurance to achieve strategic objectives. The General Manager of Risk Management explained the business drivers to establish ERM stating:

> "The company is operating in a highly complex and increasingly changing environment. As we strive to grow the business by exploiting opportunities across multiple countries and in multiple markets, we have to be fully aware of the potential risks we will face. In today's evolving environment, all activities undertaken by our company come with a level of risk. To respond to this challenge, the company has established the ERM department with the aim to increase the level of assurance to achieve objectives".

This is in line with (Khan et al., 2016) who found that the existence of growth opportunity plays a role in motivating firms to adopt ERM. Company C has achieved notable growth, expanding its operations to encompass more than 50 countries and establishing a global workforce exceeding 32,000 employees. The company's global presence is undergoing rapid expansion, supported by ambitious plans for growth that involve the development of an extensive infrastructure comprising manufacturing plants, technology centres, distribution centres, offices, and storage facilities across the world. Within such ambitious growth, the company claims: "This strategic infrastructure allows "Company C" to efficiently meet the demands of its customers in key markets globally". Company C strategically manages its manufacturing, sales, technology, and innovation facilities on a global scale through four regional offices: the Middle East and Africa, Asia, the Americas, and Europe. This organisational approach ensures a cohesive and effective management structure, enabling the company to respond proactively to the diverse needs of customers in various regions.

This recognition of external complexities aligns with its value of *inspire*, promoting a culture where employees are encouraged to innovate and proactively address risks as opportunities.

A second reason is related to legal requirements that is to establish and govern a risk management system and demonstrate its effectiveness and operability, which is required by Capital Market Authority, CMA through corporate governance law in 2006 in Saudi Arabia, which is not required for Company B because it is not yet listed in the CMA. Bohnert et al. (2017) claims that the surge in ERM implementations is significantly influenced by regulatory pressures. Thus, the increased regulatory pressure on firms regarding the transparency of their corporate governance and other compliance related regulations is a factor for organisations to adopt ERM (Beasley et al., 2008; Eckles et al., 2014; Hoyt and Liebenberg, 2011; Onder and Ergin, 2012).

Thus, the establishment of the ERM department in Company C exemplifies a strategic recognition of the complex relationship between external market dynamics and internal risk processes. This integration not only facilitates a holistic understanding of risk but also fosters adaptability in a rapidly changing environment. This is evidenced by the dual approach that allow project agents to use their own risk management standards while adhering to ERM guidelines, achieving a balance recognised by CAS. The autonomy granted to project managers demonstrates the second value of Company C, *create*, as they innovate their own solutions to effectively manage risks while ensuring alignment with broader organisational objectives. As a result of such adaptive strategy and approach agents on the micro levels including project managers and members of compliance department acknowledged the role of ERM and thus can see its values. For example, a member of the compliance team states: "the role of ERM is legitimacy put the general rules and policies and procedures and other departments enforce ERM reporting" (Participant C9). Participant 11, a project manager states:

> *"Their role (ERM) appears when associating project risks to strategy because we don't have a full vision about the link to strategy. We were speaking different language with ERM, but after embedment and change management, we started to see the value*" (Participant C11).

Another project manager elaborated on the values of ERM integration with projects outside the country providing examples from his memory as follow:

> *"I will give you two examples: in the US, we were having giga project (multi billion), there was trading competition in that time between US and China, and anti-dumping*

tax was identified with ERM with Trump administration the mitigation plan agreed with stakeholders was to spare 16% from cops for these taxes in case it applied to the project. We assigned kind of lope of communication to support the engagement with different parties. Now, project operates and we see the effect on IRR, so this 16% was avoided otherwise we would pay about $300m. In general, inside Saudi Arabia, I think we might be inherited risk management and we know ERM requirements it is part of our DNA, so maybe their effect inside Saudi Arabia is not that high as outside" (Participant C6).

Given the above discussion, the findings regarding the organisational values, external interdependencies for ERM implementation highlight several critical insights into the integration of PRM and ERM within the context of Companies B and C.

- **Recognition of Complexity**: Both Companies B and C demonstrate a sophisticated understanding of their operational environments, which significantly influences their approach to GRC and ERM. This acknowledgment of external complexities enables them to develop more adaptive and responsive risk management strategies that integrate effectively with PRM. In contrast, Company A's more rigid, internally focused ERM implementation failed to account for external influences, leading to ineffective integration.
- **The influence of values on risk management practices** is evident in the contrasting approaches of Companies A, B, and C. While Company A's internal drivers reflected a disconnect between its organisational values and risk management practices, Companies B and C exhibit a strong alignment between their values and their risk management frameworks. For instance, the values espoused by Company C—Inspire, Engage, Create, and Deliver—foster its culture of collaboration and proactive management. This cultural alignment facilitates better communication and understanding between project teams and the ERM department, promoting more effective integration of risk management processes.
- **Adaptability and Resilience**: The findings underscore the importance of adaptability in managing risks within complex environments. By integrating external motivations such as market growth and enhancing relationships with external stakeholders into their ERM frameworks, Companies B and C exemplify the adaptive capability

highlighted in CAS theory. This adaptability is crucial for resilience, allowing organisations to navigate uncertainties effectively.

Through the lens of Maylor et al.'s (2013) dimensions of complexity as outlined in the literature, the different geographical locations between the parent company and the subsidiary that is Company A, and the too many risk management processes exhibit a structural issue. This structural complexity has posed challenges for Company A in meeting the ISO Management Control System criteria (Figure 4.7), particularly in planning the scope of the ERM initiative and developing a common risk language. Additionally, the high turnover in senior management has introduced emergent complexity, affecting the continuity of the ERM process, as noted by Participant A7. The lack of top management support for ERM endorsement, combined with differing departmental agendas and inconsistent risk management processes, highlights sociopolitical complexity. Participant A8's remarks underscore conflicts in prioritising departmental risks over ERM-level risks. Managing this sociopolitical complexity can be improved through development activities that focus on stakeholder engagement, project leadership, and change and communication management (Maylor et al., 2018). Therefore, I use Lewin's Change Management Model (Figure 4.15) to propose changes in Company A's ERM strategy, integrating the concepts of sensegiving[8] and boundary management. This approach is supported by the findings of Meidell and Kaarbøe (2017), who demonstrate how organisations can effectively establish an ERM unit by engaging multiple organisational perspectives.

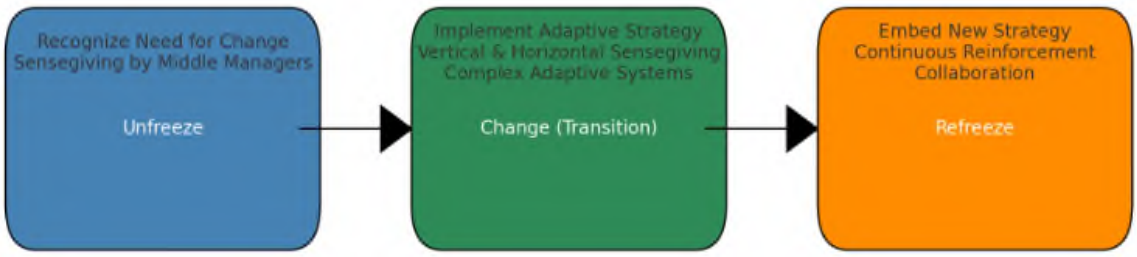


Figure 4.15: Lewin's Change Management Model

[8] Sensegiving involves influencing others' sensemaking and meaning construction toward a preferred organisational reality (Gioia & Chittipeddi, 1991). Unlike sensemaking, which focuses on how managers interpret and understand information for themselves, sensegiving involves middle managers influencing each other and higher levels within the organisation, considering power dynamics (Kraus & Stromsten, 2012).

