Management Control for Risk Management in the Public Sector: A Levers of Control Perspective

by

Vasileios Georgiou

Submitted in fulfilment of the requirements for the degree of

Doctor of Philosophy in Accounting and Finance

College of Social Sciences, Adam Smith Business School

University of Glasgow

1st of October 2024

Abstract

This thesis investigates the integration, or the interaction and influence, of risk management tools with management control systems and vice versa, within the Greek public sector. It employs the Levers of Control (LOC) framework (Tessier and Otley, 2012), to examine how these two processes are integrated and influence each other in practice, in contemporary public sector risk management. This is done in an effort to reconcile previous literature that recognises this integration but requires more evidence on their practice (Bracci et al., 2022). Hence, this study addresses a gap in the existing literature by providing empirical insights into how management control systems deployed in public sector risk management, and how they interact with each other to form response to an organised uncertainty. Through this integration, this study also unravels how management control systems are utilised to make sense of emergent risks, in an effort to answer the calls to better understand the connection of management control and risk management (Bhimani, 2009; Soin et al., 2013). Specifically, it examines the case of a Greek public sector organization responsible for overseeing projects funded by the European Union. This organisation has a well-designed and implemented risk management system, that interacts with various controls tools to build a holistic approach to managing risk. Through the revised Levers of Control framework (Tessier & Otley, 2012), it was evident that risk affects the design and function of control systems at all organisational levels, with performance management being central in that effort. Moreover, various control tools were used interactively to induce knowledge and graphically depict uncertainty.

Table of contents

List of tables

List of figures

List of Appendices

Acknowledgments

To my supervisors, George and Alvise, who kept me strong all these years, and to everyone who supported me throughout this PhD. I also want to thank everyone who believed in me. Thank you.

Progress, not perfection.

Author's declaration

I declare that, except where explicit reference is made to the contribution of others, that this dissertation is the result of my own work and has not been submitted for any other degree at the University of Glasgow or any other institution

Printed Name: Vasileios Georgiou

Signature:

List of abbreviations

Abbreviation	Meaning	Page
BIM	Building Information System	**136**
EC	European Commission	**21**
CRO	Chief Risk Officer	**99**
HR	Human Resources	**132**
IIS	Integrated Information System	**128**
KPI	Key performance Indicator	**126**
MA	Managing Authority	**95**
MCS	Management Control System	**116**
PADF	Partnership Agreement for the Development Framework	**21**
PMS	Performance Management System	**55**
PSO	Public Sector Organization	**19**
PPP	Public-Private Partnerships	**51**
QAO	Quality Assurance Officer	**99**

QAS	Quality Assurance System	**143**
SRSA	Special Regulatory Support Agency	**96**

Abbreviations list: meaning of abbreviations and page first defined or used

Managing Risk and Uncertainty in the Public Sector: A Levers of Control perspective.

1 Introduction

1.1 Introduction

In this chapter, the purpose, background and main elements of the study are introduced. Section 1.2 introduces the background of the study, in an effort to introduce, and frame the main concepts and phenomena that this study is interested in exploring. The next section, section 1.3 sets up the context of the study, in relation to these concepts and phenomena, and shows the issues, or research gaps, in the literature. Moreover, this section shows how these issues were addressed, in brief. After that, section 1.4 introduces the main contributions of the study, and the last section, describes the structure of this dissertation.

1.2 Study background

Since the mid 1990s, risk has been redefined in contemporary organisations (Power, 2004c). Two extreme organisational events, one involving a rogue trader and another involving a mismanaged disposal of an oil rig of a multinational energy company, redirected the attention of the public. These two events attracted a lot of societal attention, and resulted in high reputational damage, that shifted organisational attention from mere financial risks to a wider agenda of risks, including non-quantifiable elements (Gephart, 2009). This attention shifted organisational procedures to include a more holistic and wider focus on managing organisational risks, that they could not imagine before. These risk agendas were dictated by societal pressures stemming from the events in the mid 1990s that redefined risk and risk management in both the private and the public sector. As a result, organisations realised that they needed to focus their attention to a wider array of new risks, that could hinder their organisational objectives. This was a shift from a mere focus on financial risks, to managing a wider notion of risk in an effort to exude “auditability, controllability and accountability” (Jemaa, p.3). This attention had to do with managing risks, and also be shielded against any

kind of unknown risks (uncertainties) that could hinder their sustainable development, hence, the need to manage an organised uncertainty (Power, 2007). That shift triggered a series of reforms in organisational risk management.

First and foremost, organisations shifted their attention to new risk categories, that included operational, reputational and legal risks (Power, 2007). This risks, usually intertwined with each other, had to do with new areas of organisational attention that was not strictly quantifiable, and they also had to do with how failure in internal processes, human actions, organisational systems or external events, could prove to be detrimental in organisational success, and could result in loss or reputation and various legal commitments. As a result, contemporary organisations realised the need to be accountable to these, and other risks, that can hinder their objectives and can lead to loss of reputation, if not included in their risk appetite (Power, 2007; Jordan et al., 2013). In turn, this risk accountability gave rise to a new set of governance rules, which redefined the notion of contemporary risk management. This new umbrella of governance, risk governance, has been established to promote structures that realise risk and uncertain events that can hinder organisational objectives (Renn & Klinke, 2016), as well as to provide risk and uncertainty related decision-making tool (Hutter, 2006). Finally, and in an effort to promote good practice for all the above, regulatory and meta-organisations have emerged to help in devising, promoting and revising best approaches to manage contemporary risk (Power, 2007). These meta-organisations, such as the global COSO committee, or local authorities such as the Financial Reporting Council in the UK or Basel Committee on Banking Supervision and the regulators devising the Sarbannes-Oxley Act of 2002, are but a few examples of regulators and meta-organisations, that are responsible for promoting best practice. Therefore, contemporary risk management practice and culture, has seen a significant shift in the last two decades, with clear implications for practice.

This study is concerned with how this contemporary practice of risk management is unravelled in organisations. These processes, have to do with managing risk, but also recognising this risk as a part of a wider environment of uncertainty that any organisation is exposed to. In this sense, modern risk management has to do with managing an organised uncertainty (Power, 2007) and it has also become strategic. That is because, modern risk management has been focusing on any event or action that can disrupt, or cause uncertainty about, the ability of an organisation to meet its strategic, and operational objectives (Andersen, 2016). The main tenet

of this thesis is that understanding how contemporary organisations manage risk requires an understanding of the role that various internal controls and information systems play in the process (Power, 2007; Scheytt et al., 2006; Bracci et al., 2022). Through auditing and managing internal processes, pointing out systemic or other organisational inefficiencies, and inducing organisational learning, internal controls aim at minimising organisational risks. In turn, information systems, very integral and complementary to internal controls, offer information about all organisational procedure's that can be used to point out inefficiencies and increase organisational learning. This points out the increased importance and reliance of organisations to management control systems, that have been deemed central and closely connected with managing contemporary risks (Bhimani, 2009; Soin et al., 2013; Bracci et al., 2022).

1.3 Setting the context: summary of the study and research gap

A context that has been heavily affected by the contemporary developments in risk management, is that of the public sector (Woods, 2009; Palermo, 2014; Bracci et al., 2022). That is because, in the wake of public failures (Andreeva et al., 2014), public sector organizations (PSO) are in scrutiny and in societal and regulatory pressures to manage risks in the provision of public services. That, together with financial constraints (Louth & Boden, 2014; Palermo, 2014), demands for an increased value for money approach to the provision of public services (Rika & Jacobs, 2019) and a shift to the provision of these services by a mix of private, public and third sector organisations, has created an environment that requires a significant attention to managing risk and be shielded against uncertainty. That environment has imposed a new era of "new" risk management in the public sector (Hood & Miller, 2009, p. 3), in an effort to manage public risks (Andreeva et al., 2016) that are associated with bridging the gap between society and public service providers. That era is also characterised by an increased level of uncertainty and reputation risk management (Power et al., 2009; Vinnari & Skærbæk, 2014). Reflecting efforts to exude accountability in Late Modernity, and amidst the New Public Management reforms, public sector entities, employ management control systems to manage these public risks (Rana et al., 2019) and they even utilise sophisticated Enterprise Risk Management Systems that employ management control tools in many instances (Rana, Hoque & Jacobs 2019). In fact, management control systems are integrated with risk management practices in PSO (Bracci et al., 2022). Examples of this integration has been clearly evidenced in the literature (Woods, 2009, 2010; Collier & Woods,

2011; Rocher, 2011; Rana, Hoque & Jacobs, 2019; Rana, Hoque & Jacobs, 2019). In an effort to point out antecedents of the implementation and effectiveness of various risk management practices around the world, this literature also provides examples of the connected control tools that these processes entail. For example, of particular importance to these risk management practices was the centrality of performance management systems (Cuganesan et al., 2014), in the effort to manage public sector risks. However, in this literature, despite examples of what control are associated with managing public sector risks, they do not show how the process of integration works in practice (Rana et al., 2019; Bracci et al., 2022; Rana et al., 2022). In fact, the practice of how risk management interacts with various control tools in a PSO context still required more evidence in the literature to be understood (Bracci et al., 2022). There is some effort to provide such evidence by private sector studies (see, for example, Collier & Berry, 2002; Mikes, 2009, 2011; Arena et al., 2010; Paape & Speklé, 2012; Arjaliès & Mundy, 2013; Jordan et al., 2013; Caldarelli et al., 2016). However, even there it is still unclear, as studies do not focus on the clear integration of risk management and management control. At the same time, it is important to provide evidence of this integration in the PSO. That is because results will be different and will entail a different approach than the private sector (Rana et al., 2022). It is important to provide evidence in a context that is expected to differ in terms of processes, mainly due to the antecedents of New Public Management (Lapsley, 2009). That process of how this happens is not only worth exploring, but it will also have the potential to inform best practice (Bracci et al, 2022; Rana et al., 2022). That will fill a significant gap in both the management control (Bhimani, 2009; Soin et al., 2013) and the risk management literature (Bracci et al, 2022; Rana et al., 2022).

To fill this gap in the literature, this study utilised a case study design (Baxter & Jack, 2008; Yin, 2014) and a middle-range methodological orientation (Laughlin, 1995, 2004; Broadbent & Laughlin, 2008) to provide empirical evidence on the integration of control systems in managing public sector risks. By utilising a theoretical lens, the revised Levers of Control framework (Tessier & Otley, 2012), the author entered the field of a Greek public sector institution to gather evidence of how they utilise management control systems to manage risk and uncertainty (Broadbent & Laughlin, 2009, 2013). The case study was a Greek public sector institution, overlooked by the Ministry of Development and Investments, which, in turn, overlooks the materialisation of transportation, environmental and sustainability projects that

utilise European Union funds. The study focused on the round of funds associated with the European Commission's (EC) 2014-2020 Partnership Agreement for the Development Framework (PADF), a round of European Commission's funds allocated to European Countries, for the development of infrastructure and human capital. Data were collected between July 2022 and October 2023. This organisation, for the 2014 2020 programme period, was allocated 4.7 billion euros, to allocate to different private, public or third sector organisations, that could materialise different road, subway and port networks, as well as sustainable energy, production and development projects around Greece. To manage these funds, the case organisation utilises a sophisticated risk management tool, complemented by an amalgamation of other regulatory, performance management and self-managed systems, that have risk management as a central component. Management control systems are central to this framework.

Through the lens of Tessier & Otley's (2012) Levers of Control, evidence was collected on how the case organisation utilises management control tools to manage risk (and their operations in general) to ensure proper allocation and full absorption of all European Commission funds. In brief, the case study confirms that risk management and management control are integrated in the public sector (Bracci et al., 2022), by providing evidence of the processes behind these integrations, how risk management influences controls, and how control plays a crucial role in managing risk in the case organisation. At the same time, key success factors are also discussed, and problems of the system. Evidence suggests that the case organisation utilises a set of performance measurement and management tools, which translate targets into measurable elements to measure organisational, project and programme performance at both the strategic and the operational levels. These targets, reflect the amount of acceptable risk for managing the organisation itself and its projects. Furthermore, this process is complemented by additional control tools that reflect rules, regulations and other organisational values at both the strategic and the operational levels. Effectively, these rules reflect the risk boundary within which the organisation needs to operate in order to materialise project dictated by the European Commission. Moreover, to make sense of uncertainty, the case study utilises a web of meetings, a living network of information exchange between all organizational members, to communicate emergent risks and mitigating mechanisms for the programme and the projects. These meetings are complemented by the use of sophisticated

software, and at their heart lies the formal risk management meeting which was built specifically to communicate all organisational risks and mitigating mechanisms to all organisational levels. That is because these risk-cantered meetings collect and filter all information before it is disseminated across the organisation. Finally, and to strengthen all the above tools, the case organisation has instilled, from the top, and championed by their Chief Risk Officer and the Chief Quality officer, a risk mindset that effectively relates all organisational decisions to managing and mitigating risk and uncertainty. This risk mindset translates into the development and maintenance of a clear and sophisticated risk management tool. A key success factor, this mentality infuses risk and uncertainty decision-making at all organisational levels and enhances/strengthens the use of all other control tools for risk management. All the above, are supported by sophisticated software that depicts and communicates all relevant information required in all procedures. Conclusively, the case study, having performance management at its heart, utilises an amalgamation of interconnected control systems, to manage their operations and service delivery, with risk being at the heart of these systems, influencing their operation, structure and focus (Rana et al., 2022).

1.4 Contribution

This study contributes to current management control and risk management literature in several ways. First, this study contributes to the continuous calls to better understand the relationship between risk management and management control (Bhimani, 2009; Soin et al., 2013). These authors have argued of the interconnectedness of these two practices, and they have shown that literature would benefit from additional evidence to understand this relationship better in practice. This is of particular importance in the public sector, and this study adds to the ongoing calls for an understanding of this interconnection. Indeed, calls have been made to better understand the processes are associated with the integration of risk management and management control (Rana et al., 2019). For that matter, examples of management control systems that aid in managing public sector risk do exist (for example Collier & Woods, 2011; Rocher, 2011; Rana, Hoque and Jacobs, 2019). However, little is known on their practice, and specifically the practice of how they are integrated with risk management frameworks (Bracci et al., 2022; Rana et al., 2022). That is because literature to date has focused on the implementation of risk management and its effects on MCS, successful factors of risk management implementation and very little on the direction of the risk management and MCS

integration (Bracci et al., 2022). According to these authors, the processes of integration need to be understood better, especially through case studies from international contexts, in order to unravel risk management implementation success factors, control influences and inform policymaking and practice. This will add to the ongoing calls for more evidence on the different role management control systems play in managing risk in the provision of public services (Rana et al., 2019). These authors argue that, following the underpinnings for New Public Management, management control systems will work differently in the public sector, compared to other sectors, due to contextual contingencies, and that this is something worth exploring. In doing so, evidence will be provided for the process by which not only risk-oriented controls operate, but also how these controls co-exist and are influenced by other control systems, something that is missing from the current literature (Rana et al., 2019). As the authors suggest, this will have implications for MCS design, structure and behaviours in PSO. To summarise, this study, through a case study design, provides evidence of the integration and co-existence of management control systems for public sector risk management, with an emphasis on unravelling the processes behind this integration. In doing so, it also provides a theoretical basis to understand public sector risk management, something that is also missing from the literature (Bracci et al., 2021). The study, via the revised LOC framework, will also add to the current management control literature on its applicability and conceptual robustness, as requested by the authors, and especially through the use of case studies (Tessier & Otley, 2012).

Moreover, this study adds to the need to better understand a specific element of control, that of performance management for risk in the public sector, a tool that is key in managing public risks (Power, 2004b), but partly explored (Cuganesan et al., 2014). It is clear in the literature, that performance management systems do aid public sector risk management (Woods, 2009, 2010; Rana, Hoque & Jacobs, 2019), despite their inherent issues in quantifying public sector performance, due to its complexity and multi-dimensional character (Bouckaert & Balk, 1995; Smith, 1995). However, these are only part of the wider control system of public sector institutions, and they should be associated with other control systems (Cuganesan et al., 2014). More empirical evidence is needed to show how this is done in practice, to also understand their wider contribution to managing public risks. This will aid in understanding the role of performance management and their place in managing public risks, as part of a wider management control for risk management system or set of systems (Cuganesan et al., 2014).

Since PMS are central in PSO risk management (Power et al., 2009), this study will add to the current literature by providing evidence of their integration with risk management framework in the public sector.

Furthermore, the current study, and in an effort to further understand the use, role and influence of management control tool for managing public sector risk (Bhimani, 2009; Soin et al., 2014; Bracci et al., 2022), offers evidence on the use of management control tools in a very important area of risk management: managing emergent risks. Following the brief definition that risk management is associated with the identification, assessment and monitoring of risks (Power et al., 2013), there are limited examples in the literature of what controls systems are associated with identifying emergent risks. As a result, their integration also requires attention and it is something that will add to the needs to understand it better (Bracci et al., 2022). Such systems not only exist in contemporary organisations, but they are also important in making sense of uncertainty, which is key in contemporary risk management (Scheytt et al., 2006). In fact, they can even exist tacitly, and they play a vital role in communicating emergent risks (Fischbacher-Smith & Fischbacher-Smith, 2014). There is some very limited evidence on the use of controls towards identifying emergent risks (Themsen & Skærbæk, 2018) in the case of public sector mega-projects, but this only partly adds the literature (Jordan et al., 2013), as it offers a very specific and narrow area of focus. Since this process of identifying emergent risks is vital in public sector risk management (Power, 2007), this study, in a further effort to extend current literature on the integration processes and practice of control systems for risk management (Bracci et al., 2022), has provided empirical evidence on the matter.