1. Unfreeze: Preparing the Organisation for Change

Objective: Establish the need for change by recognising the limitations of current risk management practices and creating a sense of urgency.

In the "Unfreeze" stage, the parent company of Company A must first acknowledge that its existing approach to risk management—characterised by rigid, one-size-fits-all strategies—is inadequate for addressing the unique challenges faced by its subsidiaries. The project funding issue at Company A, which incurred significant costs, serves as a critical incident that underscores the need for a more flexible, adaptive organisational strategy.

- **Sensegiving and Issue Selling**:
  - Middle managers, acting as "issue sellers," must engage in sensegiving by framing the funding issue in a way that captures the attention of top management (Dutton et al., 2001).
  - They advocate for a shift towards a more adaptive strategy, emphasising the importance of aligning organisational practices with the specific needs and contexts of different subsidiaries (Meidell & Kaarbøe, 2017).

2. Change: Implementing the New Strategy

Objective: Transition from the old risk management practices to the new, more adaptive strategy.

During the "Change" phase, Company A begins to transition from its existing, rigid risk management approach to the newly advocated flexible strategy. This transition involves both vertical and horizontal sensegiving efforts.

- **Vertical Sensegiving:**
  - Middle managers continue to engage top management, ensuring that the new adaptive strategies are understood, accepted, and supported at the highest levels.
  - They secure the necessary resources and commitment from top management to implement the changes (Dutton & Ashford, 1993).
- **Horizontal Sensegiving and Complex Adaptive Systems (CAS):**

- Middle managers must also influence their peers across different departments—such as projects, finance, and marketing—to ensure the new strategies are integrated into the organisation's operational practices.
- This involves creating feedback loops within the CAS framework, where middle managers from different domains share knowledge, collaborate, and adapt their practices to the new strategy (Carlile, 2004).

3. Refreeze: Solidifying the Change

Objective: Embed the new adaptive strategy into the organisational culture and ensure it becomes the standard approach.

In the "Refreeze" stage, Company A should seek to stabilise the changes and ensure that the new adaptive risk management strategy becomes ingrained in the organisation's culture.

- **Continuous Reinforcement:**
  - Middle managers continue their sensegiving activities to ensure that the new practices are not only adopted but also adapted as necessary to address emerging challenges.
  - This involves formalising new processes, providing ongoing training, and establishing new norms that support the adaptive strategy (Carlile & Rebentisch, 2003).

Therefore, Company A, motivated from inside to improve its ERM programme, has the opportunity to use insights from both streams to improve its ERM framework. The first thread outlines how risk managers can persuade higher management to adopt a more holistic approach to ERM while taking into account the unique environmental context of each site. The second thread clarifies how middle managers may impact the organisation horizontally by informing decision-makers at the same organisational level about the interdependencies of risks across borders.

4.4 Discussion and Conclusion

To address the main research question- How can the integration of ERM and PRM be achieved to enhance decision making, create and protect values?

Organisations need to understand that risk management is a complex system, characterised by its non-random behaviour yet absent of a rigid pattern. Therefore, leadership and risk management functions must clearly communicate the benefits of implementing ERM with the employees. ERM should not be viewed as an additional burden but rather as a supportive framework as emphasised by the Institute of Internal Auditors (2020). The organisations must invest in educational initiatives through risk awareness sessions, risk training, and risk workshops to keep employees skilled to foster risk culture that is transparent, adaptive, open, and geared toward learning. Engaging employees in the risk strategy allows them to see the tangible benefits it brings to both them and the organisation. The "tone at the top" is essential in ensuring effective implementation. While PRM follows the guidelines set by ERM, it should maintain a level of autonomy. This independence allows PRM to collaborate effectively with ERM in a way that encourages learning, adaptation, and improvement, ultimately driving the organisation toward its objectives. Recognition of complexity as seen in both Companies B and C demonstrate a sophisticated understanding of their operational environments, which significantly influences their approach to GRC and ERM governance structure. This acknowledgment of both internal and external complexities enables them to develop more adaptive and responsive risk management strategies that integrate effectively with PRM. In contrast, Company A's more rigid, internally focused ERM implementation failed to account for external influences, leading to ineffective integration.

The impact of organisational values on risk management practices is evident in the differing approaches of Companies A, B, and C. Company A's values—sustainability, governance, and avid learning, which promote openness and engagement—contradict its rigid risk governance structure. This misalignment reflects Matisue’s (2013) critique of traditional portfolio governance, which assumes linear thinking and a predictable environment. PRM, intended to support project delivery, but in company A it does not align with the organisation’s values, highlighting issues with feedback loops and a lack of recognition of external complexities. As CAS theory indicates, this disconnect limits the organisation’s ability to adapt and respond effectively to emerging risks. In contrast, Companies B and C exhibit a strong congruence between their values and risk management governance and practice. For instance, Company C’s core values—Inspire, Engage, Create, and Deliver—play a pivotal role in cultivating a culture of collaboration and proactive risk management. This alignment enhances

communication and understanding between project teams and the ERM department, facilitating a greater integration of risk management processes and improving decision-making efficiency.

Chapter Five: Conclusions

5.1 Introduction

This chapter synthesises the key findings discussed in the findings and discussion chapter, highlighting several theoretical and practical implications that collectively contribute to an effective approach for integrating PRM into ERM. In line with this, I revisit the research aim and questions (5.2). I then summarise the findings to address the research questions and demonstrate how the aim of this thesis has been achieved based on empirical evidence from the study (5.3), primarily presented and discussed in the findings and discussion chapter. This is followed by the research's theoretical and practical contributions (5.4), concluding with limitations and suggestions for future research (5.5).

5.2 Revisiting Research aim and Questions.

The aim of this research was to explore strategies for strengthening the connection between ERM and PRM to improve integration, enhance decision-making, and promote both value creation and protection. To achieve this, I examined how each case study fostered a common understanding of risk perception across employees at different departmental and organisational levels, particularly within project settings. Additionally, I analysed the risk governance structures and assessed the risk culture maturity in each case study to understand how these factors influence self-organisation and the integration of PRM and ERM. Based on this, the main research question and three sub-questions were as follows:

How Can the Integration of ERM and PRM be achieved to enhance decision making, create and protect values?

The three sub-questions:

1- how do the organisations under study define risk?

2- how can governance, especially risk governance, influence the concept of self-organisation, a key element of CAS, in shaping the integration of PRM and ERM?

3- What role does risk culture play in the integration of PRM and ERM?

5.3 Synthesising Key Findings

5.3.1 Bridging the Gap Between PRM and ERM Perceptions

The findings suggest that, although risk was recognised as a complex and context-dependent concept that evolves with time and place, ISO 31000 played a crucial role in establishing a unified risk language between PRM and ERM. This shared understanding, particularly evident in Company C, allowed employees to align on risk definitions across both project-specific and enterprise-wide contexts. The adoption of ISO 31000 represents a form of normative isomorphism, serving as a key first step toward integrating PRM and ERM by providing a common language for risk communication and decision-making.

5.3.2 The Role of Corporate Governance in ERM/PRM Integration

The findings show that centralising both ERM and PRM functions, where PRM retains its own methodology while aligning with ERM's overarching guidelines, fosters both adaptive and institutionalised behaviours. In this arrangement, project managers appreciate ERM's value in communicating strategic project risks, particularly in international projects, while maintaining the flexibility to use their own tools and methodologies, achieving an optimal balance. This dynamic is evident in Company C, which operates as a self-organising system. In contrast, Company A's rigid, siloed structure fails to account for local conditions and the broader environment, leading to less effective integration of ERM and PRM. Furthermore, risk governance structures that acknowledge the complexity of their environment by linking project teams to internal and external dynamics and facilitating relationships with various stakeholders are more conducive to the successful integration of PRM and ERM.

5.3.3 The Role of Risk Culture in ERM/PRM Integration

The findings show that culture plays a pivotal role in the integration of PRM and ERM, as it shapes how these two systems interact and align. Key cultural attributes such as openness, compliance, learning, and adaptability are crucial for fostering a unified approach to risk management. Openness allows for transparent communication between project teams and ERM departments, facilitating the exchange of information about risks, particularly when they are complex or emerge unexpectedly. This transparency is essential for ensuring that all stakeholders are aware of potential threats and can take proactive measures to mitigate them. A culture of continuous learning encourages teams to adapt from past experiences, address new challenges, and refine their risk management strategies. This learning not only embeds

risk management into the organisation's decision-making processes but also supports rewarding appropriate risk behaviours while sanctioning inappropriate risk behaviours. Adaptability allows both ERM and PRM systems to be flexible in responding to emerging risks, ensuring that the organisation remains agile in the face of uncertainty. This cultural element is particularly important in complex environments where risks can change rapidly and unexpectedly. Adaptable systems are better equipped to reconfigure processes and strategies to deal with unforeseen challenges, rather than relying on rigid, predetermined methods.

5.3.4 Strategic Imperative and Organisational Drivers of ERM Adoption: Implications for PRM-ERM Integration Effectiveness

Understanding the operational environment played a pivotal role in shaping the risk governance structures of Companies B and C. Their values aligned with adaptive risk governance structures that acknowledged and responded to the complexities of their internal and external environments. Their risk cultures encouraged open communication and collaboration between departments, allowing for project-level risks (PRM) to be assessed not in isolation but as part of a broader ERM framework. This approach helped ensure that project risks were understood in the context of their potential impact on overall business objectives and strategic goals. Particularly, in Company C, this alignment led to continuous dialogue and co-evolution between project teams and the ERM team, facilitating more responsive and adaptive risk practices. By embracing complexity, these companies ensured that their governance structures could evolve with changing risks. In contrast, Company A's inward-facing goals and narrower risk focus created a disconnect between its values and its risk governance structure, which failed to fully account for external complexities.

5.4 Contribution to Knowledge

This thesis investigated various approaches that contribute to the integration of PRM into ERM within organisations. In doing so, it makes theoretical, methodological, and practical contributions to the process and practice of risk management integration, specifically between ERM and PRM. By applying CAS theory, the thesis offers insights that extend beyond traditional linear models, which often overlook the specific organisational context in which a risk management system operates. This approach provides a more dynamic and context-dependent framework for effective risk management integration.

5.4.1 Theoretical Implications

This study contributes to the academic literature on ERM, PRM, and CAS in five main ways. Each contribution addresses specific gaps in the literature, supported by empirical evidence from the study and positioned within relevant theoretical debates.

First, the study reconceptualises the integration of PRM and ERM as a self-organising and emergent process, rather than a formal, top-down alignment. While existing literature often treats ERM integration as a technical coordination problem solved through standards or frameworks (e.g., ISO 31000, COSO), this study demonstrates that integration also emerges through decentralised interactions, informal feedback loops, and cultural alignment. This contributes to an evolving view of integration as a complex, adaptive process rather than a purely structural task, extending the work of Mikes (2011), Arena et al. (2010), and Sheth and Sinfield (2024).

Second, the study challenges the prevailing assumption that structural complexity inherently hinders PRM/ERM coherence. Instead, it shows how some organisations, especially Company B have responded to such complexity with adaptive governance innovations, such as dual PRM directors and project portfolio oversight linked to GRC structures. These structures enable responsiveness to fast-paced project environments while maintaining ERM alignment, thereby advancing literature on structural and portfolio-level governance in complex project settings (Maylor et al., 2013; Geraldi et al., 2011).

Third, the research provides an empirical bridge between risk culture and PRM/ERM integration, a link that is often asserted but rarely demonstrated. By operationalising IRM's (2012) risk culture framework, the study identifies specific cultural attributes such as leadership commitment, empowerment, transparency, continuous learning, and adaptability that facilitate risk integration across organisational levels.

Fourth, the study contributes to CAS theory by focusing on interactions between organisational functions, specifically PRM and ERM as agents within a complex adaptive system. Most prior CAS-based risk research has concentrated on risk–risk. In contrast, this research advances the conversation by showing how distinct but interdependent functions adapt through mutual adjustments in governance, culture, and language, responding to Sheth

and Sinfield's (2024) recent call for CAS applications to focus more on function–function dynamics.

Finally, this research advances CAS literature by incorporating governance and culture as fundamental components of risk management frameworks. Traditional CAS models focus on the emergent behaviour and adaptive capacity of systems driven by interactions between agents. This study extends that view by emphasising that governance structures and risk culture shape these interactions, influencing how organisations can adapt to and manage evolving risks. Governance is seen as setting the rules and boundaries that enable or constrain agent behaviours, while risk culture reflects the shared attitudes and values toward risk within the organisation. By integrating these human and organisational factors into CAS-based risk models, this research offers a more comprehensive approach to understanding how complex systems, like ERM and PRM, co-evolve and respond to dynamic risks.

Together, these contributions provide new theoretical and empirical insights into how risk management functions evolve, co-adapt, and integrate within dynamic organisational environments. They also demonstrate how critical realist methodology and CAS theory can be used in tandem to uncover both the underlying structures and emergent patterns that shape risk governance across levels.

Table 5.1 summarise these theoretical contributions.

Table 5.1: Summary of Theoretical Contributions

#	Contribution	Gap in the Literature	Contribution	Relevant Literature
1	**Reframing PRM/ERM integration as a self-organising process**	Most literature treats PRM/ERM integration as a top-down, linear process (e.g. standards-based alignment). Little attention is given to how integration emerges dynamically within complex systems.	This study shows that PRM/ERM integration can be co-evolutionary, emerging through feedback loops, adaptive risk governance and culture. This shifts the view from structural alignment to processual emergence.	ISO 31000; Arena et al. (2010); Mikes (2011); Sheth & Sinfield (2024)
2	**Demonstrating how structural complexity enables—not obstructs—adaptive governance**	Structural complexity is often seen as a challenge to integration and risk management coherence, not a source of innovation.	This study shows that organisations facing high interdependence and diverse risk sources developed dual-director governance and portfolio-level PRM—adaptive responses that improve PRM–ERM coherence.	Maylor et al. (2013); Winch et al. (2022)
3	**Empirically linking risk culture to PRM–ERM integration under socio-political complexity**	Risk culture is often discussed abstractly, with little empirical evidence linking it to cross-level risk integration under conflicting agendas.	By applying the IRM (2012) criteria, this study shows that mature cultures of empowerment, leadership commitment, and shared values help mitigate fragmentation and support integration.	IRM (2012)
4	**Advancing CAS by focusing on function–function interactions (PRM–ERM)**	CAS literature has been criticised for focusing too narrowly on risk–risk interactions and not enough on how entire organisational functions interact adaptively.	This study addresses this gap by using CAS to examine how PRM and ERM as functions co-adapt through information sharing, governance links, and risk culture, responding directly to recent CAS criticisms.	Sheth & Sinfield (2024)
5	**Extending CAS by embedding governance and culture as systemic enablers**	Traditional CAS applications often omit formal structures (like governance) and values (like culture), focusing mainly on emergent behaviours from agent interactions.	This research conceptualises governance as boundary-setting and culture as a collective attractor within CAS, offering a richer framework for understanding organisational adaptation.	Lewin (1999); Alaa & Fitzgerald (2013); Nan (2011); Sweetman et al., (2014)

5.4.2 Practical Implications

The findings from this research offer valuable lessons for risk professionals, managers, and decision-makers aiming to better integrate ERM and PRM within complex organisational settings.