Finally, this study adds to the management control literature by utilising the revised management control framework, to test its conceptual validity and analytic generalisability, through a case study design, as requested by the authors (Tessier & Otley, 2012). As mentioned before, this study is utilising the specific management control framework, to address the gaps in the literature and offer insights of the processes of controls utilised for risk management in the public sector, and the integration between the two. The evidence suggests that the revised LoC framework is applicable to the case study, and, for the most part, its concepts are validated by the empirical evidence. However, some elements and relationships were not confirmed and therefore adjustments for the use of the framework in the public sector are also discussed.

Conclusively, this study contributes to management control and public sector risk management literature in several ways. Initially, by exploring the integration of risk management and management control through a Greek public sector case study, this study addresses calls for evidence from international contexts (Bracci et al., 2022). It also responds to the need to understand how management control and risk management tools integrate in public sector organizations (PSOs), in an effort to enhance practice and policy (Rana et al., 2019; Rana et al., 2022). Hence, this study will provide insights into management control tools used for PSO risk management and the processes by which these tools are integrated with risk management frameworks. While previous studies (e.g., Woods, 2009, 2010; Collier & Woods, 2011; Rocher, 2011; Paape & Speklé, 2012; Rana, Hoque & Jacobs, 2019) examined the implementation of risk management frameworks in PSO and what control tools were utilised in that effort, this study will extend this literature by offering insights into the processes of the integration of control tools with these risk management frameworks. In this effort, this study will focus on specific management control tools, for example PMS tools which are central to managing PSO risk (Power, 2004b), in an effort to contribute to understanding how these tools integrate within PSO risk management and operate with other control systems (Cuganesan et al., 2014). Additionally, the study will address the limited evidence on managing emergent risks through management control systems, particularly information-sharing systems (Scheytt et al., 2006; Fischbacher-Smith & Fischbacher Smith, 2014) and control tools for identifying emergent risks (Themsen & Skærbæk, 2018; Jordan et al., 2013). Finally, by applying the revised Levers of Control theory (Tessier & Otley, 2012), this study aims to enhance both risk management and management control literature, contributing to understanding how these systems integrate in practice (Rana et al., 2020), how they are connected (Bhimani, 2009; Soin et al., 2014) and how a specific management control theory is applied to management control systems integrated in PSO risk management frameworks.

1.5 Dissertation structure

This dissertation is structured as follows. Section 2 presented the main background of the study, including definitions of risk and uncertainty, and how these have been developed in managing contemporary organisational risk. After that, this section will focus on reviewing the literature on public sector risk management, its background and current state, as well as its interconnectedness with management control. That effort will later identify the main literature

in this area, and discuss the main issues of this literature, leading to the motivation, contribution, and eventually, the research questions of this study. Then, section 3 will unpack the main concepts and elements of the Levers of Control framework that will be utilised in this study, by briefly sowing how it has reached its current conceptual state. After describing the theoretical framework, a discussion on its use and importance in this study will be articulated, by clearly showing how it is conceptualising risk and uncertainty at its core, and how it is useful in providing a basis for understanding risk management associated management controls. Afterwards, section 4 will discuss and justify all the research design, methodological approaches, data collection and analysis, as well as ethical management approaches that this study will utilise. Section 5 will then present the main findings of this study, and section 6 will discuss these findings in light of previous and contributing literature. Finally, section 7 will conclude the study, and offer limitations, as well as avenues for future research.

2 Literature review

2.1 Introduction

This chapter introduces the background of the study and articulates the main research gap and motivation, through critically discussing the relevant literature. Sections 2.2 and 2.3 begins with a background of the notion of contemporary risk management, how it emerged, and how it took the shape that it has in modern organisations. The notions of strategic risk management are shaped here and their connection with management control. Section 2.4 then goes on to offer the focus of the study, and specifically how contemporary risk management in formulated in contemporary public sector institution. In that effort, this section shows how the connection between risk management and management control exists in the current literature and finishes with setting the knowledge gaps in said literature, the contribution of this study as well as its main research questions.

2.2 Defining contemporary risk and uncertainty

Beck (1992) argued in his thesis that the current society experiences an increased exposure to risks. Due to this exposure, society's members have developed a risk attitude towards identifying and being prepared to the various risks that they may cause negative consequences to them or their world. This multiplication and variety of risks that society is being exposed to consists, mainly but not completely, of man-made risks (Beck, 1992). In general, and despite the ambiguity of the term, risk is defined as the calculated probability of an event occurring and the consequences that this may have (positive or negative) to the risk taker (Anderson, 2011). Within this environment of high-risk exposure, any phenomenon that occurs, is hard to explain, be anticipated and confronted. That has to do with uncertainty and the fact that there are risks out there that exist without even being realised and with a small possibility of being confronted with. These uncertainties create fear and anxiety to the society that tries to develop way to understand and face the unknown. It is the multiplicity and complexity of risks that society is exposed to that makes uncertainty even greater. Borrowing a definition from the management control literature, uncertainty is defined as the inability of an actor to identify not only how probable an event can be but also what kind of consequences this event may have (Otley, 2014). Together, risk and uncertainty, in Beck's (1992) *Risk Society,* form the

amalgamation of known and unknown harms or opportunities that need to be realised by society since exposure to such notions is the only certain things that needs to be confronted and managed.

A significant impact from this environment has already been realised (both in terms of positive and negative effects) to one of the members of society: organizations. Organizations of any form, either private, public, governmental, regulatory or professional, non-governmental and non-for-profit have realised that they need to manage the uncertainty reflected in the risk society in order to survive. Contemporary organizations' attention has drifted away from the traditional financial risks (Power, 2004c, 2007). As part of society, they are currently exposed to a variety of risks, both tangible and intangible, that can hinder their objectives, expose them as illegitimate and thus threaten their survival. In order to survive, organizations need to pay attention and manage various risks that come from two sources. The first source has to do with the organization itself and its competency of analysing and confronting historical incidents that had negative effects on its operations (Power, 2007). The second source of risks is agreed with and comes through a discourse with the organization and its various stakeholders (Power, 2007). Together, these two sources of risks form an integrated set of risks that can have an effect on organizational objectives (Renn & Klinke, 2016). Once identified, risks are fed into the risk management apparatus of the organization that consist of various control mechanisms aiding at the identification, assessment and monitoring of risks. These practices are advised by the most prominent risk management framework named Enterprise Risk Management (COSO, 2004). The purpose of this framework is to advise organizations on a more integrated and holistic approach to managing their risks, a sophisticated approach to the use of controls towards risks management and offer guidance, and legitimacy, when there is a risk management failure.

As part of their risk management efforts, organizations are more scrutinised than ever when it comes to risk management (Power, 2007). Indeed, various regulatory and professional bodies around the globe are responsible for advising on new risk management practices and also monitor organizations to seek validation for the appropriateness of their procedures, or controls, toward managing their risks (COSO, The Institute of Risk Management and the Financial Reporting Council in the UK, among others). Moreover, organizations are also held responsible by their various stakeholders for managing the risks they are exposed to

appropriately, especially the ones that have been identified as important. Failure to do so results in public criticism and question of legitimacy (Power, 2007). In order to survive, organizations need to manage their risks and also have procedures in effect to manage various risks that they have not identified yet or have done so and have not included in their risk agenda. Therefore, organizations are exposed to a volatile environment that holds risk as its central component. Within this environment, they need to manage risks, be capable of having a more holistic approach to understanding their risks, be open to learning of new risks, be precautious of unknown risks (uncertainties) and be held accountable for any failures of doing all the above. Due to their exposure to such an environment, organizations have developed a new approach that can help them to survive and cope with these demands. That approach is the central idea to a new form of governance named risk governance (Hutter, 2006; Power, 2007). Organizations were not always required to adhere to such environment. This environment came forward due to a few significant events that shook organizational life and its relationship with society during the middle of the 1990's.

The "risk management explosion" or the so-called *Risk Management of Everything* came into consideration by organizations, regulators and the society during 1995 (Power, 2004c, p. 9). In that year, two events occurred that proved significant for the reconceptualization of risk management in organizations. The first event was the collapse of Baring's Bank. In that event, a rogue trader was responsible for the loss of millions of pounds on behalf of the bank as he engaged in probabilistic gambling of the bank's trading securities. The second event occurred when Shell, the multinational oil company, decided to dispose of one of its obsolete oil extracting bases, called Brent Spar, in the middle of the ocean. This decision, backed-up by the UK government, initiated public criticism and many organizations, such as Greenpeace, stood against such a decision and demanded a land disposal of the base. This event, magnified by substantial media coverage, cost Shell huge amounts of losses as the company's product were boycotted, followed by a loss of reputation for the company (Power, 2007). These two events proved crucial in the development of the new forms of risk management in organizations. More specifically, organizations realised that financial risks are not the only ones that can hinder their objectives and that society, especially in the form of organizational stakeholders, has expectations that need to be met for organizational success (Power, 2007). Furthermore, organisations realised that, while operating in a global environment, they are exposed to various

kinds or risks that need to be known and need to be managed to ensure survival. In order to embed more risks in their risk management processes, organisations also realised that they should look into failures of the past and use them as benchmark for risk learning and future competency (Power, 2004c).

Two imperatives for organisational risk management emerged in the wake of those events. First, society demanded a more holistic and scrutinised approach to organisational risk handling (Power, 2007). That was reflected in the rise of various regulatory and professional bodies that started seeking new ways for transparent and responsible risk management from organisations to meet, as much as possible, societal expectations (Power, 2004c). Following that, organisations turned their attention to widening the boundaries of their risk analysis into a broader understanding of risks. That would include a framework that does not depend solely on quantifiable and tangible risks (Gephart et al., 2009). That framework would be based on an interplay between risk analysis and calculative techniques and the consensus of various risks that are reflecting the expectations of various stakeholders (Power, 2007). In addition to financial risks, various risks need to be quantified, when possible, together with an information-sharing attitude towards risks that are hard to quantify, majorly with key stakeholders. The difficulty in the latter, however, intensifies the difficulty in understanding organisational risks. The more stakeholder voices are engaged in reaching an understanding of risks that organisations need to care about, the lower the accuracy of the description of such risks (Power, 2007). In such a case, it is difficult for organisations to make sense of the risks they need to pay attention to. That further creates issues with accountability and increases the uncertainty that organisations need to cope with. Subsequently, organisations realised that risk management has to do more with managing uncertainty rather than risks. Within an environment where stakeholder engagement is crucial to risk identification and organizational success, uncertainties about risks themselves become multiplied as stakeholders' expectations become multi-faceted (Power, 2007). Considering that, organisations, assisted by various regulatory and professional bodies, started implementing new forms of control to manage their risks, expanding their risk horizons, meeting stakeholder expectations and holding a defensive stance against uncertainty. This effort included the invention and consideration of new categories of risk, which, together with the financial and currently identified ones, would

inform the areas of accountability and responsibility of organisations towards the management of an organised uncertainty.

2.2.1 Towards managing uncertainty: new risk categories, stakeholder engagement the pursuit of risk accountability

2.2.1.1 The emergence of new risk categories

Prior to the major events of 1995, organisations were majorly concerned with specific and limited types of risks. Those risks were mostly quantifiable and analysed through probabilities, included in the aforementioned risk analysis, and they were cantered around financial risks (Power, 2007). Limited attention was given to other risks categories, for example, health risks for hospitals. The two major events of the 1995 described in the previous section gave birth to two more major categories of risks: operational and reputational risks. On the one hand, the failure of Baring's Bank made society and organisations aware of the failures that people and constant, repeated and routinized rogue operations can have to an organisation (Power, 2004c). On the other hand, the power and influence of stakeholders, enhance by the intervention of non-governmental bodies, focused the attention to organisational reputation loss and, subsequently, value loss, in the wake of certain events (Power, 2007). Those events pointed out that misinterpretations of the effect of primary organisational risks, could have a huge negative effect on the organisation's reputation. As mentioned before, these categories of risk are not the only area of organisational attention, but they form its core conception. Especially for reputational risk, they are reflected to the general picture of risk management because there are numerous risks that can negatively impact organisational reputation (Power, 2007). These risks give birth to additional risks and are well connected as the one can influence the other (Power, 2007). In addition, they represent the core part of the organisational risk picture that incorporates other risks as well as classification of processes towards uncertainty handling.

Operational risk considerations, although very limited, existed prior to the mid 1990's events (Power, 2007). However, they were majorly ignored and undermanaged. Indeed, prior to that era, operational risks were not visible because organisational operations were so routinized, standardised and unquestioned that no one was able to make sense of signals and internal controls were weak in that respect (Power, 2007). The collapse of Baring's Bank served to

institutionalise, expand and rationalise the term operational risk. One of the meta-organisations, i.e. organisations formed by various organisations of the same industry to overlook the industry's regulation, that had already made sense of the importance of operational risks was the Basel Committee of the bank industry (Lleo, 2009). The Basel Committee was the first proponent of the expansion and institutionalisation of operational risks as they are made sense up to the present. That is not surprising, however, because the era of the rise of operational risk coincides with an era of intense regulatory reforms concerned with risk handling and internal controls in the banking sector (Power, 2007). Such an analysis, however, is out of the scope of this chapter and serves only as a starting point for defining operational risks. Indeed, it is also not surprising that the Basel Committee offers a definition about what operational risks is. According to that, operational risks are defined as the risks "of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events" (Basel Committee of Banking Supervision, 2001, p. 2). This definition is appropriate, but it is also characterised as very general, with a particular purpose (Power, 2004c). Indeed, operational risk is any loss or damage to the organisation that can occur from rogue employee behaviours, failure of systems to capture malfunctions in the organisation and any failure to capture the harmful effects of external events (Lleo, 2009). It is also not rare for organisation to face legal consequences in the wake of such events. Such cases are characterised by high impact and, at the same time, low probability events that are not easily identifiable by organisations and that can emerge from various sources (Power, 2007). Organisations have accepted that to manage such risks, they need to manage a package of "unknown and incalculable" risks and uncertainties (Power, 2004c, p. 30). Two consequences are evident from that. First, contemporary organisations have adopted sophisticated internal control systems that serve as evidence provided channels to transform such risks into visible and manageable entities (Power, 2004c). In the same way, organisations and regulators of risk management have accepted that operational risk is far from being completely understood and its management reflects an evolutionary process in search of the full picture of organisational risks (Lleo, 2009). That has an effect on internal controls as they need to be remodified constantly to serve as information providers for operational risks (Power, 2007). Equally important is the multidimensional presence of operational risks across organisations. As it is evident, they differ across organisations due to their character and nature of operations (Power, 2007). Therefore, operational risks serve as "boundary objects" across organisations (Power, 2007, p. 112). In

that sense, different internal controls and processes are utilised for different kinds of operational risks across organisations. Hence, operational risks represent both an important focus and a challenge for contemporary organisations. They are also very much connected with reputational risks as they have the ability to create a negative impression of an organisation's image once they occur (thus the high impact, low probability character) (Power, 2007).

Operational risks represent, but not fully, another category of risks that has equally concerned companies since the events of 1995. This is the category of reputational risks that are associated with loss of reputation and, in turn, loss of value and business due to loss of legitimacy (Power, 2007; Power et al., 2009; Huber, 2011; Rika & Jacobs, 2018). The influence of media and lobbying organisations shape stakeholder perceptions about an organisation, thus majorly enhancing the impact of those risks (Bebbington et al., 2008). In the case of Shell and the Brent Spar incident, the decision to pollute international waters by the disposal of oil rig equipment did most damage to the organisation due the involvement of various media coverage and pressures from Greenpeace. Shell received a negative reputation; people around the world boycotted its products and the company lost value. This event became an urge for organisations around the globe to attend reputational risks. Such risks were majorly unattended before due to organisational technocratic focus and interest. However, as they represent stakeholder expectations, incorporating them in the organisational agenda is crucial for meeting objectives and gaining legitimacy. In order to assess the reputation of organisations, stakeholders have developed ranking measures over the years that represent and attempt to understand and judge such reputation (Power, 2007). By those measures, society imposes transparency of the handling of operational risks to organisations. Higher ranking means better reputation and more adequacy to the governance of reputational risks and vice versa (Power, 2007). However, meeting society's expectations through an ethical approach to operations and decision-making is not the only reason behind such an attention to reputation. There are two additional reasons that deem operational risks crucial to the survival of organisations. First, any loss to an organisation's reputation has a systemic effect (Power, 2007). An organisations reputational loss equals the reputational loss of the industry this particular organisation is a member of (Rika & Jacobs, 2018). Similar to operational risks, risks associated with reputational loss impose various damages to organisations that derive from failure to comply with laws (Power, 2004c). In the event of a decision that results in legal damages to the organisation, those damages are

often followed by loss of reputation. Therefore, another consideration for organisations falling into the category of reputational risk is that of legal risks. Those risks are defined as risk associated with the loss of organisational value due to failure to comply with regulation. For the above reasons, organisations are paying particular attention to any risk that can hinder their reputation by feeding them into, once again, a set of internal control procedures.