1. Foster an ERM-Minded Culture for Long-term Success:

Company C, through its long history of developing ERM, serves as an example of how organisations can benefit from a strong, cohesive risk culture. A key takeaway is that embedding ERM within the organisational structural requires time and sustained commitment. Companies that want to achieve effective PRM-ERM integration should focus on cultivating an ERM-oriented culture, aligning risk management with core organisational values, and fostering consistent buy-in from both leadership and staff. As seen in Company C, path dependency played a role in this journey in which the long-standing commitment to risk management strategies helped shape resilient and adaptive system. Managers then must recognise the value of this gradual process and invest in cultivating a culture that views risk management as integral to organisational strategy.

2. Cultural /Governance Alignment for Integration:

For effective PRM-ERM integration, companies need to focus on building a strong risk culture that fosters collaboration across different levels. Insights from Company B highlight the importance of helping project teams understand their roles in the broader organisational risk structure. This points to the need for ongoing risk training, open communication, and a culture where risk management is not siloed but treated as an organisation-wide priority. Firms should align their risk culture with strategic objectives, enabling them to adapt to evolving risks and external complexities.

3. Use Sensegiving to Influence Leadership and Decision-Making:

For companies that are still in the early stages of ERM development such as Company A, middle managers and risk professionals can play a critical role in shaping how ERM is perceived and resourced. A practical strategy is to engage in "sensegiving," where risk professionals act as issue-sellers to leadership, framing ERM as an essential part of the organisation’s strategic direction. This approach allows risk managers to influence decision-making by presenting ERM as not just a compliance function but as a value-adding process that contributes to

organisational resilience. This method empowers professionals to advocate for more robust ERM frameworks, helping secure the necessary support from executives.

4. Leveraging Governance Intersections to Enhance Integration:

The governance intersect as described by Winch's diagram (owners, projects, suppliers), is critical to understanding the strategic implications for integrating PRM and ERM. As seen in Company B and to a greater extent in Company C, governance structures that address both strategic and operational risks can drive integration and coherence. Company C's mature governance structures allow it to coordinate effectively across various stakeholders, owners, and projects, ensuring that both strategic ERM objectives and operational project risks are managed in tandem. This model serves as a guide for organisations looking to design governance frameworks that enhance PRM-ERM integration.

Drawing on these practical implications, Figure 5.1 serves as a diagnostic tool to guide project managers, risk managers, and decision-makers in evaluating and improving PRM–ERM integration.

Company	Risk Culture	Governance Structure	Complexity Awareness	Integration Readiness	Actionable Recommendations
Company A	Closed, Misaligned with espoused values	Rigid, top-down, inflexible contracts	Low – Lacks external system recognition	❌ *Low* – Siloed, poor integration, weak feedback loops	🔷 Project managers should act as issue sellers both vertically (to ERM and senior managers) and horizontally (across different department and functions), especially where "one-size-fits-all" approaches limit adaptability. 🔷 ERM directors must recognise ERM as a nested system and involve the parent company as a key stakeholder to appropriately resource ERM processes.
Company B	Mostly open, with gaps in culture absorption	Adaptive, with dual PRM-GRC governance	Moderate – Aware of internal complexities, learning externally	⚠️ *Emerging* – On the path toward integration	🔷 GRC and ERM managers should intensify risk awareness sessions and workshops, promoting bottom-up learning and understanding of risk culture. 🔷 Project managers must actively engage and give feedback, allowing the culture to emerge over time through practice and interaction.
Company C	Open, collaborative, values-driven	Adaptive, responsive, project-empowered	High – Strong internal/external systems awareness	✅ *Optimal* – Fully integrated, self-organising, learning-oriented	🔷 ERM directors must maintain resourcing and education strategy of risk management to preserve the effectiveness of the current system. 🔷 Project managers should continue as self-organising agents, engaging in ongoing feedback loops and adapting project delivery within ERM frameworks.

Figure 5.1: PRM/ERM Integration Diagnostic Matrix

5.5 Limitations and Future Research

Every thesis inevitably encounters limitations, and this study is no exception. First, during the data collection stage, none of the three participating companies permitted participant or non-participant observations. This constraint stemmed from a combination of organisational confidentiality policies and ethical considerations approved by Newcastle University (see Section 3.7). As a result, I was unable to observe first-hand the culture that governs each company's risk practices, particularly the informal interactions, behaviours, and expressions of transparency during risk workshops and everyday decision-making.

This limitation inevitably shaped the research design, directing the study toward interviews and documentary analysis as the two core data sources. While interviews provided valuable insights into perceptions, values, and formal structures, the inclusion of internal documents such as risk governance frameworks, risk registers, assurance reports, and ERM guidance allowed for a more grounded understanding of how risk practices are institutionalised within each company. In this sense, documentary analysis played a crucial role in compensating for the absence of direct observation, particularly in tracing how risk-related norms and expectations are formally communicated and reinforced.

Nevertheless, the inability to observe everyday practices limited the ability to assess how risk culture is enacted in real organisational environment. Future research should incorporate participant or non-participant observation where access permits, to deepen the understanding of cultural norms, values, and behaviours as they unfold in practice. This would enable triangulation between interviews, documents, and observed behaviour, offering a more robust account of how risk is interpreted and enacted on the ground.

Second, although having three different organisations in size, field of operation, and structures offer wider approaches that can be applied to PRM/ERM integration, the comparison between these cases presents limitations. Specifically, Company C, a large corporation with substantial capital and extensive resources differs significantly from Company A, a smaller subsidiary with limited resources, and Company B, which, despite high financial resources, has fewer employees.

From this perspective, future research could explore the impact of organisational scale and resource availability on integrating PRM/ERM in greater depth. It is suggested that a more balanced comparison between the organisations' structures such as a comparison between a subsidiary to a subsidiary or project - passed to project-based companies. This would help control for variables such as organisational scale, governance maturity, and sectoral influence, leading to clearer causal inferences about the conditions that facilitate or hinder PRM/ERM integration.

Third, while the sample size was appropriate for a qualitative, case-based study, it remains limited in scope. This was further compounded by the fact that several participants declined to answer the question on risk perception, explaining that it was too obvious or simplistic to warrant discussion. Although this response was not expected, it was treated analytically as a reflection of how risk perception may be normalised and unexamined within some organisational contexts. To address this limitation, data triangulation with documentary sources and follow-up questions during interviews were employed to deepen understanding of implicit risk beliefs and frameworks. Nonetheless, this constraint reduced the richness of data in one key area of inquiry. Future research should aim for larger, more diverse samples and consider alternative ways of eliciting perceptions—perhaps through indirect or scenario-based questioning—to access deeper insights and mitigate participant disengagement.

5.6 Conclusion

In conclusion, this thesis has explored the integration of PRM into ERM, contributing valuable insights into both theory and practice. By examining how organisations address risk management across various levels and contexts, the research highlights the importance of aligning risk governance structures and cultivating a strong risk culture. The findings demonstrate that a balance between standardised ERM frameworks and the autonomy of PRM is essential for effective integration, particularly in dynamic and complex environments.

The use of CAS theory has allowed this study to go beyond traditional linear approaches, providing a more comprehensive understanding of the interdependencies and feedback loops that drive risk management practices. Through the lens of CAS, the research emphasises the need for continuous adaptation and context-awareness, reinforcing that risk management is

not a one-size-fits-all approach but rather an evolving process that requires flexibility, responsiveness, and leadership support.

Ultimately, this thesis provides both theoretical and practical contributions to the field of risk management, offering a nuanced understanding of how PRM and ERM can be integrated within organisations. It underscores the importance of governance, culture, and adaptive behaviors in ensuring the successful alignment of risk management systems. While the study has identified several key factors for integration, it also opens avenues for further research, particularly in exploring how organisations can continuously adapt their risk management practices to meet emerging challenges and complexities.

References

Agarwal, R. & Virine, L. (2019) 'Integration Stages of Project Risk Management (PRM) into Enterprise Risk Management (ERM)', *International Journal of Risk and Contingency Management (IJRCM)*, 8(1), pp. 13–33.

Albasteki, O.N.M.S. (2021) *Corporate stakeholders, environmental and social risks, and enterprise risk management: towards an integrating framework*. Thesis. [Online]. Brunel University London.

Ali, H.M. (2019) 'Saudi Arabia regulations on corporate governance', *International Journal of Asian Social Science*, 9(2), pp. 229–239.

Allen, P.M. (2012) *Cities and regions as self-organizing systems: models of complexity*. Routledge.

Al-Tayan, R. (2022) *Empirical analysis of Enterprise Risk Management in Middle East countries*. thesis thesis. [Online]. Loughborough University.

Andringa, L., Ökmen, Ö., Leijten, M., Bosch-Rekveldt, M. & Bakker, H. (2022) 'Incorporating Project Complexities in Risk Assessment: Case of an Airport Expansion Construction Project', *Journal of Management in Engineering*, 38(6), p. 05022015.

Andronache, A., Matin, M. & Althonayan, A. (2018) *Exploring the Ineffectiveness of Enterprise Risk Management and GRC's Role in the Maturity of Organisations' Risk Management*.

Annex, S. (2019) *ISO - Management system standards*. [Online] [online]. Available from: https://www.iso.org/management-system-standards.html (Accessed 9 July 2024).

Assibi, A.T. (2022) 'The Role of Enterprise Risk Management in Business Continuity and Resiliency in the Post-COVID-19 Period', *Open Access Library Journal*, 9(6), pp. 1–19.

Aven, T. & Renn, O. (2010) *Risk management and governance: concepts, guidelines and applications*. Vol. 16. Springer Science & Business Media.

Beck, U. & Holzer, B. (2007) 'Organizations in', *International handbook of organizational crisis management*, p. 1.

Boulton, J. (2012) 'Strategy for a Complex World', in Julie Verity (ed.) *The New Strategic Landscape: Innovative Perspectives on Strategy*. Cass Business Press. [Online]. London: Palgrave Macmillan UK. pp. 13–30.

Bowen, G.A. (2009) 'Document Analysis as a Qualitative Research Method', *Qualitative Research Journal*, 9(2), pp. 27–40.

Brinkmann, S. & Kvale, S. (2018) *Doing Interviews*. SAGE Publications Ltd.

Brooks, J. & King, N. (2016) 'Template analysis for business and management students', *Template Analysis for Business and Management Students*, pp. 1–120.

Byrne, D. & Callaghan, G. (2013) *Complexity Theory and the Social Sciences: The state of the art*. London: Routledge.

Chairani, C. and Siregar, S.V., (2021) The effect of enterprise risk management on financial performance and firm value: the role of environmental, social and governance performance*. Meditari Accountancy Research*, 29(3), pp.647–670.

Carlile, P.R. & Rebentisch, E.S. (2003) 'Into the Black Box: The Knowledge Transformation Cycle', *Management Science*, 49(9), pp. 1180–1195.

Carlsson-Wall, M., Kraus, K., Meidell, A. & Tran, P. (2019) 'Managing risk in the public sector–The interaction between vernacular and formal risk management systems', *Financial Accountability & Management*, 35(1), pp. 3–19.

Cilliers, P. (1998) *Complexity and Postmodernism: Understanding Complex Systems*. London: Routledge.

Clements, F. (2022) *An investigation into the experiences of adults with intellectual disabilities of online risks : online contract, conduct, content and contact, including online negative comments and/or messages*. Ph.D. thesis. [Online]. University of Wolverhampton.

Connelly, J. (2001) 'Critical realism and health promotion: effective practice needs an effective theory', *Health Education Research*, 16(2), pp. 115–120.

Corporate Governance institute (2022) *What is corporate governance?* [Online] [online]. Available from: https://www.cgi.org.uk/about-us/policy/what-is-corporate-governance.

Coso, I.I. (2004) 'Enterprise risk management-integrated framework', *Committee of Sponsoring Organizations of the Treadway Commission*, 2.

Cox, J.C., Webster, R.L. & Hammond, K.L. (2009) 'Market Orientation within University Schools of Business: Can a Dynamical Systems Viewpoint Applied to a Non-Temporal Data Set Yield Valuable Insights for University Managers?', *American Journal of Business Education*, 2(7), pp. 73–82.

Capital Market Authority (CMA) (2006) Corporate Governance Regulations in the Kingdom of Saudi Arabia. Riyadh: Capital Market Authority. Available at: https://cma.org.sa (Accessed: [2024]).

Dutton, J.E. & Ashford, S.J. (1993) 'Selling Issues to Top Management', The Academy of Management Review, 18(3), p. 397.

Davenport, T.H., De Long, D.W. & Beers, M.C. (1998) 'Successful knowledge management projects', MIT Sloan management review, 39(2), p. 43.

Dhal, M. (2020) 'Labor Stand: Face of Precarious Migrant Construction Workers in India', Journal of Construction Engineering and Management, 146(6), p. 04020048.

Denzin, N.K. (2017) The Research Act: A Theoretical Introduction to Sociological Methods. New York: Routledge.

Earle, T.C. (2010) 'Trust in Risk Management: A Model-Based Review of Empirical Research', *Risk Analysis*, 30(4), pp. 541–574.

Easton, G. (2010a) 'Critical realism in case study research', *Industrial Marketing Management*, 39(1), pp. 118–128.

Easton, G. (2010b) 'Critical realism in case study research', *Industrial Marketing Management*, 39(1), pp. 118–128.

Eisenhardt, K.M. (1989) 'Building theories from case study research', *Academy of management review*, 14(4), pp. 532–550.

Elshaer, A.M., Marzouk, A.M. & Khalifa, G.S.A. (2023) 'Antecedents of Employees' Perception and Attitude to Risks: The Experience of Egyptian Tourism and Hospitality Industry', *Journal of Quality Assurance in Hospitality & Tourism*, 24(3), pp. 330–358.

Emblemsvåg, J. (2020) 'Risk and complexity – on complex risk management', *The Journal of Risk Finance*, 21(1), pp. 37–54.

Florio, C. & Leoni, G. (2017) 'Enterprise risk management and firm performance: The Italian case', *The British Accounting Review*, 49(1), pp. 56–74.

Flyvbjerg, B. (2006) 'Five Misunderstandings About Case-Study Research', *Qualitative Inquiry*, 12(2), pp. 219–245.

Fraser, J.R.S., Quail, R. & Simkins, B.J. (2022a) 'Questions asked about enterprise risk management by risk practitioners', *Business Horizons*, 65(3), pp. 251–260.

Fraser, J.R.S., Quail, R. & Simkins, B.J. (2022b) 'Questions asked about enterprise risk management by risk practitioners', *Business Horizons*, 65(3), pp. 251–260.

Fraser, J.R.S. & Simkins, B.J. (2016) 'The challenges of and solutions for implementing enterprise risk management', *Business Horizons*, 59(6), pp. 689–698.

FRC (2024) *UK Corporate Governance Code*. [Online] [online]. Available from: https://www.frc.org.uk/library/standards-codes-policy/corporate-governance/uk-corporate-governance-code/ (Accessed 24 November 2024).