The presence of legal risk, which is a by-product of both operational and reputational risks, emphasizes the centrality of the latter but also points out that they are not the sole concentration of organisational attention. Organisations are also concerned, to a lower extend, with other categories of risks, equally important, deriving either from operational or reputation risk, or, from other risks reflecting the expansion of an integrated and holistic approach to risk management. It is evident that reputational risks are also associated with ethical and public perception risks (Power, 2007). Ethical risks are those associated with an unethical behaviour of the organisation when it comes to meeting organisational objectives (Power, 2007). These risks can cause reputational loss because organisational interests are prioritised against stakeholder interests. Equal to reputational risks, that results in a loss of trust to the organisation and, often wise, the industry, and results into a bad image for such organisations. That is extended to a distorted organisational image, which results in loss of trust reflected in public perception risks (Power, 2007). The latter are associated with risks staining the image of the organisation and are interconnected with reputational risks. Finally, organisations are also considering a variety of political risks, or risks associated with failures to meet organisational objectives due to changes in the political environment (Power, 2007). Indeed, corporations, especially those operating in multinational territories, are faced with the political agenda in those territories. Thus, it is imperative for organisations to decide which of those risks are important to them and how they can influence them. In considering such risks, organisations form risk objects reflecting each one of these categories. Risk objects are, by definition, the risks, or risk packages, that organisations have identified as crucial to meeting their objectives and represent the translation of risks into manageable entities (Power, 2007). Due to the multi-faceted nature of those risks, the risk management of an integrated number of risk objects represents a challenge. And that challenge, stems from the enhanced need to exude accountability.

2.2.2.2 The rise and necessity of risk accountability

The central reason behind such a shift to organisational attention to increase awareness of exposed risks was the requirement, especially from society, for risk accountability (Tekathen & Dechow, 2013; Andreeva et al., 2014; Palermo, 2014). As Power (2007, p. 196) points out, organisations need to manage, under the idea of an organised uncertainty, a "growing inventory of risks objects". As mentioned before, risks objects delineate the domains of risk categories that the organisation needs to manage. This form of accountability is very closely associated with the operations of the organisations and their existence. These operations need to exude, together with opportunity and enterprise for organisational success, the value creation and stability of the organisational environment (Power, 2007). The first step to increase accountability and transparency is to make sense of the organisational risk appetite. Such appetite delineates all those risks that an organization is willing to incorporate in order to meet its objectives (Jordan et al., 2013). The experts and the guardians of such appetite are the Chief Risk Officers and the internal auditors whose role has significantly intensified to help organisations adhere to the new demands for risk management (Power, 2007). On the one hand, the role of the internal auditor was not a new in organisations, however it was overlooked by external auditing (Spira & Page, 2013; Power, 2007). It as the intense dependence upon internal controls that increased the necessity of internal auditors (Power, 2007). On the other hand, Chief Risk Officers did not exist as much prior to the risk explosion era (Power, 2007). It was the requirement of an extended approach to risk management that necessitated their role in organisations as risk experts and organisational members that have a concrete responsibility towards risk management, risk learning and internal control (Jemaa, 2022; Power, 2016). These experts, especially more recently, strive to promote best practice in all organisational members, in an effort to make them realise the value of engaging with risk management (Brivot et al., 2017). These risk talks, as they have been coined, aim at increasing organisational effectiveness, value, and more efficient resource allocation (Mikes, 2016). With those two roles, organisations strive for risk accountability. However, this accountability is not one-dimensional.

First, organisations are responsible for the risks they have identified and have included into their risk appetite. That said, organizations are held responsible for, in the event they are aware of a risk, letting their activities be held in such a way that this risk is resulting in unfavourable

consequences for the organizations itself, but also the environmental-societal parameters that define it (Power, 2009). Once risks have been identified, negotiated and settled within the risk appetite of the organisation, then the organisations itself need to assess and mitigate, or exploit, the effect of such risks to its organisational objectives (Andreeva et al., 2014). Throughout this process, organisations have developed an attitude towards organising risk and uncertainty in an auditable form" (Power, 2007, p. 165). Furthermore, that form of auditability creates a specific "risk culture" within organisations that is centred on transparency and traceability of risk management processes (Power, 2007, p. 176).

As discussed before, one of the reasons behind the rise of internal controls towards managing risk in an uncertain fashion lies their capability of exuding transparency and reporting procedures (FRC, 2014). Organisations are developing an attitude towards effective reporting and standardised internal control procedures that has a direct effect on auditability of operations (Power, 2007). In this way, processes are easily traced and failure, or organisational risk learning is enhanced towards a greater effectiveness for risk management operations. The role of internal control has turned organisations, with specific attention to their risk management processes, "inside out" (Power, 2007, p. 34). That means that internal control is at the heart of organisational accountability towards responsibility of risks because it responds to the demands of auditability of operations towards managing the organisational risk appetite (Sarens & Christopher, 2010). The role of the internal auditor to supervise and trace the internal control processes is highly important in such an environment (Power, 2007). Internal auditors are the gatekeepers of internal controls implementation, auditability and operation. Moreover, the reliance on internal controls, their intense auditability and their role in risk accountability is so crucial that reflects organisational attitude towards risks. Indeed, organisations have developer a "risk culture", which, based on the intensification of formal reporting and transparent procedures, leads to a greater ease on transparency and auditability or risk management operations that exude a blueprint for accountability concerns (Power, 2007, p. 176).

Another area that organisations are held accountable for is strongly connected with the management of an organised uncertainty. First, organisations have a limited capacity to understand their complete risk appetite (Scheytt et al., 2006). That derives from the aforementioned exposure to an uncertain business environment that leads to the imperative of organised uncertainty. Throughout this process, organisations need to build defences and be

prepared to handle a shock of uncertainty. Therefore, accountability rises from the fact that organisations need to build strong internal control defences to anticipate uncertainty and failing to do so will result in being held accountable to regulators and society (Andreeva et al., 2014; Palermo, 2014). Organisations, need to develop an "as if" attitude towards their operations and their internal controls need to be built in such a way as to point out or anticipate uncertain events and absorb them (Power, 2004c, p. 59). In order to ensure alignment with this attitude, internal controls are once again built to be auditable and transparent with the production of relevant information and data. These data contribute to the analysis of uncertainty, transformation of this uncertainty into risk objects and risk appetite enhancement towards an accountability of known risks. Therefore, the accountability of known and unknown risks complements one another with a central proprietor, the internal controls and their auditable function (Power, 2007). These practices of accountability, risk management of an organised uncertainty and the understanding of risk appetite, through expertise and organisational learning, are not scarce as definitions and reflect practical underpinnings in organisations (Tekathen & Dechow, 2013). They are working together as a system under the umbrella of the established, yet still proposed and under-developed, Enterprise Risk Management framework as merged by the Committee of Sponsoring Organisations of the Tredway Commission in 2004.

2.2.2.3 Risk governance: an umbrella for decision-making under uncertainty

The recent corporate failures, the development of the all-inclusive ERM practice of handling risks and the role of society as a crucial player to risk management and accountability, raise the demand of a new set of governance structures. These structures promote an effective management of an organised uncertainty through the analysis of an integrated set of risks and defences towards events that can hinder organisational objectives (Renn & Klinke, 2016). This new approach to governance has been termed Risk Governance and is concerned with the fundamental ideals of managing risk and uncertainty by involving risk-related decision-making (Hutter, 2006; Andreeva et al., 2014). In particular, this form of governance in contemporary society includes such organizational structures that deal with identifying and handling organizational risks (Power, 2007). However, because this form of governance emerged to promote societal needs, the kinds of risks have to be negotiated with various factors that are affected by the organization such as the government, various authoritative bodies, society and other relevant stakeholders (Andreeva et al., 2014). The need for negotiations arises due to the

fact that the organization needs to adhere to mitigating its negative impact both to the internal and its external environment. The aforementioned negotiated risks are transformed by organizations into organizational risks and are part of their organizational risk tolerance (Renn & Klinke, 2016). Even though this form of risk governance is imposed by authoritative bodies (see IRGC, 2005) and the ambiguity of its existence in contemporary organization (Renn, 2008), many organizations are reforming their governance structure to include the risk-handling element. Through appropriate tools and mechanisms, this element transforms the organization into a risk identifying, analysing and risk communicating entity that manages its internal and external risks imposed by the environment within which it operates. These tools are not other than various forms of internal controls, information systems and uncertainty precautionary structures. Through complementing activities and function for risk management, this integration leads to organisational improvements such as "value creation and targets achievements" (Arena et al., 2017, p. 67). This new form of governance is strictly associated with the approach to risk management and uncertainty as this is reflected by the rise of internal controls, the need to identify, understand and incorporate new risk categories and other forms of accountability and responsibility to the society (Palermo, 2014). All these structures that form the fundamentals of Risk Governance are overlooked, audited and improved by various, similar to COSO, regulatory and professional risk expert bodies. These bodies emerged to reconcile the challenges that contemporary organisations are facing with devising a complete and adequate focus on all organisational risks that they are faced with.

2.2.2.4 The emergence of regulatory and meta-organisations in managing uncertainty

The events of the mid 1990s expanded the understanding and handling or risks for organisations, which realised that they need to survive in an uncertain world. This understanding gave rise to a framework of risk governance within which, various internal controls are collaborating to help organisations manage a handful of risks they can identify and build defences against risks they might be engaged with. This endeavour, as reflected by the establishment and expansion of the organisational risk appetite, delineates the acceptable domain of uncertainty handling which aims at risk responsibility and accountability. Various organisational stakeholders are pushing for that accountability because history has suggested that risk-handling failures have resulted in the loss of value in the society (Power, 2007). As discussed before, this idea of uncertainty handling reflected in the aforementioned framework

is not easy to be managed by organisations. Internal controls are difficult to be applied and evolved, risk identification capacity is limited, and stakeholder engagement creates even greater uncertainty (Scheytt et al, 2006; Power, 2007; Andersen, 2016). To aid their efforts in efficiently and effectively managing risk, and to ensure compliance and best practice, organisations have to be exposed to various regulatory and professional bodies around the world. Often associated with a particular industry or country, the role of these bodies is to regulate and over watch the risk management processes and environments in organizations in order to ensure mitigation and exploitation, when appropriate, of risks. In doing so, these self-regulating, or industry and standards enforcing, organisations are devising their own risk strategies.

The most prominent self-regulating organisation that is associated with overseeing risk operations in organizations is the designer of the aforementioned ERM framework. COSO, or the Committee of Sponsoring Organisations of the Tredway Commission, is a global self-regulating, meta-organisation whose guidance is centred around organisational risk management. Formed by five private sector organizations (the American Accounting Association, the American Institute of Certified Public Accountants, the Financial Executives International, the Association of Accountants and Financial Professionals in Business and the Institute of Internal Auditors), COSOs central operations are associated with the guidance and development of the ERM framework and guidance on the implementation and use of internal controls with an aim at decreasing fraud (COSO website https://www.coso.org/Pages/default.aspx). Similar to COSO, two organisations are responsible for overlooking risk management operations in the UK. The Financial Reporting Council and the Financial Services authority are two organisations that are associated with guiding and devising appropriate risk management practices in the context of the UK. More specifically, the Financial Reporting Council is responsible for the development of a report that offers guidance for the development of a version of ERM in the UK. Indeed, the Turnbull report (ICAEW, 1999, later revisited by the Financial Reporting Council in 2005) is a framework that guides organizations in developing and executing appropriate risk practices according to their needs (FRC, 2005). Another similar risk management regulator is the state itself, which has devised the Sarbannes-Oxley act of 2002. In this act, there is a special section, named 404, that aims at offering guidance and standardisation of internal controls to organisations, associated

with risk management and the prevention of fraudulent activities (Power, 2007). Finally, another self-regulating, meta-organisation, widely associate with the definition and understanding of operational risks, is the Basel Committee on Banking Supervision. Overlooking the banking industry, the Basel Committee has devised the Basel (former Basel I, current Basel II and future Basel III) Accord, regulating the management of risks, especially operational risks, and overseeing the risk management process in banks (Wahlstrom, 2009). To extend the picture, various organisational networks around the world are working together with the aforementioned organisations and form a network of self-regulating organisations associated with devising various risk management framework following the principles of ERM. To name a few, the OECD, the World Bank, together with national and international standard setters, academics and practitioners work together with organisations like COSO, FRC, FSA and the Basel Committee to form the "global" risk management actors of a standardised risk management environment in organisations (Power, 2007, p. 97). These networks of risk agents have, and are not limited to, specific areas that act upon.

The areas that self-regulating meta-organisations are responsible for are associated with a holistic approach to risk and uncertainty management and an evolutionary approach to risk management process though organisational learning (Palermo, 2014). First, these bodies are associated with scrutinising and overlooking the risk management especially that of internal control environment of organisations, thus playing the role of the risk management auditor of organisational processes. Throughout this process of analysing the auditable internal controls of organisations, weaknesses are spotted (Power, 2007; Sarens & Christopher, 2010). Those weaknesses have to do with failures in the internal controls or limitations to the risk appetite of the organisation. This process aims that devising new approaches to risks management and offering an evolution of risk management processes through a better use of risk information and internal controls. Following that, self-regulating organisations play a key role in guiding and inspiring organisational risks management through the development and modification of various frameworks, such as the ERM. Finally, these organisations are mediators of stakeholder engagement as they are responsible for advising and understanding the risks the latter expect organisations to handle (Andersen, 2016). To conclude, the aforementioned risk management processes, the realisation of risks in organisations and the new regulation and self-regulation networks built to ensure risk management enhancement and accountability form the reality of

managing uncertainty in contemporary organisations. Crucial to that reality is the use and development of information systems to share and communicate risk and uncertainty.

2.3 Risk management: a brief background

To accommodate all the recent organisational changes towards risk and uncertainty, organisations are relying on procedures that will help them make sense of their risk environment. As such, risk management is defined as the identification, assessment and monitoring of risks within the organization and its members, with an aim at not only managing and mitigating them but also being responsible for them when they occur (Power et al., 2013). Another definition in the management accounting world is that of CIMA (Woods, 2010, p. 3) that state that risk management is "the process of understanding and managing risks that the entity is inevitably subject to in attempting to achieve its corporate objectives". In the same definition "risk is not something to be managed away", but "…something to be understood and harnessed in pursuit of a clear goal: sustainable performance". Taken into organizational terms, that is anything that can disrupt, or cause uncertainty about, the ability or an organization to meet its strategic, tactical and operational objectives (Andersen, 2016). Risk management includes all the processes that aim at mitigating the negative effect of identified risks, or to maximize the potential positive effect of risks, both in line with the relevant organizational objectives (Power, 2007; Andersen, 2016). In fact, risk is already so well associated with strategic objectives that risk management itself has been deemed, to a great extent, strategic (Andersen, 2016). However, the notion of risk in that definition of risk management is not only limited to risks, but also to uncertainty. Risk management includes the processes that aim at uncertainty management or, in other words, the recognition that there are existing threats to organisational objectives due to factors unknown to organizations. In such a case, the management of uncertainty has to do with all the processes that serve as precautions and information providers for the unknown risks. That category includes various information systems crucial to the identification of risks (Scheytt at al., 2006). Power (2007) argues that the multiplicity of risk embedded in organizations, the fact that the latter cannot be known to the full extend and the fact that risk embeddedness in organizations is an evolutionary process (risk process and risk embeddedness are still evolving), has classified risk management as the management of organizational uncertainty.

2.3.1 The role of internal control in managing risk and uncertainty

Central to the management of the risks mentioned above, is the role of internal control (Leitch, 2008). From the discussion so far, it is evident that contemporary organisations operate increasingly in a highly risky and uncertain world that requires their attention. Organisational risks are multiplying and the fact that it is difficult for organisations to grasp their full extend represents a form of uncertainty towards meeting their organisational objectives. Organisations also need to evolve and try to understand the full of extend of the risks they are facing in an effort to manage them (Power, 2004). This is where various information systems, focusing majorly on stakeholder engagement, play a crucial role in making sense of the unknown risks in order to be transformed into risks that can be managed (Scheytt et al., 2006). Finally, organisations need to develop a defensive stance towards failures from the uncertainty that derives from the fact that some risks will always be unknown. Such behaviour reflects a proactive and precautious attempt to manage organisational uncertainty. The most valuable weapon towards surviving in such environment is internal control systems, because they offer the most appropriate tools towards managing organisational risks (Power, 2007).

Internal control is defined as the management of a set of controls, with a financial and non-financial focus, that are established in organisations to provide security that their operations are as planned, their finance elements are in place and are working as intended, and that the organisations complies with relevant laws and regulations (CIMA, 2005). According to this definition, internal control systems must focus on efficiency in the endeavour to produce accounting records that are more reliable and make the existence or emergence of fraudulent events less possible or more difficult (CIMA, 2005). Therefore, internal control systems are the amalgamation of standardized procedures that aim at ensuring efficiency of operations, law compliance and provision of relevant data that depict the situation on such cases. Internal control has become the main source of risk handling in contemporary organisations and is often replacing or equally representing the attempt to manage organisational risks reflecting the notion of organised uncertainty (Power, 1999, 2007). Such a representation is not arbitrary. In responding to the management of the organised uncertainty, organisations, as mentioned before, paid attention to various risks. Moreover, the management of those risks is made in light of the need for stakeholder engagement and meeting their expectations towards risk handling. That is also reflected into the transparency of risk management processes that aims

at analysing and standardising the risk management process of organisations. In adapting to those demands, internal controls are suitable for many reasons.

The first response to the management of an organised uncertainty comes from the fact that internal controls offer the necessary transparency and auditability of organisational processes towards higher risk handling effectiveness (Leitch, 2008). Internal control systems represent standardised procedures that are easily traced for deficiencies and risk-related capabilities. Moreover, the data generated by such internal processes represent evidence of the risk management performance of the organisation (Beasley & Frigo, 2007). Through that evidence, internal control also serves as a blueprint that promotes organisational learning in the endeavour to increase risk-handling agendas (Power, 2004c). Through internal controls, organisations have also made it easier to follow their compliance and opportunity-seeking endeavours that need to attend to. More specifically, internal controls ensure compliance with laws and regulations, through rule and routines, and provide all the necessary information that can be used for exploiting new opportunities (Spira & Page, 2003). Such requirements are crucial into meeting organisational objectives and strengthen the usefulness of internal controls. Another reason for the usefulness of internal controls is the fact that they can impose self-assurance and monitoring of the risks of the organisation as well as provide the necessary information about the quality standards of the risk management procedures in place (Power, 2004c). Finally, internal controls represent the core of the new governance that was developed by organisations towards contemporary risk handling. However, more details on this topic will be discussed in a subsequent section.