Freeburg, D. (2020) 'Leadership and innovation within a complex adaptive system: Public libraries', *Journal of Librarianship and Information Science*, 52(2), pp. 451–463.

Freeman, R.E., (1984) Strategic management*: A stakeholder approach.* Boston: Pitman.

Gephart Jr, R.P., Van Maanen, J. & Oberlechner, T. (2009) 'Organizations and risk in late modernity', *Organization studies*, 30(2–3), pp. 141–155.

Gioia, D.A., Corley, K.G. & Hamilton, A.L. (2013) 'Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology', *Organizational Research Methods*, 16(1), pp. 15–31.

Gioia, D.A. & Chittipeddi, K. (1991) 'Sensemaking and sensegiving in strategic change initiation', *Strategic Management Journal*, 12(6), pp. 433–448.

Guba, E.G. (1981) 'Criteria for assessing the trustworthiness of naturalistic inquiries', *ECTJ*, 29(2), pp. 75–91.

Guba, E.G. & Lincoln, Y.S. (1982) 'Epistemological and Methodological Bases of Naturalistic Inquiry', *Educational Communication and Technology*, 30(4), pp. 233–252.

Hampton, J. (2009) *Fundamentals of enterprise risk management: How top companies assess risk, manage exposure, and seize opportunity*. Amacom.

He, Q., Dong, S., Rose, T., Li, H., Yin, Q. & Cao, D. (2016) 'Systematic impact of institutional pressures on safety climate in the construction industry', *Accident Analysis & Prevention*, 93pp. 230–239.

Hunziker, S. (2021) *Enterprise Risk Management: Modern Approaches to Balancing Risk and Reward*. Wiesbaden: Springer Fachmedien Wiesbaden.

Institute of Internal Auditors (2020) *Three Lines Model – an update of the Three Lines of Defence IIA*. [Online] [online]. Available from: https://www.theiia.org/globalassets/site/about-us/advocacy/three-lines-model-updated.pdf.

IRM (2022) */IRM/irm-report-iso-31000-2018-v2.* [Online] [online]. Available from: https://uk.search.yahoo.com/search?fr=mcafee&type=E211GB105G0&p=%2FIRM%2Firm-report-iso-31000-2018-v2. (Accessed 9 July 2024).

ISO (2018) *International Organization for Standardization*. [Online] [online]. Available from: https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100426.pdf.

Jean-Jules, J. & Vicente, R. (2021) 'Rethinking the implementation of enterprise risk management (ERM) as a socio-technical challenge', *Journal of Risk Research*, 24(2), pp. 247–266.

Jepson, J., Kirytopoulos, K. & Chileshe, N. (2022) 'Isomorphism within risk-management practices of the Australian construction industry', *International Journal of Construction Management*, 22(8), pp. 1508–1524.

Jiang, H., Jia, J. & Chapple, L. (2023) 'Enterprise risk management and investment efficiency: Australian evidence from risk management committees', *Australian Journal of Management*, p. 03128962221144513.

Kerstin, D., Simone, O., Nicole, Z. & Lehner, O.M. (2014) 'Challenges in implementing enterprise risk management', *ACRN Journal of Finance and Risk Perspectives*, 3(3), pp. 1–14.

Kraus, K. & Strömsten, T. (2012) 'Going public: The role of accounting and shareholder value in making sense of an IPO', *Management Accounting Research*, 23(3), pp. 186–201.

Khan, M.J., Hussain, D. & Mehmood, W. (2016) 'Why do firms adopt enterprise risk management (ERM)? Empirical evidence from France', *Management Decision*, 54(8), pp. 1886–1907.

King, N., Brooks, J. & Tabari, S. (2018) 'Template Analysis in Business and Management Research', in *Qualitative Methodologies in Organization Studies*. [Online].

Kommunuri, J., Narayan, A., Wheaton, M., Jandug, L. & Gonuguntla, S. (2020) 'Firm performance and value effects of enterprise risk management', *New Zealand Journal of Applied Business Research*, 14(2), pp. 17–28.

Lalonde, C. (2020) 'Enterprise Risk Management & Treasury Board Secretariat: A Policy Evaluation', *Major Papers*,

Lalonde, C.R. (2020) *Enterprise Risk Management & Treasury Board Secretariat: A Policy Evaluation*,

Lapsley, I. (2009) 'New public management: The cruellest invention of the human spirit? 1', *Abacus*, 45(1), pp. 1–21.

Liang, H., Saraf, N., Hu, Q. & Xue, Y. (2007) 'Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management', *MIS Quarterly*, 31(1), pp. 59–87.

Liebenberg, A.P. & 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.

Mabelo, P.B. (2023) *Risk Management and Project Context1*,

Mahsoon, T. (2023) *Shariah corporate governance and risk management in Saudi Arabian banks*,

Makmor, A., Razak, N.S.A., Kamaluding, M. & Alshurideh, M. (2023) 'The Influence of Enterprise Risk Management Framework Towards Company Performance at Conglomerate Group of Companies', in Muhammad Alshurideh, Barween Hikmat Al Kurdi, Ra'ed Masa'deh, Haitham M. Alzoubi, & Said Salloum (eds.) *The Effect of Information Technology on Business and Marketing Intelligence Systems*. [Online]. Cham: Springer International Publishing. pp. 1213–1235.

Meidell, A. & Kaarbøe, K. (2017) 'How the enterprise risk management function influences decision-making in the organization – A field study of a large, global oil and gas company', *The British Accounting Review*, 49(1), pp. 39–55.

Malik, M.F., Zaman, M. & Buckby, S. (2020) 'Enterprise risk management and firm performance: Role of the risk committee', *Journal of Contemporary Accounting & Economics*, 16(1), p. 100178.

Martinsuo, M. (2013) 'Project portfolio management in practice and in context', *International Journal of Project Management*, 31(6), pp. 794–803.

Mason, J. (1996) *Qualitative researching*. London ; Thousand Oaks, Calif. : Sage.

Maylor, H., Meredith, J., Söderlund, J. & Browning, T. (2018) 'Old theories, new contexts: extending operations management theories to projects', *International Journal of Operations & Production Management*, 38pp. 1274–1288.

Maylor, H.R., Turner, N.W. & Murray-Webster, R. (2013) 'How hard can it be?: Actively managing complexity in technology projects', *Research-Technology Management*, 56(4), pp. 45–51.

Meadows, D. & Wright, D. (2008) *Thinking in Systems: International Bestseller*. White River Junction, Vermont, UNITED STATES: Chelsea Green Publishing.

Miller, K.D. (2009) 'Organizational risk after modernism', *Organization Studies*, 30(2–3), pp. 157–180.

Mitchell, V.L. (2006) 'Knowledge Integration and Information Technology Project Performance', *MIS Quarterly*, 30(4), pp. 919–939.

Miterev, M., Engwall, M. & Jerbrant, A. (2017) 'Mechanisms of Isomorphism in Project-Based Organizations', *Project Management Journal*, 48(5), pp. 9–24.

Nisula, J.M. (2018) *A risk management framework for a complex adaptive transport system*. Ph.D. thesis. [Online]. Université Paul Sabatier - Toulouse III,.

Norberg, J., Wilson, J., Walker, B. & Ostrom, E. (2008) 'Diversity and resilience of social-ecological systems', *Complexity theory for a sustainable future*, pp. 46–80.

ONS (2023) *Office for National Statistics*. [Online] [online]. Available from: https://www.gov.uk/government/organisations/office-for-national-statistics (Accessed 4 May 2024).

Paape, L. & Speklé, R.F. (2012) 'The Adoption and Design of Enterprise Risk Management Practices: An Empirical Study', *European Accounting Review*, pp. 1–32.