Similar to risk objects, internal controls are also affected by the risks the organisations are exposed serving as boundary objects (Power, 2007; Mikes, 2011). For instance, internal controls offer valuable support into managing operational risks. Indeed, they are responsible for delimitating the acceptable behaviour of organisational members, trace dysfunctional operations and signal for the emergence of problems. They also offer the standardised procedures that promote a culture of refraining from behaviours that can cause operational failures. Moreover, when reputational and legal risks are concerned, internal controls offer the necessary procedures that ensure compliance with laws and regulations as well as improve the organisational functions that can cause reputational damages (Power, 2007). Finally, by delineating the standardised procedures of managing organisational risks, internal controls also

offer the necessary precautionary tools to deal with uncertainty (Power, 2007). The consideration of and expanded agenda of risk and uncertainty to be handled through the extensive use of internal controls has a specific aim for organisations: being responsible and exude accountability that they can manage their risks, be prepared for uncertainty shocks and legitimise themselves in the eyes of society.

2.3.2 Organised uncertainty: the role of information systems

The role of information systems in contemporary risks management is central to managing risks, and within internal control systems. Organisational risks, with an intensive attention to managing an organised uncertainty, lie in the capacity of organisations to learn. In order to be held responsible and accountable for managing their risks and being defensive against uncertainty, organisations need to be flexible in developing the capacity for learning (Power, 2007). Such learning has to do with understanding organisational risks, making sense of the full risks the organisation is being exposed to, improve internal control and enhancing the risk appetite. That way, organisations enhance their competence and capacity towards practice, evolution and objective attainment through surviving in an uncertain world of accountability. Central to such endeavour is the implementation, development and maintenance of information systems that can communicate and share known risks and uncertainties to be managed (Scheytt et al., 2006; Power, 2007).

First, information systems in the form of information sharing enhance the risks appetite of organisations (Andersen, 2016). Through engaging with practitioners, following historical data, meeting with regulators and engaging in discussion about risks with various societal actors, organisations can expand their risks appetite (Power, 2004c). Through that expansion, organisations can better understand their risks, enhance their management approaches to mitigating and exploiting them and follow, as much as possible, a holistic approach to risk-handling (Scheytt et al., 2006). When information systems are used this way, various risks are communicated throughout the organisation, information is also shared on unknown events that can cause harm to the organisational objectives and new risk objects emerge to be managed (Power, 2007). Speaking of stakeholder engagement, information systems are also useful in sharing the descriptions of risks that an organisation needs to adhere to reflecting society's demands (Power, 2007). Following various physical and digital channels, stakeholders can

engage in a dialogue with the organisation to inform it about risks they are expecting the organisation to care about (Andersen, 2016). Furthermore, information systems aid in the request for transparency of risk management and internal control operations by sharing the reality of the latter and making them transparent to the public and various regulatory and professional bodies. That way public scrutiny is enhanced, and information systems aid in holding organisations accountable. This external use of information systems is complemented by their use inside organisations when it comes to risks management. For instance, information sharing occurs when organisations are assessing the quality and adequacy of their internal controls in managing risks (Power, 2007). In such a case, organisation can spot weaknesses or provide assurance of the standardised use of internal controls. Through spotting weaknesses, organisations can improve their internal control process and evolve their risk management procedure to reflect a better implementation of procedures. Being present in most risk management functions; information and communication systems are evidently at the heart of managing organised uncertainty in contemporary organisations.

2.3.3 The integrated Enterprise Risk Management (EMR) framework

In the middle 2000s, following the years of the risk understanding in organisations, organisational efforts towards managing risk and uncertainty occupied the need to adopt an approach to risk management that would be all-inclusive to managing risks (Arena et al., 2017). With the introduction of new risk categories and the expanded attention to risk agendas, it was difficult for organisations to cope with changes. For instance, the rise and expansion of operational and reputational risks posed a difficulty when it came to identify them (Power, 2007). Moreover, the complexity of the process of the new form of internal control was challenging as the multi-dimensional nature of risk was making process alignment difficult (Power, 2004c; Power, 2007). Regulators and professional bodies with a risk management overseeing character realised this challenge and started guiding organisational practice. However, most frameworks up until that point in time were compartmentalised to a few areas of risk management attention (Power, 2007). It was the Committee of Sponsoring Organisations of the Tredway Commission that, in 2004, developed and established a risk management framework that would guide an all-inclusive approach to the management of uncertainty. That framework was coined the Enterprise Risk Management Framework (ERM) (COSO, 2004). Throughout the years, the framework attracted a lot of attention from

organisations, developed and, despite its criticisms (See Power, 2009 and Arena et al., 2017), it is still the most influential framework that guides the practice of organisational risk management (Power, 2007).

The ERM framework was initially proposed as a standardised and integrated practice to risk management in organisations (Hayne & Free, 2014; Arena et al., 2017). According to COSO, ERM is defined as "a process, affected 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 managed risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives" (2004, p. 2). That definition expands to a multifaceted approach to risk and uncertainty management. Central to that framework lies the role of internal controls as these are seen as a standardised and practical utilisation of internal controls in an effort to manage uncertain and risky events and ensure auditability and scrutiny of risk management operations (Paape & Speklé, 2012). Of particular attention is the guidance on the identification of operational and reputational risks, a challenge faced by many organisations. Crucial for that idea, the framework emphasizes the necessity to implement various information sharing systems that serve as tools for identifying, with the aid from internal controls, various risks that are important to the risk appetite of the organisation (Arena et al., 2017). However, information systems utilisation does not end there. As the framework proposes, these systems can provide data for risk management weaknesses, expand organisational learning on the application of internal controls and serve as a crucial tool for the evolutionary process to an expanded approach to risk management (Power, 2007). Hence, ERM is a framework that offers guidance for the various tools and processes that organisations need to adhere to, especially in practical terms, to cope with a better approach to managing their risks, develop defensive mechanisms towards uncertainty and enhance their organisational learning and decision-making when it comes to risks and risk management (Meidell & Kaarbøe, 2017). ERM is a proposed blueprint for practice that has been adopted by many organisations (Weitzner & Darroch, 2010)). However, adoption does not follow the same pattern in all organisations (Power, 2007). Indeed, compartments of the ERM practice are adopted according to the needs of any particular organisation (Arena et al., 2010).

To further understand their risk management activities, as advised by ERM, organisations can follow the step-by step process of adherence to eight distinct and connected "managerial

objects" (Power, 2007, p. 77). First, organisations should look at their internal environment and make sense of the fundamentals of both their internal controls and the risk environment they operate within. Second, after understanding their competence in such environment, organisational objectives need to be negotiated and set, majorly following a top-down approach (Power, 2007). From managers to lower-level employees, organisational goals need to be understood in the context of the responsibility of each organisational member. Third, once objectives are set, what follows is the identification of events that have an impact on those objectives (Power, 2007). This step constitutes all information sharing and communication procedures of identifying risks, either already known or hard to understand and assess. What follows as the fourth step is assessing the impact of those risks through various techniques. On the one hand, quantitative techniques can be utilised for easily quantifiable risks while, on the other hand, discussion and information sharing can be utilised for harder to define intangible risks. The whole process leads to the most crucial part of the risk management process which has to do with the formation of the risk appetite of the organisation with particular reference to the ways risks are going to be mitigated, or exploited when possible, and the defences built to tackle uncertain events. That forms the "risk response" of the organisation (Power, 2007, p. 77). Once the risk response is established, various controls are utilised or existing ones are remodified to exclusively adhere to such response. Hence, the next step has to do with devising, where necessary, risk internal controls that aim at mitigating organisational risks, handling uncertainty and promoting organisational risk learning. This step concludes the formation of the fundamentals of the ERM practice. What is left to complete the puzzle is what follows after the establishment of the risk management agenda. That is the formation and utilisation of various information and monitoring tools. Information sharing, and communication channels are important in devising organisational learning and response to new identified risk, especially those ones negotiated with society. In a blur connection with information systems lie the monitoring systems that are sets utilised for quality assurance of all the above operations for an optimal understanding of the risks the organisation is exposed to. These eight managerial objects, once followed in sequence, inform the way ERM works and its proposed risk management practical underpinnings. ERM is but a voluntary and popular framework that has been accepted as the most appropriate answer to the need for a new approach to risk management (Power, 2007). However, it has been evident that it is still in its infancy and lacks fundamental conceptualizations.

Despite the early efforts to mitigate risks in organisations, the corporate failures of the early 2000s (see Enron and Parmalat), which intensified the financial crisis of 2008, showed that any effort to handle uncertainty is still premature. A lot of improvements are necessary to make risk management relevant to a continuous emergence of negative events, as reflected to the practice of ERM. Following Power's (2009) seminal work, the particular risk framework has failed for several, well connected with each other, reasons. This failure also has to do with the inconsistencies of the risk management framework itself and its implementation, rather than the people who manage it. Organizations utilising the Enterprise Risk Management framework have been the proprietors of corporate failures because of the restrictive, and inconsistent with society's expectations, manner of the framework's practice. Indeed, the framework is limited because it focuses on delineating a very restrictive risk appetite for organizations limited to the scope of financial and capital terms. That way, other intangible risks as well as the risk that emerge from organizational members' behaviours are neglected and Power (2009) argues that this is the reason behind various failures in the 2000's. In that way, an important player in the game of accountability through risk management is neglected: society. Through the identification of financial risks, the assignment of risk management to specific gurus within the organization and the legitimacy nature of Enterprise Risk Management practices, society has been neglected. Furthermore, organizational behaviour as a risk object has been overlooked, risk identifiers from all levels of the organizations have been silenced and risk management in that way has lost its relevance (Power, 2009). Despite the shortcomings of the framework, the author does not argue against its use but rather for its improvement to incorporate a wider picture of risks to be managed as well as a less restrictive nature of its terms. The framework needed to incorporate various voices that can identify organizational risks, worked on them to be responsible to societal expectations and broadened the imposed risk appetite of organizations to include a wider variety of risks to be managed (Power, 2009). Another reason for this incomplete adherence to organizational external environments comes from the organizations themselves. In particular, evidence has shown that organizations not only might implement the framework just to gain legitimacy (Arena et al., 2010), in addition to their pre-existent risk management practices, but also, they might feel it is irrelevant to them after the implementation because their risk practice tools were already regarded as sufficient. Another factor that affects the failure of Enterprise Risk Management adoption is the context within which it operates (Mikes, 2009). That brings forth the various way that organizations adopt,

utilise and bring forth Enterprise Risk Management to build the concise and complete picture of their organization's risk management approach. A detailed analysis of the failure underpinnings of ERM is out of the scope of this thesis. However, by this brief analysis, it is evident that the ERM and organisations in general, have still a lot to learn and change in order to incorporate a world where risks are mitigated, and defences are built towards less corporate failures.

The ERM framework of risk management practice entails a detailed approach to managing risks, building defences against uncertainty and providing guidance of how to ensure accountability and organisational learning towards better risk management. Despite its criticism, it is still a widely accepted, adopted and utilised set of risk management principles that are useful for mitigating and exploiting the vast organisational risks included in their risk appetites. With the emergence and establishment of the ERM framework, organisations have shifted their focus on a more strategic approach to managing risks, as it is evident from the ERM definition itself. Indeed, while managing organizational risks, organizations develop a set of strategies that aim at translating the organization's risk management into activities of identifying, assessing and monitoring the risks of the organization. These activities form a set of risk related strategies that the organization has in place to mitigate the negative effects of risks and identify new opportunities in terms of its risk appetite (Andersen, 2016). However, in order to ensure sustainability and attainment of organizational objectives, organizations need to adapt and change, if necessary, their risk strategies in line with the environment within which they operate. That is, in the identification of new risks or in the inclusion of a more integrated risk appetite, organizations need to adapt their risk strategies to incorporate the emergent risks. To ensure that the proper risk related strategies are in place and to adapt to the new risk strategy requirements, organizations utilise various sets of management controls. These management controls are also associated with the improved risk strategies and the way they are executed to adapt to the new business environment demands of the organization (Andersen, 2016).

2.4 Managing risk in context: public sector risk management and control

2.4.1 Setting the context

One sector that has been significantly affected by the advancements in risk management is the public sector (Bracci et al., 2022). Following the contemporary risk agenda described in section 2.3, public service failures in the public sector context (see Andreeva et al., 2014) have triggered external and regulatory pressures to devise risk management agendas to exude accountability and control as an answer to the rising demands for public accountability in the provision of public services. That, together with significant financial constraints for public sector entities (Louth & Boden, 2014; Palermo, 2014), demands for an increased value for money approach to the provision of public services (Rika & Jacobs, 2019) and an increase in the provision of public service by a mix of public, private and third sector organisation (Fischbacher-Smith & Fischbacher-Smith, 2014) have led to a new era of managing risks in the public sector: an approach to a "new" generic approach to risk management (Hood & Miller, 2009, p. 3), or as it has been termed, new risk management (Palermo, 2014; Carlsson-Wall et al., 2019). Preliminary traces of the term lead back to the late 1990s (Fone & Young, 2000; Collier, 2009; Woods, 2009), however, the agenda has attracted more scholarly research attention recently (Palermo, 2014; Carlsson-Wall et al., 2019). This form of risk management replies to the need for accountability and control for public risk in two ways. First, new risk management is associated with an abstracted and formalised adoption of risk management tools that aim at solving the issues of accountability and control, proliferated by regulatory pressures, and eventually enhance risk management for public sector organisations. This conveys the logics of New Public Management (NPM) to borrow tools from the private sector to organise risk management procedures (Lapsley, 2009). To further define the term in the context of PSO and in relation to contemporary risk management, risk accountability in the provision of public services by public sector institutions refers to the obligation of public officials and organizations to identify, assess, manage, and transparently report risks associated with their operations, ensuring responsible use of public resources and maintaining public trust. This concept underscores the responsibility of public sector entities to not only achieve desired outcomes but also to do so through processes that are ethical, transparent, and aligned with established standards (Bracci et al., 2021). In their review, the authors highlight that risk management in the public sector has gained significant attention as a means to enhance

accountability and performance. They note that integrating risk management practices into public administration contributes to better decision-making and service delivery. Furthermore, emphasis is placed in formal risk management frameworks as accountability tools in public sector organizations. These frameworks enable public institutions to disclose risk-related information, thereby extending accountability to external stakeholders and enhancing transparency (Palermo, 2014). Hence, risk accountability in public services involves a comprehensive approach where public sector institutions are answerable for both their actions and their associated risks. This encompasses the implementation of formal risk management frameworks, transparent reporting practices, and a commitment to ethical standards, all aimed at safeguarding public interest and enhancing trust in public administration.This risk accountability is connected, or integrated, with management control systems, that play a fundamental role in ensuring risk accountability in public sector institutions by establishing structured frameworks for decision-making, performance evaluation, and resource allocation. These systems encompass formal and informal mechanisms, such as budgeting, strategic planning, internal audits, and performance measurement, which collectively reinforce transparency, efficiency, and responsibility in risk management. Their integration strengthens an organization's resilience, ensuring that public institutions can effectively anticipate, mitigate, and respond to uncertainties while maintaining service delivery and fiscal discipline (Hiebl (2024). In fact, as the public sector faces unique challenges, including political pressures, regulatory complexities, and budget constraints, the need for effective risk accountability even more pressing. Management control systems, in turn, provide a structured approach to aligning organizational objectives with risk management practices, ensuring that risks are not only identified but also systematically addressed. As noted by recent research, the convergence of performance management and risk management within management control frameworks enhances decision-making by linking risk exposure with key performance indicators, thereby fostering a proactive rather than reactive approach to governance (Bracci et al., 2024). This is in line with the objective of contemporary risk management, that is the management of uncertainty which PSO are majorly exposed to (Power, 2007). Furthermore, strong internal control mechanisms embedded within control systems play a crucial role in further reinforcing accountability. Internal audits, compliance checks, and continuous monitoring of financial and operational risks help public sector organizations maintain ethical standards and prevent fraud, mismanagement, or inefficiencies. As a matter of fact, literature

has suggested that well-developed internal control systems significantly contribute to strengthening risk management by ensuring that accountability measures are embedded into daily operations (Rabaiah et al., 2021). Ultimately, MCS serve as the backbone of risk accountability in public sector institutions, ensuring that governance structures are transparent, decision-making is informed by data-driven risk assessments, and public trust is upheld. Through the integration of risk management into control systems, public sector institutions can enhance their adaptability to emergent risks while ensuring compliance with regulatory requirements and ethical standards.

As a consequence of the above, new risk management in the public sector follows an integrated and holistic approach to risk management (Mahama et al., 2020). This means a shared corporate adoption and execution of risk practices, as guided by top-down approaches to implementation and definition of risks (Palermo, 2014). Central to that effort is the presence of key risk champions (usually risk officials) that are responsible for the diffusion/operationalisation of and guidance for the risk management procedures throughout the organisation, even though it has been evidenced that they take the blame for inefficiencies on many occasions (Power, 2007). Therefore, new risk management in the public sector context is the holistic adoption and operationalisation of formal, majorly top-down infused, risk management practices that aim at providing public sector entities with the tools to exude accountability and control for the risks they are exposed to.