Paley, J. (1998) 'Misinterpretive phenomenology: Heidegger, ontology and nursing research', *Journal of advanced nursing*, 27(4), pp. 817–824.

Project Management Institute (ed.) (2017) *A guide to the project management body of knowledge / Project Management Institute*. PMBOK guide. Sixth edition. Newtown Square, PA: Project Management Institute.

Qazi, A. & Simsekler, M.C.E. (2021) 'Quality assessment of enterprise risk management programs', *Journal of Risk Research*, 0(0), pp. 1–21.

Racz, N., Weippl, E. & Seufert, A. (2010) 'A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC)', in Bart De Decker & Ingrid Schaumüller-Bichl (eds.) *Communications and Multimedia Security*. Lecture Notes in Computer Science. [Online]. Berlin, Heidelberg: Springer Berlin Heidelberg. pp. 106–117.

Rammel, C., Stagl, S. & Wilfing, H. (2007) 'Managing complex adaptive systems — A co-evolutionary perspective on natural resource management', *Ecological Economics*, 63(1), pp. 9–21.

Reid, L.A. (1959) 'Review of Personal Knowledge: Towards a Post-Critical Philosophy', *British Journal of Educational Studies*, 8(1), pp. 66–71.

Sayer, A. (1997) 'Critical realism and the limits to critical social science', *Journal for the theory of social behaviour*, 27(4), pp. 473–488.

Shaikh, I. and Randhawa, K., 2022. *Managing the risks and motivations of technology managers in open innovation: Bringing stakeholder-centric corporate governance into focus. Technovation,* 114, p.102437.

Schuett, J. (2023) 'Three lines of defense against risks from AI', *AI & SOCIETY*,

Sheth, A. & Sinfield, J.V. (2024) 'Advancing the complex adaptive systems approach to enterprise risk management with quantified risk networks (QRNs)', *Scientific Reports*, 14(1), p. 22312.

Siegrist, M. (2021) 'Trust and Risk Perception: A Critical Review of the Literature', *Risk Analysis*, 41(3), pp. 480–490.

Spira, L.F. & Page, M. (2003) 'Risk management: The reinvention of internal control and the changing role of internal audit', *Accounting, Auditing & Accountability Journal*,

Sweetman, R., O'Dwyer, O. & Conboy, K. (2014) 'A Complex Adaptive Systems Perspective on Self-Organization in IS Project Portfolios', in *9th Pre-ICIS International Research Workshop on Information Technology Project Management (IRWITPM 2014)*. [Online]. 2014 p. 28.

Vincent, S. & O'Mahoney, J. (2018) 'Critical realism and qualitative research: An introductory overview', *The Sage handbook of qualitative business and management research methods: History and traditions*, pp. 201–216.

Winch, G.M. (2014) 'Three domains of project organising', *International Journal of Project Management*, 32(5), pp. 721–731.

Winch, G.M., Maytorena-Sanchez, E. & Sergeeva, N. (2022) *Strategic project organizing*. Oxford University Press.

Woods, M. (2009) 'A contingency theory perspective on the risk management control system within Birmingham City Council', *Management Accounting Research*, 20(1), pp. 69–81.

Wynn Jr, D. & Williams, C.K. (2012) 'Principles for conducting critical realist case study research in information systems', *MIS quarterly*, pp. 787–810.

Yin, R.K., 2009. *Case study research: Design and methods* (Vol. 5). sage.

Appendixes

A. Demographic Samples

A.1 Company A's Sample

Participant number	Occupation	Gender	Years of experience in the current position
A1	Previous ERM Director	Male	2
A2	A Project Lead	Male	8
A3	A Chemical Engineer from Health and Safety Department	Female	2
A4	A member of the `International Supply and Trading Department	Male	3
A5	A Project Manager	Male	1
A6	A Project Lead	Male	11
A7	Head of IT	Male	5
A8	Head of Legal	Male	5
A9	Current ERM Director	Female	1

A.2 Company B's Sample

Participant number	Occupation	Gender	Years of experience in the current position
B1	Senior Manager at GRC	Female	2
B2	Executive Risk Director	Male	4
B3	Senior Manager at GRC	Female	3
B4	Resilience Director	Female	3
B5	A Risk Champion for Change Management	Male	2
B6	A Risk Champion for Marketing Department	Male	1
B7	Divcar	Male	1.5
B8	PRM Director at the Delivery level	Male	3
B9	A Member of the Resilience Team	Male	2
B10	A Project Risk Director at GRC Level	Male	2
B11	A project Manager	Male	4
B12	A project Manager	Male	4

A.3 Company C's Sample

Participant number	Occupation	Gender	Years of experience in the current position
C1	Previous ERM Director	Male	4
C2	Current ERM Director	Male	1
C3	General Manager for Risk Management	Male	5
C4	Senior Manager at ERM	Male	5
C5	A Project Manager	Male	6
C6	A Project Manager	Male	9
C7	A Project Manager	Male	8
C8	ERM Specialist in PRM	Male	10
C9	A Member of the Compliance Team	Male	8
C10	Engineer in the Manufactory	Male	
C11	A Project Manager	Male	10
C12	Senior Manager at ERM	Male	8
C13	A Project Manager	Male	12

B. Interview Protocols

Research title: Risk management

Date _____

Time _____

Location _____

Organisation _____

Interviewer ____Naif Aldwais_____

Interviewee _____

Release form signed? ____

Notes to interviewee:

Thank you for your participation. I believe your input would be of value to this research that is to understand why there is a mismatch between PRM and ERM and how to integrate the two systems. Just to facilitate my note-taking, and after your permission I would like to audio tape our interviews today. The confidentiality agreement forms were signed off with each case study. For your information, only researchers on this project will have access to the tapes which will be eventually destroyed after they are transcribed. Each interview should take between thirty minutes to an hour. Once the interview ends, all participants will be thanked for taking part, researcher information will be exchanged if the participants wish to be informed of the study's outcomes, or should they wish to withdraw their information. All transcribed and translated interviews will be analysed using Template Analysis (King et al., 2018).

Interview Background

This research starts with generic demographic background questions including name, gender, previous career, current position, qualifications, and years of experience.

What is your name?_____

What is your current position?_____

How long have you been in your present position?_____

General risk management questions.

What do you understand by the concept of risk and risk management?

What are the tools adopted by the company to manage risk and uncertainty?

What challenges do managers face in managing risks and uncertainty through their existing methods?

C. Interviews questions

Typology of Research Questions, Adapted from Alvesson and Sandberg (2013) p.15

Question Type	*Generates knowledge about*	*Example Questions*
Descriptive (First Order)	The characteristics of a particular phenomenon including what it is, what it does and why it has the qualities that it does.	What is risk and risk management according to the organisations' understudy? Why implementing Enterprise Risk Management, ERM? How are ERM and PRM adopted in the organisations' understudy? To what extent is ERM role appreciated by project managers and project teams? What are the ERM and PRM standards adopted by these organisations?
Comparative (Second Order)	Relations among phenomena including, concomitance, equivalence and difference.	To what extent do employees in the different departments have common perceptions of risk and risk management? What are the similarities and differences between ERM and PRM adaptions in the literature and the organisations' understudy? Compared to the international standards and methodologies, how similar or different are the ERM and PRM standards used in these organisations?
Explanatory (Third Order)	Contingent relations between phenomena and their attributes. This includes correlation, conditionality and causality.	Has the adoption of specific standards or methodologies resulted in better or worse ERM/PRM integration? How can knowledge sharing activities result in ERM/PRM success? How can risk workshops contribute to a common risk language and risk value recognition?
Normative (Fourth Order)	How something should be done.	How can complexity theories (CAS) assist traditional processes in integrating a micro-level system[9] (PRM) into macro-level organisational systems (ERM)? How can the concept of self-organising systems improve effective governance structures impacting on the interaction of PRM and ERM?