Although much debate has been had around the term risk (Power, 2007), public sector entities are largely associated with the management of public risks (Andreeva et al., 2014), that is reflected in what Power et al. (2009) have defined as Late Modernity. In that era, risk "refers to risk that cannot be known – to unquantifiable uncertainties (Gephart et al., 2009, p. 141). That identifies the notion of risk as more related to uncertain events than quantifiable, known, and manageable risks. That applies well to the public sector, as a public sector entity specifically is exposed to a wide variety of risks that cannot be known and uncertainties that cannot be quantified (Gephart et al., 2009). Compared to the private sector, for example, public sector entities are not basing their risk agenda on quantifiable risk and their exposure to uncertain events is higher, and more impactful, leading to issues with reputation loss and majorly, reputational risk management (Power et al., 2009). For that matter, evidence has shown that, largely associated with the adoption of contemporary formal risk management

systems, risk is part of a wider uncertainty for public sector organisations (Vinnari & Skærbæk, 2014) and that is what the notion of public risk entails. To define the term, public risks are "those risks that may affect any part of society and for which government is expected to respond" (RRAC, 2009, p. 3). However, as it has been evidenced in the literature, the government is only the major facilitator of understanding and managing these risks (Andreeva et al., 2014). Although these authors only tried to establish the theoretical foundations of the matter, they articulated risk as something that is shaped and realised, and eventually managed, through the interaction of a network of public sector entities and groups (or individual) stakeholders, that bear risk, with the main (central) government entities assuming the final responsibility load. For that matter, a key risk that plays a central role to public risk is reputational risk. These kinds of risks are very prevalent in contemporary public sector organisations and are defined as "a purely human-made product of social interaction and communication" (Power et al., 2009, p. 301-302). They derive from an expectation gap between the public and the public service provider (Fombrun et al., 2000; Rika & Jacobs, 2019) and have negative consequences for public services providers as, in the event of a failure being uncovered in any matter of public service, damaged reputation and embarrassment follows. That can lead to blame-shifting, especially from politicians in their agendas, and more negative consequences as the public might follow a perception of different magnitude for the public service provider, or other constituents for that matter, influenced, for example, by the media (Rika & Jacobs, 2019). In other words, the public sector is exposed to a wide array of risks, the majority of which reflect uncertainty and is characterised by a challenging multiplicity in the establishment of risk that needs to be managed. Subsequently, due to the nature of this risk agenda, it has been evidenced that public sector entities have expanded their networks with private organisations, to form public-private partnerships (PPP), in an effort to transfer their risks to the private sector (Demirag et al., 2012). Despite evidence that this can create adverse effects with risk being transferred back to public sector entities (Demirag et al., 2012), the formation of PPP is central to the established era of new formalised risk management in the public sector. For instance, this has been evidenced in the case of the Australian federal police, where a collective approach was established between the police and their supporting PPP entities, to form a formalised risk management inter-organisational approach, with collective practices (Lacey et al., 2012). The purpose of that effort was to mitigate the reputational risks of the justice system as a whole, and engage in cross-agency practices, for example the

reporting of performance (positive) as part of the wider system and not per individual organisation. To summarise, the public sector is framing and managing a complex and multifaceted array of risks, as part of a network, and the most prevalent solution to doing so, as part of a wide network of agencies and stakeholders, is through a formalised approach to risk management practices in a top-down fashion.

Literature on the matter, however, disagrees with the sole reliance on this formalised agenda. There is evidence, although limited, to the presence of bottom-up and informal systems that convey important information and play a vital part in managing risks in the public sector (see Sceytt et al., 2006; Fischbacher-Smith & Fischbacher-Smith, 2014) and a good number of researchers that discuss the content-dependency of the adoption of risk management frameworks and how these frameworks actually work, in an informal manner (Carlsson-Wall et al. 2014), in public sector organisations. Indeed, the way risk management is adopted, implemented, facilitated and practiced in various public sector entities around the world varies with context, external environment, regulatory oversight, expertise and political factors for each public sector organisation, and expectation on reaping the benefits from the adoption (Woods, 2009, 2010; Rocher, 2011; Collier & Woods, 2012; Palermo, 2014). For example, Carlsson-Wall et al., (2019) provided evidence of the creation of vernacular risk management systems that, following the new shift in focus for risk management, were designed and operationalised for local department needs, despite the provision of a different risk management element in the organisations they studied. That is, local managers devised their own systems, one of which was later accepted as part of the formal risk management agenda of the organisation. Furthermore, information-sharing regimes, although not fully utilised by the public sector yet (Fischbacher-Smith & Fischbacher-Smith, 2014) serve as the sharing of risks that an organisation might not be aware of. With reference to crisis management, the authors point out the presence, and importance, of informal, and sometimes noticed or unnoticed, networks of information sharing within the public sector that have the potential, although not yet known how, to carry important information for avoiding crises, and by extension, uncertainties. These information systems are present in both private and public sector organisations, and they aim to facilitate internal exchange of information, relevant to the identification of risks (Sceytt et al., 2006), but that is the only evidence the literature has so far, that is, their presence. In other words, despite the prevalence of the new risk management

agenda, and despite public sector organisations adopting and operationalising risk management agendas that fit them, there is an interplay of formal and informal procedures of managing risks. Despite the hierarchical approach to facilitation and decision-making in risk management, informal processes, especially informal information-sharing avenues, exist in these organisations, despite literature not being fully aware of their effects. These procedures are part of the wider umbrella, central to the effort of managing contemporary public risks for new risk management in the public sector. That is the procedures in place aiding in the effort to control for those risks (Collier & Woods, 2011; Rocher, 2011).

2.4.2 Management Control for public risks: ERM and the centrality of PMS.

In the public sector, one framework that is prevalent, although not completely adopted to its fullest and by many public sector entities, is the Enterprise Risk Management framework developed by COSO in 2004 (Rana, Wickramasinghe & Bracci, 2019). This framework, despite its applicability to the private sector, has been found to be difficult to be transferred to the public sector. Compared to the private sector, the public sector is more exposed to complex, uncertain and unknown situations (Andersen & Young, 2023). The public sector aims at addressing a wider array of socio-economic and socio-political events that have to do with situations of financial crises, natural disasters and climate change. As a result, PSO need to manage the provision of services that adhere to the public concern that these events reflect on. Hence, these events, that represent a higher-level exposure to uncertainty, require more mechanisms to provide services that reduce these concerns for the public good, rather than offer risk mitigation and insurance (Kim et al., 2021). That does not align with the ERM practices that derive from the private sector. The very notion of risk management that ERM tries to convey, is not applicable directly and unequivocally to a context that is mainly characterised by uncertainty and the challenging management of the exposure to a wide range of events with uncertain public effect. That is because, this level of uncertainty the PSO faces, cannot be captured by the instructions the ERM framework adopts, which rely on a more measurable element of risk. As the authors suggest “from both political and economic perspectives, the nature of public sector exposures provides a rather distinct risk management context that is categorically different from private enterprise concerns” (Andersen & Young, 2023, p. 2). In that context, political, moral and economic directions need to be considered when managing the risk of public sector exposures. Moreover, the provision of public services

is structured in a way that decentralised, self-operating units offer specific specialised public services, and these units have low levels of co-ordination with each other (Mahama et al., 2022). That, in turn, can hinder one of the main objectives of ERM, which is an enterprise-wide, holistic approach to risk management. At the same time, due to the focus of the provision of public services, which tend to be aiming at cost reduction and effectiveness and efficiency of public service provision, ERM is seen in two ways. One through the lens of reducing costs to the provision and safeguarding of public services. The second way is that ERM is seen, majorly, as a regulatory and compliance box-ticking exercise to reduce public service failure. Therefore, for PSO, ERM is seen as a costly exercise, that requires a level of compliance, and that is what PSO is characterised by (Andersen & Young, 2023). These two approaches hinder the creation of an enterprise-wide risk awareness culture, and a focus on adopting risk management strategies that have a long-term strategic orientation for the provision of public services, which are important elements in the adoption and effectiveness of ERM systems (Capaldo et al., 2018). For these reasons, the ERM framework is not applicable the same way to the public sector, as compared to the private sector, and the enterprise-wide framework is seen as to be adopted in either an incomplete, situational to the relevant context and PSO entity needs, or in a regulatory-compliance fashion (Rana et al., 2019).Irrespective of the challenges, the ERM guiding framework, both for the private and the public sector, has one characteristic in common, that is the significant importance it gives in one of its core elements: controlling for risk. The connection of risk management and management control is not new but explored only partly in the two distinct streams of literature (Bhimani, 2009, Soin et al., 2013; Bracci et al., 2022). Indeed, the risk management literature has identified the connection between the two concepts and has already provided evidence for a big part of these risk management processes and their connection with strategic risk management within organizations. What links the notions of risk management and management control, is their association with the strategic domain of the organization (Mikes, 2009; Arena et al., 2010; Arjaliès & Mundy, 2013). Notably, risk management processes, are important for organisations in reaching their organisational objectives (Binder, 2007; Tessier & Otley, 2012). However, especially in the public sector, the process of this relationship is majorly unexplored. That is because, these two notions are integrated as in risk management influences and is influenced by control tools (Bracci et al., 2022). However, little is known what processes are behind this integration in practice (Rana et al., 2019; Bracci et al., 2021; 2022).

Following the aforementioned definition of risk management, the management control literature identifies risk management as "a process that aims to improve the chances that objectives are achieved, that damaging things are less likely to happen and that beneficial outcomes are more likely to be achieved" (Soin et al., 2014, p. 182). To further support this argument, the Enterprise Risk Management, clearly offers more evidence of the connection of risk management and management control. According to COSO (2004):

> *"Enterprise Risk Management is a process, affected 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 risks to be within its risk appetite, to provide reasonable assurance regarding the achievements of the entity's objectives".*

That definition can be further translated into the identification of events or activities that are, either in or out of control of the organization, associated with affecting an organization's strategies, either positively or negatively, and can affect, in a similar manner, its objectives. Therefore, there is an evident connection, in that regard, with the function of management control. Management control is "the process by which managers assure that resources are obtained and used effectively in the accomplishment of the organization's objectives (Anthony, 1965, p. 17). However, this conceptualisation was criticised as it neglected operational controls, marginalised the concept of strategic planning and did not pay attention to non-financial factors affecting organisational performance (Otley, 1999). Such an approach is inadequate in understanding management control in contemporary organisations embedded in a dynamic environment (Otley, 1999). Therefore, following a more complete approach, management control has to do with directing organizational behaviour and effort towards implementing, monitoring and modifying, where necessary, the strategic agenda of the organization to adhere to the organizational goals, with reference to the external environment within which it operates (Simons, 1995; Merchant & Van der Stede, 2012). Moreover, management control systems are designed to provide useful and relevant information for "decision-making, planning and evaluation" of the business and its core activities (Merchant & Otley, 2006 in Widener, 2007, p. 757). The current study sticks with that term and does not adhere to the definition of controls as a package (Malmi & Brown, 2008). The reason behind this choice is that Malmi and Brown (2008) define controls designed outside the space of decision-making, whereas the central

agenda behind contemporary risk management is the notion of decision-making under risk and uncertainty, especially when it comes to public sector organisations (Woods, 2010; Louth & Boden, 2014; PWC, 2015; Rana, Hoque & Jacobs, 2019). Conclusively, and reflecting to the analysis above, it is evident that both notions are associated with the identification of flaws into strategies and their maintenance to adhere to the general and specific organisational objectives.

To further provide insights on the integration of management control in managing public sector risk, literature in both areas, has offered a significant number of examples of that integration. For instance, Collier & Woods (2011), studied the adoption of different risk management tools when comparing PSO risk management, between Australia and the UK. Through a comparative case study approach, they interviewed and observed members of local authorities in both countries of interest, and they also analysed publicly available information and archives, to show the contingencies in risk management practice in these two contexts. In that effort, they also provided examples of management control tools that are associated with managing risk in their case studies, while showing that these vary within these different contexts. However, even though they pointed out how important is management control in managing PSO risk, and despite some examples of control tools that are utilised in this process, the authors did not go any further in exploring any process consideration of these controls and how they work or how they are associated with risk management practices. The only pointed out their importance, and they suggested that, similar to risk management practices, risk management associated controls will also vary between different contexts. Similar evidence was also provided by Rocher (2011), via a case study of the adoption of a new risk management tool, in a local urban community organisation in France. The aim of this particular case study was to explore the adoption of a new risk management tool and show its implementation and how this was perceived by the organisational members. A combination of interviews with organisational members and local politicians, observations during and after the implementation phase, and analysis of various relevant documents, revealed that the new risk management tool, at an initial phase, was implemented to cover the needs of the organisation under study. In fact, the tool, which was initially devised from the local government, ended up being implemented in a different way than intended, to cover the needs of the local authority. The new risk management tool served as control tool in the end, to manage relationships with different external stakeholders. However, the authors, mainly due to the focus of the study, offered no further

information on how the tool worked and what its role was as a management control mechanism in supporting the risk management process of the organisation.

Furthermore, risk management literature has also focused on the centrality that Performance Management Systems (PMS) play in managing public risk (Cuganesan et al., 2014). That reflects Power's (2004, p. 13) suggestion that "the concept of risk is being enrolled in a new focus on outcomes and performance" in the public sector. Despite their design being substantially affected by external factors, politics and institutional powers, PMS contribute to mitigating known risks to the public sector, especially in the form of risk registers. They are also used to reap the benefits of risk management in the sector, as they are used as tools for mitigating risks to a certain level, which in turn serves for opportunity creation and manifestation for the organisation (Cuganesan et al., 2014). However, there are mixed views on the level of this integration, as there are barriers to it (Bracci et al., 2024). These barriers range from risk managers focusing on their area only, bureaucratic compliance-oriented cultures that disregard strategy connection with risk management, assignment of separate responsibilities of PMS and risk management, and a lack of a shared risk culture. However, other contexts might offer different results, as these were only evidenced in the Italian PSO (Bracci et al., 2024). Moreover, PMS do not come without their own risks. Externalities and various organisational inefficiencies and mindsets inherit risks to the PMS in the public sector and that requires them to be manageable and mitigated (Cuganesan et al., 2014). That is PMS are another set of risks that need to be managed by a public sector entity. Moreover, examples of how PMS is integrated in managing public sector risk have been provided (Woods, 2009; Woods, 2010; Rana, Hoque & Jacobs, 2019). For example, with a clearer focus on PMS for risk management, Rana, Hoque & Jacobs (2019) provide evidence of partial integration between risk management and control systems in the aftermath of a legislator reform affecting the Australian public sector. Evidence suggests that the reform imposes various forms of controls for risks that organisational members have to translate into daily practices. For instance, the act imposed a "risk culture", translated into risk processes and subsequent control systems in the organisations examined (Rana, et al., 2019, p. 40). This culture pertains to risk management through risk measurement, the inclusion of intangible risks through the analysis of non-financial information and the setting of objectives related to pre-determined risks. Utilising a multi-site case study design, the authors explore the effect of the Public Sector

Governance, Performance and Accountability Act 2013 (PGPA) on the PMS of the Australian public sector before and after the reform and show the implication of this legislation. To set the scene, the reform focuses on accountability, strategic decision-making and accountability for performance measurement for Australian public sector entities and has implications for risk management in this context and, by extension, to the controls utilised. Through a mix of data from 103 semi-structured interviews with participants from 34 government organisations at various hierarchical levels (CEOs, operational managers and members of an external public audit committee relevant to the sector), archival documentation analysis from government websites and a focus group with 22 representatives of each research site, the authors offer valuable examples of controls that the new regulation imposed. To elaborate, despite the lack of in-depth analysis of the controls used, it was clear in the study that the reforms imposed a more sophisticated performance management system for risk management in the sites under study, with an aim at identifying and mitigating significant material threats. But the processes of this sophisticated tool were not elaborated upon. Furthermore, this new regulation had implications for accountability, because now the agents responsible for these threats had a responsibility to mitigate them in line of meeting organisational objectives (Rana, Hoque & Jacobs, 2019). This responsibility could be evident when each agent or area of responsibility, as per the PGPA 2013 requirements, had a performance measurement apparatus for risk measurement in assessing government services. To that end, the organisations under study met the requirements, with some deviations. Being very vague for the risks fed into their systems, the organisations under study prioritised performance management for risk management and created risk management activities to exude a wider accountability for their organisations. As far as the MCS are concerned, the integration of MCS with issues of risk management was low. That is, the financially oriented practices and auditing of expenditure were the main control devices for performance risk management, while issues of integration, contextualisation, implementation and failure risk were largely overlooked by the organisations under study. The practice was heavily oriented towards compliance activities that were fed to the PMS and served as a performance tool. Moreover, these procedures were embedded into the risk culture of the majority of organisations under study showing that the reforms provided a new focus of risk performance mindset to the agents of the government (Rana, Hoque & Jacobs, 2019). This study is a prime example of the fact that new risk management practice and regulation imposes

control tools to organisations who adopt these, but it does not show the process by which these controls work.

Probably the most relevant study that actually offers a few more insights on the use of control tools in PSO risk management is that of Woods (2009, 2010), with a study of the Birmingham City Council, a public service providing organization in England. The focus of the study was to show the structure of the control system that was present in this organisation, and the contingency details that affected the elements of this control structure. That control system structure was imposed by the risk framework, which was imposed by external regulation (Woods, 2009). The purpose of the study was not to offer any insights on how control systems worked, but on the contingency factors that affected the use of controls imposed by risk management regulation. By utilising a case study of a single department agency, and its networks, offering services for culture media and sports, the author collected data through extended interviews (majorly with a few senior managers) and direct observation in meetings and training sessions. Through the study, it was evident that the organization had specific approaches to dealing with its imposed risks. First, the organization was departmentalized into services and their relevant managers were held responsible for the risk management and the risk handling of their consecutive service area. In terms of identifying risks, the paper illustrated that mechanisms were placed in each service, but the process by which this happened were absent apart from an example of communicating risks with relevant partners (other network councils). Indeed, risks were identified at the middle-level of management, and then the highest-ranking risks were communicated at the senior level management (Woods, 2010). Once risks were identified, in various areas and for various financial and non-financial elements, they were codified and were fed to the top-level management to agree on tolerance. Then this was sent to the departments and an activity plan for risk registers was formed, including the use of appropriate controls for these risks. Examples of risks that the council was targeting for were environmental, legal, political, financial, social, reputational, managerial, physical and technological risks associated with the provision of services (Woods, 2010). At this stage, the risk management framework informed the risk performance of the study, that set and targets for risk handling (Woods, 2009). Risks were classified in three categories: severe, material and tolerable, to indicate the extend of risk mitigation or opportunity seeking in every service area. Attention was given to the severe risks, which were treated more substantially in

order to deem them tolerable at least, through the use of tighter controls. These risks were then fed to the performance registers of the case study, they were reviewed annually through an end-of-year self-assessment, including underlying activities, and a reviewed risk management agenda was devised. Finally, lower levels managers, and some employees, were also called into the discussion and were given authority to use their own feedback systems to manage their risks in their area with an aim at decreasing the bureaucratic responsibility of risk expert reviewers within the organisations (Woods, 2010). Here, risk communication served as a way to induce acceptable action for managing risks. Moreover, serving as a method of feedback and feed-forward support on risk strategy and the attainment of organizational objectives, target risks were set to each service, their risk performance was constantly communicated with top level management and the internal audit committee, and appropriate actions (tighter controls or strategy modification) were implemented.

Following that, performance measurement in the Council was enhanced due to the monitoring of the risk management process from an external authoritative body, the Comprehensive Performance Assessment (CPA) (Woods, 2009). As external verifiers of the risk processes, they offered guidance on the controls used and assessed their effectiveness. In their agenda, higher performing organizations were assessed based on the inclusion of various members of the organization in the process. Then, in terms of risk handling, the same organizations were assessed based on their impact of services, which was a result of embedded risk management controls and handling of risks that resulted in higher quality service. Therefore, as part of an organizational contingency, the CPA review from the internal audit committee imposed an advanced performance measurement system for the council, because they needed to rate the CPA score as a risk target. Failing to achieve this risk target would mean lower score to the CPA and thus undervaluation. With the introduction of another risk indicator, the BVPI, risk-responsible service managers were monitoring the services and risk handling processes that would offer high or low scores and developed strategies to increase their risk handling performance. Again, this risk target was monitored through a performance evaluation system within each service. But the study did not explain the process of how this happened. In general, controls were used in a fashion to manage performance and see how targets were met and to analyse how well the organization handled its risks to attain its risk target within each service and attain their objective of higher quality service provision. In addition, the risk appetite was

broadened further through the introduction and the necessity of councils to form partnership with other similar councils and learn from their peers (in terms of risk, risk management and risk control). In that case, the communication with other partners was a control that was used in a learning-inducing fashion, to enhance risk knowledge, for identifying and managing risks. But details on how this worked, were not given.

Finally, in light of the pressure from regulation for best value rules for councils in England that pushed senior management and board of directors to embed and manage key strategic risks and develop formal risk management procedures (Woods, 2010), the author summarises her study's findings in relation to the risk management apparatus in the council and further points out the centrality of controls in that effort. Eventually, the council was found to address its risks at both group and directorate level, aiming at exuding external accountability and corporate assurances. Risk management over the years became fundamental to the council's ability to deliver it core services, as seen their agenda that was previously discussed. That offered substantial help in prioritising key risks (Woods, 2010). In that effort, internal audit procedures offered assurance on controls and crucial support in enhancing risk management and resulting in the council investing in dedicated risks systems to help risk registers being up to date and effective. Furthermore, in the case of partnerships, the final risk registers completed by the departments of the city council were used as guidance for pointing out the relevant risks of the partnership, assigning risk responsibilities to the partners, and, eventually, allocating risks to the relevant bodies under contract (Woods, 2010). To conclude, Woods studies offer insights on the effect of an imposed risk management framework to a public sector organisation, to the control tools specifically related to that framework. As such, it offers examples of the types of controls that were used to inform the main risk performance of each service in terms of their target risks and a learning approach was further utilised to re-arrange key strategic activities to manage these risks. The study, however, focused only on the risk management procedures that delineated these controls. As a result, this study further highlights the connection of management control and risk management in the case study. However, these two studies, in most cases, show the way the risk management procedures worked. The way controls interacted with the risk management tools, or affected the wider control agenda of the organisation were absent. Finally, insights were given for only part of the process of managing PSO risks, that is the monitoring and managing, and not the identification of emergent risks.

2.4.3 Summary of current research issues and research questions

For one thing, despite evidence of the integration of MCS to manage public risks in PSO (Collier & Woods, 2011; Rocher, 2011) and their facilitation towards managing a variety of risks, mainly because risk management practices are connected with meeting organizational objectives (Hood & Smith, 2013), literature to date, offers little to no evidence on how this works in practice (Bracci et al., 2022). As shown in the literature review above, there are studies that are clearly associated with providing evidence on the implementation of risk management procedures in the public sector and showing examples of a clear connection between management control and risk management. Many of the studies were associated with risk management reforms and the implications these had for controls, with a lot of indications on what these controls are, but without unravelling the processes of how these controls worked and how risk management affected them and vice versa. Thes integration levels were also contingent to various contexts. For that matter, literature to date has informed practice by showing how risk management is implemented and its effect on MCS, successful implementation drivers of risk management and limited evidence on the integration issues and processes (Bracci et al., 2022). The studies reviewed in the previous section, are only part of this literature, that has some examples of the control tools that are associated with risk management in the public sector. Despite these studies showing the importance and connection of management control processes for public sector risk management, they offer little to no evidence on the *processes* of the control systems that are utilised for managing public sector risks. That is important to understand best practice, issues of integration and further understand the integration itself, in terms of policy-making and managerial decision-making (Rana et al., 2019; Bracci et al., 2022). Understanding this practice, will offer avenues for better PMS, better strategy implementation and understanding of the design of control systems in PSO. For the latter, all the studies mentioned in the previous section indicated control tools that are either utilised or are imposed to certain PSO contexts. Despite the fact that these controls exist, the way they worked and contributed to managing risk in these contexts, is still unclear. Take for instance the notion of performance management. As discussed in the previous section, PMS play a central role in managing public sector risk, despite some mixed views on their level of integration (Rana, Hoque & Jacobs, 2019; Bracci et al., 2024). That was evidenced by the use of different PMS tools related to risk in most relevant studies articulated. However, PMS are

only part of the whole control system in public sector organisations, and literature has suggested that they are and must be associated with other controls or control systems (Cuganesan et al., 2014). At the same time, the PMS processes and procedures are still unclear as to how they are integrated with risk management, in the current literature. Indeed, more empirical evidence is required to understand how PMS work in PSO risk management, and how they contribute to the universal approach to risk management in the public sector, reflected in the use of an amalgamation of controls in that effort (Cuganesan et al., 2014). That points another issue in the literature, that it does not show how controls for risk management are connected with each other (Bracci et al., 2022). It is also articulated by Cuganesan et al. (2014) that, since PMS incorporate risks by themselves, studying the interconnectedness of these systems as a part of a wider control system, has a lot of potential to uncover practical considerations in the public sector. Especially to the PMS contribution to the wider control system in managing risk. This has implications for both for organisational strategy and risk management in the public sector, even though "public services are complex, and performance is multi-dimensional, making it difficult to measure performance in a quantitative fashion" in the public sector (Bouckaert & Balk, 1995; Smith, 1995 in Cuganesan et al., 2014, p. 281). PMS is prevalent in contemporary risk management of public sector entities in Late Modernity, and they play a key role as tool to manage and mitigate reputational risks (Power et al., 2009). However, it is still unclear how these systems work in practice and a case study would provide a good starting point to solve this issue in the literature (Cuganesan et al., 2014).

To summarise, the studies discussed in the previous section, as they reflect the most recent direction of risk management and management control research, do not show how these two notions are tied and are influencing each other in practice. Literature to date has identified their connection and had provided some evidence of control tools that are utilised in some contexts. However, literature has not clearly understood the processes and procedures associated with the interplay between risk management and management control in the public sector. This interplay has been clearly identified in the literature (Bracci et al., 2022). However, these authors argue that current literature on the matter requires more evidence, especially in the form of in-depth case studies from international contexts, to show how this interplay unravels in practice, since it is clearly understood that these two notions of controlling for risk management are well integrated in the case of public sector institutions. The same applies to

the private sector, but with different characteristics (see Collier & Berry, 2002; Mikes, 2009, 2011; Arena et al., 2010; Paape & Speklé, 2012; Arjaliès & Mundy, 2013; Jordan et al., 2013; Caldarelli et al., 2016). For the public sector, there is knowledge, as indicated in the previous section, that MCS play a central role in the management of risk in the provision of public services and public management (Rana, Wickramasinghe & Bracci, 2019). Following the influence of NPM, these authors also argue that MCS will exist differently in the case of public sector risk management, due to contextual contingencies, and differences in performance aspects and accountability agendas. As a result, MCS for risk management in PSO will and should have contextual practical implications, something that the authors argue could be unravelled through more research on the matter. Similar to Bracci et al. (2022), Rana, Wickramasinghe and Bracci (2019) also argue that controls for risk purposes will and should co-exist with other controls within a public sector organisation. However, they suggest that practice on how this is done is not evidenced in the literature (Rana et al., 2019). Here, co-existence means integration with current control systems, and not synergy of controls (Tuomela, 2005; Adler & Chen, 2011). Integration implies the incorporation of risk-oriented controls, to either existing control systems or the creation of clear risk-oriented controls that are part of wider control systems (Posch, 2022). Moreover, integration in PSO is connected with the notion of management control practices influencing risk management processes and vice versa (Bracci et al., 2022). For example, Posch (2022) identified evidence of risk integration in results controls (performance-oriented controls) that were clearly associated with risk performance.

Moreover, literature has suggested that management control systems not only co-exist with the risk management process in the public sector, but they are also influencing and are influenced by this process (Gong & Subramaniam, 2018). PMS also play a central role in this interplay. However, the practice via which this integration and influence (interplay) happens, and the processes and procedures that are associated with these, are not clear and literature lacks empirical evidence (Rana et al., 2019; Bracci et al., 2022), more so, when it comes to PMS and their role within the risk management and the wider control system for that matter (Cuganesan et al., 2012). Hence, this study aims at contributing to the current literature through providing empirical evidence on the processes of risk and risk management in the public sector, and how these are integrated into various controls and control systems to form a wider control

framework. Through empirical evidence, this study will show how risk management processes influence control tools and vice versa, in an international context. This will be done through a cases study, in answering literature calls (Bracci et al.,2002), and there will be a specific theoretical framework that will be utilised to enter the case study field, to unravel processes of risk management and management control integration. That way, not only empirical evidence will be provided on the matter, but a theoretical lens will be provided, as a basis to understand PSO risk management, something that is lacking from the current public sector risk management literature (Bracci et al., 2021).

Considering the interplay of management control for risk management, another important aspect of risk management needs particular attention here. As noted in the literature discussion in the previous section, talks around controls reflect the definitions of risk management as these are given in the introductory section (to remind, identification, assessment and monitoring of risks). With a limited scope on how management controls are used to identify risks, except from the fact that experts offer valuable insights on that matter, previous studies offer indications of controls on the assessment, but majorly, the monitoring of risks in public sector organizations. In general, risk monitoring within the sector has been evidenced as being done in a way of understanding how public sector organisations perform in managing key risk areas (Paape & Speklé, 2012). Moreover, as discussed in the previous section, literature has shown the importance of feedback and learning-inducing avenues that are utilised by PSO to deal with the assessment and monitoring of their risks. Furthermore, the monitoring of risks, in terms of the strategies that are in place to deal with them, was done through the use of various risk measures through risk performance management systems. However, and towards a complete relation of control to all the aspects of contemporary risk management practices, there is very little discussion around what and how controls are utilised in identifying risks. The limited indications are wrapped around some indicative comments that this is done through utilizing the competence of risk experts and senior managers (responsibility centres) within the organizations, backed up by imposing codes of conduct and communicating those risks through various avenues. As a result, not only the scope of the literature discussed above is very limited in providing evidence of how control processes are working and are integrated in the case of PSO risk management, but it also neglects a very important aspect of this process, that is the controls utilised for the identification of unknown risks within organizations, and in the public

sector in particular. As pointed out by Scheytt et al. (2006), the identification of risks is an important and an on-going process that utilised different information functions within organizations for the identification of risk and unknown or potential risks. The importance of identifying risks (and emergent risks for that matter) stems from the need for organizations to expand their risk appetite, such systems exist within organizations and are used for the identification of risks. However, both the risk management and management control literature have neglected this. Identifying risks (or making sense of uncertainty), is integral in the risk management process of PSO (Power, 2007) and since management control is integrated in PSO risk management (Bracci et al., 2022), controls are expected to play a vital role here. However, both the management control and the risk management literature has neglected to offer insights of the management controls used for the identification of emergent or potential risks that can harm the organization and hinder its strategic objective attainment.

Finally, and connected to the above, it is known in the literature that organisations utilise information sharing tools and processes/environments, even tacitly, (Fischbacher-Smith & Fischbacher-Smith, 2014) that reflect the notion of emergent risks and are important towards communicating those risks. The importance is reflected in the fact that the integrity and reputation of organizations in the post-crisis era lies on their competence in identifying and managing a great variety of risks, both quantifiable and intangible, most of which were neglected before (Power, 2009; Andersen, 2016). However, this competence is hindered by the fact that not all organizational risks are included into the subsequent risk appetite as there are unknown by organizations. Before managing any risks, organizations are required to identify the risks that are important to them and those that need to be included into their risks appetite to ensure strategic objective attainment. Subsequently, after forming their risk appetite and risk management framework, organizations are held accountable to their external environment, majorly the society, for the management and mitigation of their identified risks. However, as mentioned before, it is difficult for organizations to understand their full risk framework. They are limited by both their decision-making capacity in risk identification (March, 1994), but also by the complex and demanding environment within which they operate that is a source a source of high uncertainty (Andersen, 2016). More specifically, organizations tend to neglect various risks that are important to them due to their inability to process huge loads of information about risk (Scheytt et al., 2006) and because they are exposed to an environment of uncertainty due

to the complexity of operations they are required to attend to. In recognising this and by understanding that the inclusion of more risks, especially operational and reputational ones (Power et al., 2013), organizations are indeed utilising appropriate information systems within their operations to overcome this challenge. As described in the previous section, that also applies to the public sector. However, to date, literature on the use of management controls in the process of identifying those risks is scarce to none. When it comes to public sector institutions specifically, research and empirical evidence on risk management does follow the contemporary agenda of risk management, which is managing risk, as a part of a wider uncertainty, and harnessing information for uncertainty for proactivity and opportunity-seeking (holistic risk management) (Power, 2007; Andersen, 2016). To reconcile this gap, Themsen & Skærbæk (2018), offer some insights on how uncertainty is realised using performative risk frameworks and technologies in public sector mega-projects. Through a qualitative case study of a multi-billion public sector mega-project, they show how public agents utilised a performative framework in conjunction with an IT-based visual system, to filter out emergent risks and establish new risk or discard uncertainties. This happened by the public agent engagement with the performative framework which was fed to the IT-based system to visually present the emergent risks, their causes and impacts (Themsen & Skærbæk, 2018). The final uncertainties, which were later translated into organisational risks, were made sense by the agent's perceptions and engagement with the field of work. Effectively, new emergent risks were fed into the IT system and were agreed upon communication with other agents and the field needs. Then, the results were filtered out and visualised. However, how this happens only shows part of the story as this study only focuses on a single project. This only marginally adds to the literature on public sector mega-projects (Jordan et al, 2013) in the effort to understand what elements affect uncertainty, including technologies and relevant agents associated with these projects. That is because these findings do not offer a holistic approach to risk management, and they also do not offer any interaction of control with the risk management tool to show full integration. They focus on a single project of a single public sector institution, with specific characteristics. As such, the findings are still unclear on that matter, as more evidence is required to understand how uncertainty is shaped, from the interplay of a variety of sources and interactions (Themsen & Skærbæk, 2018). In fact, the authors, in realising the complexity of managing public sector risks, call for more research on how risks are constructed, in a holistic manner, with particular attention on conditions of limited budgets,

time and specific requirements (Themsen & Skærbæk, 2018). In that respect, the role of MCS in managing uncertainty, is still overlooked. Especially in the matter of controls, as it was seen in the previous discussion of the literature, evidence is provided for controls for pre-defined risks, and formal risk management procedures, despite the presence of the informal and tacit information exchange channels (Fischbacher-Smith & Fischbacher-Smith, 2014). Moreover, the literature presented above concentrated on the risk management element of the organisations under study and the reference to the controls utilised in the process were majorly a by-product of the studies. Understanding MCS utilised for managing uncertainty (emergent risks) ill further add to the integration knowledge of MCS and risk management and offer valuable insights for practice.