[9] The scope of a micro and a macro level in this study is limited to organisational level, where leadership in a macro level focuses on the executive roles such as ERM that leads to organisational success. From the other side, leadership in a micro level concentrates on the achievement of a specific job or task such as PRM.

D. Definitions of the Initial Themes

Theme	Description
Communication	Demonstrates how risk is communicated among the different functions (special between ERM and PRM) throughout the entire company, plus the issues surrounding the existing communication systems, and suggestions for improving the communication system
Bridging the Gap Between ERM and PRM Perceptions	Illustrates how various participants perceive risk, as well as how other departments view ERM and vice versa
Governance structure	Considers the risk flow information and reporting channels, as well as how the organisational structure influences risk communication. Moreover, it looks at ERM's scope
ERM Drivers	Refers to the factors that led the company (A) decide to establish ERM which are internal factors including integration, reporting, and overcoming inconsistency
Risk Culture	Guided by IRM's successful risk criteria including but not limiting to transparency, risk awareness, and the way participants from different departments understand ERM
Challenges	The obstacles the companies face with risk management especially when implementing ERM, include the use of different risk languages and the high rate of staff turnover
Risk standards	Discusses the impact of the previous standard on risk management and whether the organisation now uses a standard such as COSO, ISO, or PMI.

E. The final template

1. Bridging the Gap Between ERM and PRM Perceptions

1.1. Distinguishing Internal Audit from Risk Management.

1.2. Context-Dependent Definition of Risk.

1.2.1. The Role of Standards in Unifying Risk Language.

1.3. A Siloed Risk Perspective.

2. The Role of Corporate Governance in ERM/PRM Integration.

2.1. A Siloed Risk Governance Structure Hindering PRM/ERM Integration.

2.1.1. Failure of ERM as a Management System.

F. Confidentiality Agreement with the University

Newcastle University

Confidentiality Agreement (Annex A)

Name of Student	Naif Aldwais		
Student Number	B4065 1874	**Programme:**	PhD.NUBS
School/Institute			
Name of Supervisor/s *(Please list all known)*	Karen Elliott		
Topic of Research:	Risk management		

During the course of your research project at the University, it is possible that you may contribute to the generation of intellectual property (in the form of, for example, patentable ideas, design rights, copyright, including copyright in computer code, know-how etc.) or receive information in confidence. The agreement below is to be signed where you need to keep such information confidential as set down in the University's *Policy Statement on Confidentiality and Intellectual Property (including Inventions) and Results for Research Students: Policy on Ownership and Use* which may be found on the University's web page: https://www.ncl.ac.uk/media/wwwnclacuk/research/files/Confidentiality%20and%20IP.pdf.

Does the Research Project require the Research Student to sign the Confidentiality Agreement below?

(Please note that the Faculty of Medical Sciences requires all research students to sign the Confidentiality Agreement.)

Yes ☑ No ☐ Signature of Supervisor KElliott

(If yes, the student read the text below and then sign where indicated below.)

Accordingly, I hereby agree to:

Keep secret any information which is given to me, and which is identified (either verbally, or by appropriate mark), as confidential to either the University, or to a research sponsor. (Should an external research sponsor ask me to personally sign a confidentiality agreement I shall first present the document for scrutiny by my Supervisor, or other officer of the University. If in doubt, I shall contact the University's Research and Enterprise Services, Intellectual Property and Legal Services Team).

Seek comment from my Supervisor prior to making any publication relating to my Student Project and accept the decision of my Supervisor should I be requested to remove any of the content which may either breach an obligation of confidentiality to a third party or compromise the ability of the University to subsequently seek patent protection.

In the event of a disagreement between my Supervisor and myself over confidentiality as applies to a proposed publication, I agree to refer the matter to the Post Graduate Dean of my Faculty for resolution.

Student Signature	Naif	Date	08/11/2021

Revised Learning Agreement – May 2018 PGR Sub-committee of UTLSEC

G. Confidentiality Agreement with the Organisation

N... DISCLOSURE AGREEMENT

(INDIVIDUAL)

STRICTLY PRIVATE & CONFIDENTIAL

To: ***Naif Aldwais***

[redacted]

Date: *[13] [04] [2022]*

Dear Sir,

You, ***[Naif Aldwais]*** holding [***national identification card number*** [redacted] in the [redacted] (the **Project**). This Undertaking sets out the terms on which we, [redacted] **Company (The Employer)**, agree to supply you with certain Confidential Information in connection with the Project.

In this undertaking (the **Undertaking**):

an **Affiliate** of Employer means any person Controlled by [redacted] and;

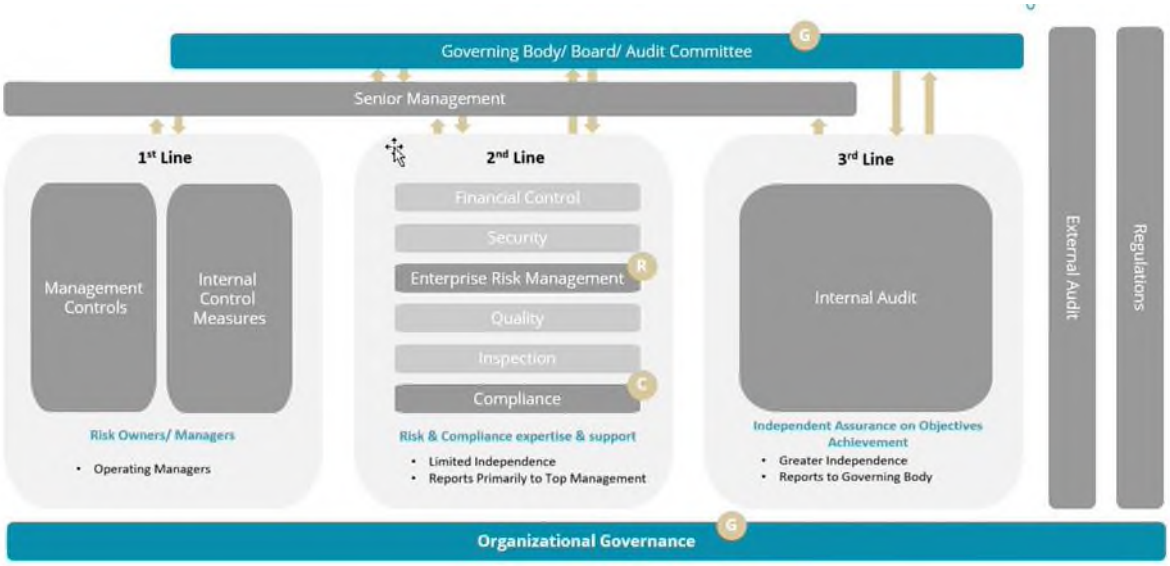
Controlling (including the terms **Controlling**, **Controlled by** and **under Common Control**) with respect to the relationship between two or more persons, means the possession, directly or indirectly by equity ownership, contract or otherwise, of the power to direct the management or policies of the specified person;

a party's **Group** means, in relation to that party, it and its Affiliates;

Confidential Information means all information of whatever nature relating wholly or partly to the Project or the affairs of any member or members of [redacted]

(a) is supplied by or on behalf of any member of [redacted] Group to the Employee whether orally, in writing or otherwise and whether before or after the date of this

H. Three Lines of Defence Model Adopted by Company B (Document 10)



I. Corporate operational and ERM reporting model (Document 6)