To summarise all the above, literature has identified the interplay and integration of management control tools for risk management in the public sector. That includes identifying the central role of control tools in managing public sector risk. However, this literature lacks evidence on the integration of these controls with risk management procedures in practice in a holistic manner, and with specific attention needed to the processes that are reflected in this integration, especially that of PMS. Moreover, specifically for emergent risks, controls utilised in that process need to be uncovered and their processes need to be better understood, within this integration agenda. The literature, as seen above, requires more case studies to unravel those issues and provide empirical evidence to inform academia and practice (Cuganesan et al., 2014; Fischbacher-Smith & Fischbacher-Smith, 2014; Rana, Wickramasinghe & Bracci, 2019; Bracci et al., 2022), which will add to the ongoing demands to better understand the controls utilised in the risk management process of contemporary organisations (Bhimani, 2009, Jordan et al., 2013; Soin et al., 2013). Understanding the processes of integration, especially through case studies from international contexts, will unravel risk management implementation success factors, control influences and inform policymaking and practice. It is clear that management control is integrated to the effort to manage PSO risks. However, what is not clear and required in the literature, as argued above, is evidence of the processes that are associated with this integration in controlling for PSO risks. To address this gap in the literature, this research will attempt to answer a number of research questions. The main question under which the rest of the questions will reside in is:

"How are management control systems integrated with risk management in public sector organisations?

More specifically, the following specific questions will be asked:

1. What management control systems are utilised to manage risk in the public sector?
2. What are the processes by which PMS in is integrated in PSO risk management?
3. How do different control systems facilitate the risk management process in the public sector and complement PMS to form a wider control framework?
4. What are the processes by which a PSO controls for emergent risks as part of their risk management framework?

2.4.4 Contribution of the study

This study contributes to the current management control and public sector risk management literature in a number of ways. At a starting point, this study aims to answer the calls of the public sector risk management literature for a better understanding of the integration of risk management and management control through case studies of international contexts, to unravel the processes behind this integration (Bracci et al., 2022). This is of particular importance, as calls have been made in the public sector literature to better understand the processes by which these two tools are integrated in PSO (Rana et al. 2019; Rana et al., 2022). As a result, these authors argue, that providing evidence of the processes behind the integration of management control and risk management in the public sector, will have implications for advancing practice and policy, in an effort to advance more effective risk management practices in the sector. Therefore, this study, through a case study from the Greek public sector, will offer evidence of the management control tools that are utilised to manage PSO risk. In recognising the integration of these tools with risk management, in the literature, this study will provide evidence of the *processes* by which these management control tools are integrated with risk management frameworks in this context. Hence, this evidence will also advance current management control literature. For instance, while studies that provide evidence of the integration and examples of various control tools do exist (for example Woods, 2009, 2010; Collier & Woods, 2011; Rocher, 2011; Paape & Speklé, 2012; Rana, Hoque and Jacobs, 2019)), this study will advance these studies by offering evidence of *the process* how these

notions are integrated. Within this effort, a few control tools will be paid particular attention. For instance, in recognising the importance of PMS tools in managing PSO risk (Power, 2004b), this study will add to the public sector risk management literature by answering the calls to better understand how this tool is integrated in PSO risk management, and also how PMS tools operate and are associated with other PSO control systems to form a wider control framework in PSO (Cuganesan et al., 2014). These authors called for more research on the matter that should provide evidence on how this is done in practice to manage PSO risks, and also how other systems are utilised to manage the inherent risks of PMS tools in PSO (Cuganesan et al., 2014). Therefore, this study will provide evidence of the operation and integration of PMS systems in PSO risk management, in an effort to also reconcile the level of integration of PMS and risk management in PSO, as there are mixed results in the literature at the moment, mainly due to evidence being provided from rather few contexts (Bracci et al., 2024). At the same time, this study will add to the management control literature by answering the calls to better understand the role of management control systems in managing emergent risks. Literature to date has recognised the importance of such systems, especially in the form of information sharing systems (e.g. Scheytt et al., 2006; Fischbacher-Smith & Fischbacher Smith, 2014). Literature has also provided some evidence of control tools utilised towards identifying emergent risks (see for example Themsen & Skærbæk, 2018), but there is very little evidence to date (Jordan et al., 2013). In recognition of the importance of identifying emergent risks for PSO (Power, 2007), this study will provide more evidence to the current literature on what control tools are utilised to manage emergent risks in PSO, and how are these integrated within the wider risk management framework of such a context. Subsequently, by providing evidence of the integration of management control tools with risk management frameworks in PSO, this study will add to the ongoing risk management literature on how these two systems are integrated (Rana et al., 2019; Bracci et al, 2022), while at the same time adding to the wider management control literature, that has asked for more evidence of the interconnectedness of risk management and management control as a practice (Bhimani, 2009; Soin et al., 2014). For that matter, and through utilising a the revised Levers of Control theory (Tessier & Otley, 2012) as a lens to identify and explore the management control systems that are utilised in PSO risk management, this study will add to the management control literature that calls for more case studies to test its conceptual validity and analytic generalisability (Tessier & Otley, 2012),

especially when it comes to its applicability to public sector management control for risk management.

3 Understanding risk handling in organizations: a theoretical framework

3.1 Introduction

This chapter introduces the theoretical framework that this study will utilise to answer its research questions. Section 3.2 gives a brief background of the development of the theoretical framework, Simons' Levers of Control (1995) and its main concepts. Section 3.3 discusses the limitations of the original framework as identified in the literature, and the rest of the sections discusses how Tessier & Otley reconciled these issues in a revised form of the framework, which will be the one utilised in this study as a theoretical lens to explore the phenomenon of how controls are utilised to manage risks in the public sector context. Finally, section 3.4 justifies the choice of the said framework in light of answering the research questions of this study and articulates the theoretical contribution that it will make.

3.2 Levers of Control: background.

As discussed earlier, risk and the management of uncertain events that can affect organizational objectives have already permeated the way organizations operate and perform in pursuit sustainability and success of their operations (Power, 2007). In order to survive and succeed, organizations utilise various ways of handling risk, understanding uncertainty in their strategy and transforming this uncertainty into risks to be managed. An understanding of the capability of organizations in handling risks and uncertainty derives from the management control theory. More specifically, the Simons' Levers of Control framework (1995) offers an adequate understanding of how risks exist in organizations and how they are handled by control systems. Moreover, the role of uncertainty and how organizations make sense of it is also established. Understood together, risk and uncertainty inform the implementation and modification, where necessary, of organizational strategies with an aim at meeting the desired organizational objectives.

Simons (1995) developed a theoretical framework that aims at understanding how managers implement strategies and how they control those strategies to meet organizational objectives (Ferreira & Otley, 2009). More specifically, the Levers of control framework was developed to offer an understanding of how managers design and use various management control systems

to implement their business strategy and achieve organizational objectives through guiding employee behaviour and remodifying strategy when dynamic changes in the environment occur and strategic objectives are threatened (Simons, 1995; Malmi & Brown, 2008). In his framework, Simons (1995) argues that in order for contemporary businesses to survive in a demanding and constantly changing business environment, they need to take into consideration the management of three dynamics. The first dynamic has to do with "creating value" (p. 14) and is considered with the tension between the limitless opportunities that the organisation might have and the limited attention its managers can pay to them. The second dynamic has to do with the "dynamics of strategy making" (p. 18), or, in other words, the way intended strategies are handled and matched with emergent strategies. The final dynamic considers the way "human motives" (p. 21) come into play and delimitates the tension between the opportunistic behaviour of organizational members and their desire to contribute to the collective benefit of their organization. For Simons, each of these dynamics is equally important and organizations are required to find a way to manage the tension between these dynamics in order to achieve success. In order to manage those tension, to achieve a balance, organizations focus their attention on managing four strategic imperatives namely, core values, risks to be avoided, strategic uncertainties and critical performance variables (Simons, 1995). This is where organizations utilise the Levers of Control. The levers utilised to control for the aforementioned imperatives are, consecutively, belief systems, boundary systems, interactive control systems and diagnostic control systems.

3.2.1 A closer look to the Levers of Control framework: Risk and uncertainty under the lens

Contemporary organizations are faced with continuous innovation, fierce competition and volatile ever-changing business environments (Alawattage & Wickramasinghe, 2014). As a result, controlling for organizational strategy is a crucial, yet complex task for organizations. More specifically, increased competition, ever-changing products, markets and organizational forms as well as the need to sustain an adequate knowledge database for sustainability, brings about new circumstances in business making. As a result, organizations need to re-focus their attention and effort to create adaptive strategies to those conditions in order to ensure sustainability and growth (Simons, 1995).

In order to achieve the aforementioned success, organizations are faced with a challenge. That is, considering the existent organizational dynamics and reconciling for their tension within both their organizational and strategic environment. For Simons (1995), organizations need to manage tensions "between freedom and constraint, between empowerment and accountability, between top-down direction and bottom-up creativity, between experimentation and efficiency" (p. 4). First, a balance needs to be struck between the numerous opportunities that can be available to organizations at any point in time and the issue of limited attention by their managers (Simons, 1995). On the one hand, organizations may be faced with new growth and development opportunities at many points in time throughout their existence. That is, opportunities for new products or innovations can emerge from competition, accidental events from customer feedback or even unpredictably through the daily operations of a firm. On the other hand, in order to exploit such opportunities, organizational members, and managers in particular, need to devote effort and attention. Such attention to opportunity seeking is scarce in contemporary organizations (Simons, 1995). More specifically, management can only devote a specific amount of attention to emerging opportunities while apprehending opportunity-seeking responsibilities on other organizational members, usually subordinates. The latter are helpful to achieve the greatest opportunity exploitation with the lowest amount of attention provided by managers. Therefore, organizations need to find a way to exploit as many opportunities as possible with the realisation that only a limited amount of attention will be devoted towards that goal. This limited attention is tackled by opportunity-seeking delegation to subordinates in order to exploit as many business opportunities as possible.

Closely related to opportunity seeking comes the matter of emergent strategies in organizations and the dynamics that exist within. In contemporary organizations, strategies can emerge in two ways (Simons, 1995). One way is for top-level managers and directors to impose their own strategy as they see fit for the strategic objectives of the organization to be operational and sustainable over time. The second way is for low-level organizational members to come up with a new strategy direction based on their day-to-day operations or their interaction with customers and their market. Therefore, organizations should allow both avenues of strategy to emerge in a complementary way informed by all levels of the business (Simons, 1995). Intended and emergent strategies should not replace one another but rather influence and inform the creation of the whole business strategy.

The final balance that needs to be struck when controlling for organizational strategy has to do with the dynamics crated by human motivation. Indeed, individuals, in general, tend to be opportunity-seekers that are strongly inclined to maximising their personal gain or interest if conditions permit (Simons, 1995). Now, if they are properly motivated and led, then individuals might feel the need to exploit opportunities but do so in a collegial and collective manner. That is, individuals can have a high level of personal satisfaction when they are feeling needed and important in the accomplishment of a significant task (Simons, 1995). Therefore, the human condition for opportunity seeking lies on top of a line with two extremes: self-interest and complete collective interest. If both extremes exist in an organization, negative results will emerge endangering the organizations and its members. Therefore, organizations need to find a way to "reconcile" or bring a balance in the aforementioned line where individual opportunity-seeking lies by motivating individuals to behave in a manner that is beneficial for them and the organization at the same time (Simons, 1995, p. 24).

In order to adapt to their volatile environment and strike a balance between the aforementioned opposing elements, organizations are paying attention to four critical areas that aid them in successfully implementing and maintaining their strategies and strategic goals, either intended or emergent. These four areas have a dedicated control system that organizations are using to manage them. First, the organizational needs to establish and communicate, throughout its various internal and external stakeholders, its core values. These have to do with the vision, mission and purpose of the organizations, as well the appropriate-accepted opportunity-seeking domain enforced to organizational members delineating their relevant activities. Core values serve as the backbone of an organization's everyday activities and routines and, to be effective and relevant, they need to be constantly re-evaluated in adapting to the changes of the business environment. To control for this imperative, managers design and use the "belief systems", which serve as a formal tool for guiding behaviour and imposing direction of employee. As Simons puts it, a beliefs system is the "explicit set of organizational definitions that senior managers communicate formally and reinforce systematically to provide basic values, purpose, and direction for the organization" (1995, p. 34). In a sense, core values are the direction that managers want their subordinates to adopt and are associated with the strategy of the firm.

Then, organisations need to evaluate and establish the avenues within which their strategies will operate and gain shape by delineating the acceptable and non-acceptable domains of such

activity (Simons, 1995). These choices are influenced by ethics, business conduct, social norms and organizational capacity and are denoting the organizational risks to avoided, the second strategic imperative. This imperative is controlled by the second lever of control, the boundary systems. Boundary systems are further categorized into two parts based on how they operate. The first part delineates the strategic boundaries of opportunity seeking and clearly defines the business areas that the organization should be prohibited to enter and exploit. The second part has to do with enforcing the acceptable business conduct mapping the domain of how organizational members should operate when doing business and what they should avoid doing. In brief, boundary systems are designed to communicate ad establish the acceptable domain of strategic opportunity and business conduct of the organization.

The third strategic imperative that organizations pay attention to is what Simons calls "critical performance variables" (1995, p. 66). These are the essence of strategy implementation as they serve as key indicators of its performance. That is because they measure the way organizational actions align with strategic underpinnings by reflecting on pre-set targets. To control for this imperative, managers design and utilise the diagnostic control systems, the third lever of control. The control of this lever is exercised in three steps. Managers need to identify and measure the key performance variables that are capable of informing the strategic and operational outcomes of the organization. When these variables are understood, their intended outcome I used as a benchmark against the actual outcomes of the organisations in the relevant strategic and operational domains result in. The last step is to go forth and correct any deviations that might be observed between the actual and the intended outcomes. As it is obvious, diagnostic control systems are concerned with controlling for the variables and outcomes of the intended strategies of the organization. Moreover, because of their use as evaluating and benchmarking the performance of different areas within the organisation, they are closely related to the use of cybernetic controls (Otley & Berry, 1980).

Finally, organizations are paying attention to elements that have the potential to jeopardize their strategy and eventually their strategic objectives and sustainable growth (Simons, 1995). This particular area has to do with managing the strategic uncertainties of the organization. As discussed before, the current volatile and highly competitive business environment within which organizations operate imposes a form of strategic uncertainty. That uncertainty is translated into threats that can hinder or invalidate the current strategies of the organization. In

order to ensure sustainability, organizations need to provide answers and minimise that uncertainty. To tackle those threats, organizations need to gather information about such uncertainties, see how they can hinder their objectives and re-modify their strategies based on that. The company that can obtain the most advanced and proper information for the market, has the greater chance to survive in such an environment. However, it is difficult for organizations to obtain such information levels, thus organizations lack knowledge and therefore experience strategic uncertainties (Simons, 1995). Interactive control systems are the fourth lever of control, and their job is to communicate and understand the strategic uncertainty imposed to organizations, thus enriching their capability of identifying strategic threats and proceeding to strategy innovation. In an endeavour to enhance organizational learning, interactive control systems impose a dialogue, promote communication and information gathering outside standardised function of the organizations to obtain information about strategic uncertainties. This is where emergent strategies might surface to question intended strategies and promote an organizational learning. It also needs to be mentioned here that interactive control systems are always present in organizations and are re-modified for organizational learning. Moreover, any control system can be deemed an interactive control as long as it serves the purpose of organizational learning (Alawattage & Wickramasinghe, 2014). The levers of control framework can be depicted in Figure 1.3. What follows is a brief summary of the framework with specific relations to controlling for organizational strategy.

As Figure 1.3 depicts, the management control systems that are designed to implement and innovate the strategic underpinnings of organizations are not isolated from each other. They need to be used together to promote the strategy of the organization and collaborate in reaching the organizational objectives (Simons, 1995). In the same manner, strategic control happens by utilising the four control systems in a complementary manner. For example, when an uncertainty is communicated within the organization, the re-modification of strategy is possible on by the acceptable domain of opportunity-seeking. Indeed, strategy can only be remodified within the boundary of strategic reform as denoted by the boundary systems backed up by the purpose this emergent strategy can have as denoted by the imposition of the core values by the belief systems. In turn, new strategies might impose new critical variables which will be brought under the attention of interactive control systems.

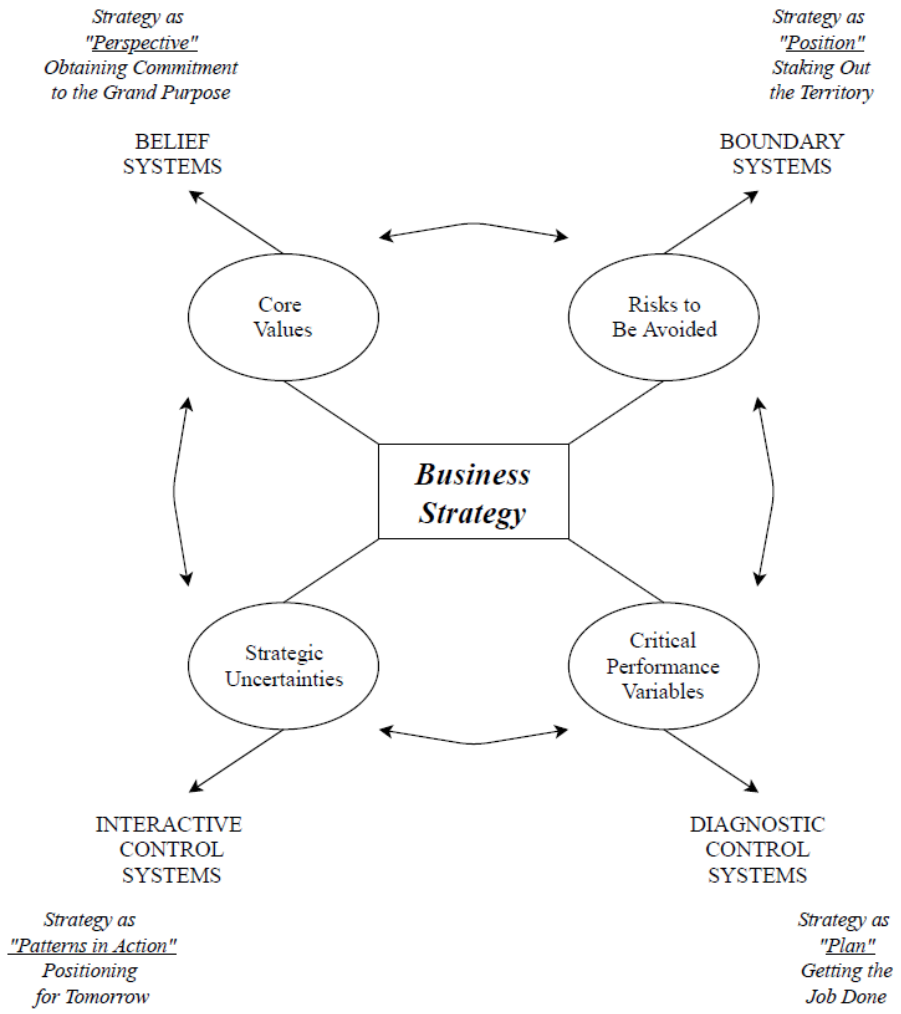


Figure 1.3 *The Levers of Control Framework (Simons, 1995, p. 159).*

3.2.2 Criticism of Simons' initial framework

Throughout the years, many researchers have utilised the levers of Control framework to make sense of how different organizations design controls to guide their strategy implementation and innovation (Tuomela, 2005; Widener, 2007; Mundy, 2010; Arjaliès & Mundy, 2013; Bedford, 2015). Indeed, Simons' (1995) initial management control framework has been criticised for its loosely defined concepts in understanding the use of controls (Ferreira & Otley, 2009). For example, there is a controversial view of the interactive controls. Indeed, on the one hand, Bisbe et al. (2007) have specific requirements for controls to be characterised as interactive. For the authors, a control should be intensely used by both managers and subordinates, should include the element of communication for strategic uncertainties and the channel of

communication should be characterised by freedom of use as in managers are not interfering with the control and the information provided. On the other hand, Ferreira & Otley (2009), distinguish interactive controls as a two-sided concept: various controls that are used interactively through all levels of the organization and "strategic validity controls that are interactive controls associated only with the validity of the strategy (p. 274). Tessier & Otley (2012) address these ambiguities in the concepts more thoroughly and propose a revised framework of the Levers of Control that aims at offering a more holistic approach to controls with a higher conceptual strength. Although the purpose of this section is not to present the ambiguities thoroughly, a brief discussion of them will follow in order to make a better sense of the framework. Then the revised Levers of Control framework will be presented as constructed by Tessier & Otley (2012).

3.2.3 Ambiguities in the original framework

Tessier & Otley (2012) explicitly point out that their work of concept refinement on Simons' (1995) framework derives from controversy about it in the literature. There are two distinct areas that the original framework lacks conceptual clarity: the dual role of controls and the levers themselves, as the latter were discussed in the previous section. With an emphasis to the dual role of controls, literature has been ambiguous of their concept. By the term dual role of controls, according to Simons (1995), the way they are used to manage tension is explicitly intended here and not the levers themselves. The first conceptual difficulty with the dual role of control has to do with their explicit duality (Tessier & Otley, 2012). For example, there are authors who suggest that the dual role of controls has to do with how they are used: for employee's compliance and performance towards objectives and/or for encouraging strategic opportunity seeking (Mundy, 2010). On the contrary, evidence suggests that the role of controls can be considered as referring to their quality as "good", or enabling controls introducing higher efficiency and effectiveness, and "bad" or coercive controls that are only used for compliance irrespective of being dysfunctional for the organization (Ahrens & Chapman, 2004; Tessier & Otley, 2012). Another issue with the dual role of controls has to do with the way designers (managers) and users (employees) of controls perceive them. More specifically, this duality, as Tessier & Otley (2012) argue, has to do with managerial intentions on the one hand and employee perceptions on the other that have not been explicitly pointed out in the literature. The way controls are presented are also implicit in the literature as a factor mediating employee

perception and attitude. The latter, according to the authors, should be classified as negative, positive, or neutral according to if they are helpful to employees or limit their space. Tessier & Otley (2012) argue that these aspects of controls should be included in the framework. Finally, the ambiguity in the dual role of controls has to do with their objectives. Literature has distinguished the objective of controls as positive and negative, when they are associated, respectively, with the achievement of organizational objective of following laws and regulation (Cunningham, 2004). However, since Tessier & Otley (2012) already gave these labels to employee attitudes towards controls, they propose a different classification of control objectives by reconceptualising their role according to what they are aiming for. Moreover, literature suggests that only performance is to be rewarded with controversial evidence that compliance can also be rewarded. In brief, to address the ambiguities about the duality o controls and to build more robust concepts, Tessier & Otley (2012), attempt a revision of the framework's main concepts. First of all, by abolishing the "good" and "bad" role of controls, the authors distinguish between enabling and constraining controls. According to their definitions, enabling controls promote "creativity and flexibility", while constraining controls "reduce options and thus increase predictability" (Tessier & Otley, 2012, p. 175). This distinction goes over the use of levers of controls as they can be used in both these ways. Furthermore, controls incorporate the reasons they were designed by managers and the way they are perceived by employees, as mediated by the way they are presented to the later. Following presentation and exposure, employees can develop certain attitudes towards controls. Finally, the objectives of controls are only either compliance or performance and managers can reward or punish both objectives in the event they are met or not, respectively. After addressing the issues with control duality, Tessier & Otley (2012) go on to address the issue of the levers of control vagueness next.

Apart from the ambiguity of the duality of controls, the Levers of Control themselves lack conceptual clarity and understanding as they are characterised as "vague" concepts (Tessier & Otley, 2012, p. 177). First of all, the concept of diagnostic and interactive controls lacks clarity and is debated in the literature as discussed above. Moreover, various control systems are used either interactively to ensure communication or focus on strategic uncertainties to promote learning, or diagnostically to observe current strategy performance (Ferreira & Otley, 2009; Adler & Chen, 2011). Evidence suggests that a single control can also be used both ways

(Tessier & Otley, 2012). Therefore, the authors argue that interactive and diagnostic controls are not by themselves control systems, but they rather represent the way various controls system are used in an organization. They support their argument by stating that when a system is used interactively to obtain information about strategic uncertainty, it later on transforms to a system used in a diagnostic way following the strategy re-modification. To refine the concept, first of all, Tessier & Otley (2012) follow a combined approach to the competing definitions of Bisbe et al. (2007) and Ferreira & Otley (2009). The authors consider their revised framework as considering that interactive controls have two distinct concepts: controls intensively used throughout the organizations to promote communication and learning and "strategic validity controls" to point out the way strategic uncertainties influence the strategy performance of the organization. Between these concepts lies the concept of diagnostic controls that represents controls used once the strategy, either emergent or intended, has been clearly established in the organization. Following that, control systems are not interactive or diagnostic anymore. Controls systems are separate, and they are used either interactively or diagnostically.

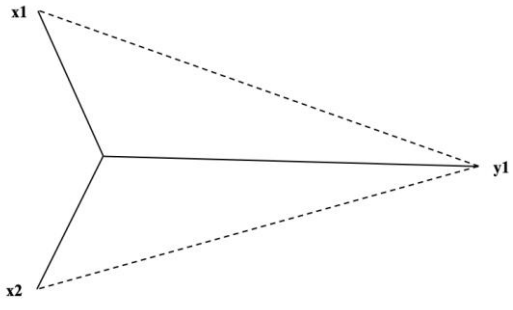
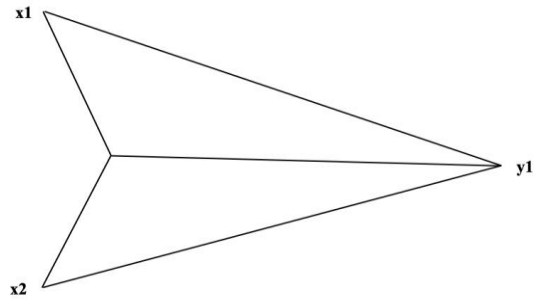
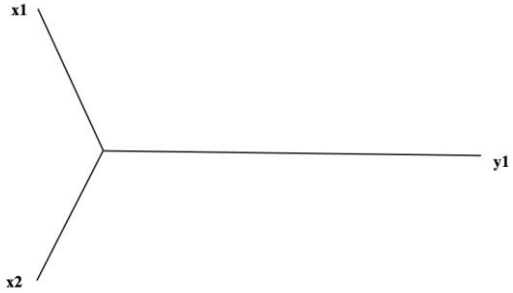
The second ambiguity has to do with the notions of belief and boundary systems. The ambiguity for these terms lies both in their concept and in their relationship with each other. However, before expanding on this discussion, two definitions need to be provided, that of social and that of technical controls. On the one hand, social controls are controls associated with core values of the organizations, including beliefs, norms and symbols (Alvesson & Karreman, 2004; Simons, 1995; Malmi & Brown, 2008). On the other hand, the term technical refers to the controls that are used for how tasks need to be performed and how individuals need to be organised and are based on rules, procedures and standardised processes (Perrow, 1986; Malmi & Brown, 2008). The notion of cybernetic and output controls is included in technical controls (Tessier & Otley, 2012). The conceptual ambiguity of belief and boundary controls, and their relationship, lies in the fact that their relationship is blurred. According to Simons (1995), belief controls can influence boundary controls and vice versa. Moreover, they both represent a type of control and are present in different levels of analysis (Tessier & Otley, 2012). Hence, boundary controls are composed of both technical and social types of controls while associated with promoting compliance of the organizations to rules, regulation and the law. In a similar vein, belief systems are composed of only social controls and their objective is both organizational performance and compliance as discussed above. Therefore, the

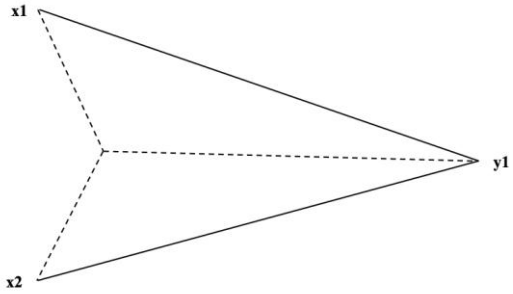
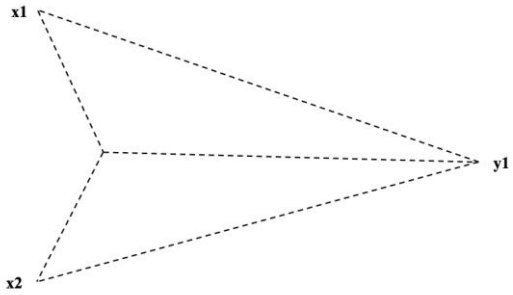
ambiguity rises from the fact that the notions of belief and boundary controls are interrelated and do not represent a system but rather a characteristic of controls (either social or technical). To clear this point, Tessier & Otley (2012), distinguish between social and technical controls, which can both be characterised as belief controls, or boundary controls. The new category of controls is working together to construct four control systems.

Speaking of systems and following the re-conceptualisation of diagnostic controls, interactive controls, and boundary and belief systems as not systems per se, four control systems emerge as central to the revised framework. Within those systems, a "synergy" of controls can occur (Tessier & Otley, 2012, p. 180) as it will be discussed below. The authors borrow Simons' classification of boundary systems to point out that their objective of compliance is embedded into both the strategic and the operational levels of organizations levels. In the previous section, the notions of business boundaries and strategic boundaries were associated with risks to be avoided (Simons, 1995). For Tessier & Otley (2012), this distinction leads to the clarification of two distinct control systems that are associated with one objective at both levels of the organization. These control systems are called operational boundary and strategic boundary respectively associated with "the following of rules and the preservation of value" (p. 178). Compliance informs a way of accountability as well. Following the same logic and pointing out the strategic performance controls discussed earlier, two control systems emerge with the objective of performance. On the one hand, there is the strategic performance system associated with monitoring the performance of the strategy of the organization. In this case, performance is defined as "the achievement of organisational goals and the creation of value" (Tessier & Otley, 2012, p. 176). On the other hand, there is the operational performance system associated with the monitoring of the critical performance variables of the intended strategy of the organization. As mentioned before, these four control systems are constituted of different types of controls (i.e. social and technical controls). The aforementioned synergy emerges when a specific social or technical control is incorporated into more than one control systems. Indeed, a social or technical control can inform both compliance and performance at both levels of the organization (Tessier & Otley, 2012). Through this characteristic, various controls form a connection and by extension, they create a synergy of the various control systems. The revised Levers of Control framework will now be presented as a whole for further clarity. This synergy, this co-existence of controls, can also be further established by how they

support each other (Bedford, 2020). In Bedford's typology, controls are seen to be working with each other and have a relationship, mainly through their operation and area they are targeting for control, for example a specific strategy. In recognition of this, the author conceptualised the position of this relationship of controls that form a wider control system in organisations. As a result, control tools exist with each other in many fashions and are there to complement, or substitute, each other. The notion of complementarity comes into effect when different control practices that have weaknesses, are less effective or need further support to operate are complemented by other tools that are utilised in conjunction, to reconcile these issues, for the same control aim. Moreover, when control tools suffer from inefficiencies due to the operation of co-existing control tools, this is when controls are substituting each other. These are called the interdependent effects. At the same time, as Panel B of table 1.3 shows, this interaction can cause specific effects on the aims of controls in an independent fashion. For example, a control tool that might be used for a specific purpose, might supplement the operation of another tool and increase its effectiveness or vice versa. At the same time, a control tool might be used that hinders the effectiveness or goal of another. Since this thesis argues towards a system of control tools that aid in PSO risk management, this typology would be helpful to see the different relationships of controls and how they exist in relation to each other, interdependently or independently, and how they affect each other's operaton and purpose, in the case of PSO risk management. That, will offer insights on the validation of this typology to the setting of PSO, as the author called for further evidence to support these concepts, and how MCS tools co-exist and also affect each other. More details on this typology can be found in Table 1.3. This table describes control practice connections, exactly as the author coined them.

Panel A: Interdependent effects		
Causal Mechanism	**Definition**	
Complements		

Compensating	The MC practice counteracts the weaknesses or limitations of another MC practice in resolving a control problem.	
Reinforcing	The MC practice enhances the effectiveness of another MC practice in resolving a control problem.	
Enabling	The MC practice creates the conditions for another MC practice to contribute to resolving a control problem.	
Substitutes		

Inhibiting	The MC practice hinders the effectiveness of another MC practice to resolve a control problem.	
Exacerbating	The MC practice accentuates the detrimental effects of another MC practice to worsen a control problem.	
Instigating	The MC practice creates the conditions that trigger another MC practice to worsen a control problem.	
Panel B: Independent effects		
Causal Mechanism	**Definition**	

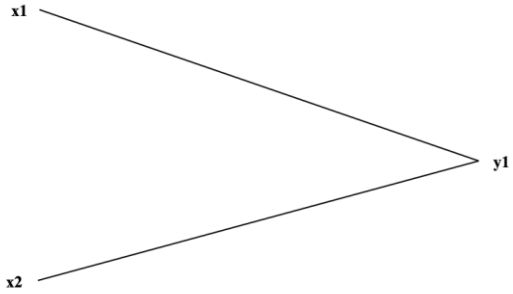
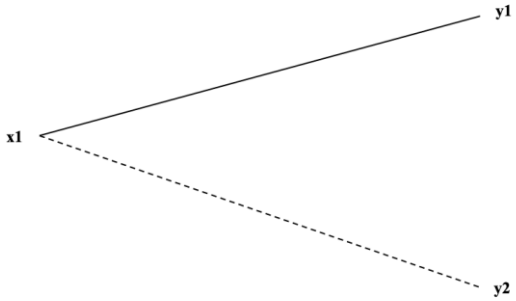
Supplementary	The MC practice contributes to resolving a control problem in addition to one or more other MC practices.	
Conflicting	The MC practice contributes to resolving one control problem but hinders the resolution of another.	
Redundant	The MC practice (x3) is unnecessary for a control problem to be effectively resolved.	(x1*x2 + x1*x2*x3) ↘ y1
Interchangeable	The MC practice (x3) can be replaced with one or more other MC practices (x4) to resolve a control problem to equal effect.	(x1*x2*x3 + x1*x2*x4) ↘ y1

Table 1.3: Complementarity and substitution of management controls as a system (Bedford, 2020, p. 3-4).

3.3 The Revised Levers of Control framework

The revisited framework will be presented with a central reference to the management control systems that are designed and used by organizations and their managers. As shown in Figure 2.3, at the centre of the framework lies the interconnection and collaboration of various social and technical controls in every control system. These control systems are both in the same box to represent the fact that they influence each other, this influence and interconnectedness is required for organizational control coherence (Alvesson & Karreman, 2004). This depiction also emphasizes the use of controls as a package (Otley, 1980; Malmi & Brown, 2008). As it will be shown now, different types of social and technical controls are utilised in every control system to form the four control systems that Tessier & Otley (2012) propose.

The first two control systems are concerned with controlling for performance at both organizational levels. The first control system is called Operational Performance Control System and is associated with the use of control systems that aim at pointing out what actions must the organization take into consideration for strategy coherence through relying on the assessment of critical performance variables at the operational level. The role of cybernetic control is central here, as dictated by the diagnostic use of controls, complemented by the various use of "values and organisational symbols that promote organisational performance" and technical procedures that delineate the acceptable organisation of activities (Tessier & Otley, 2012, p. 180). Here, performance is regulated by formal control tools that managers utilise to "communicate formally and reinforce systematically to provide basic values, purpose, and direction for the organisation (Simons, 1995, p.34). At the same time, controls are used diagnostically to communicate critical performance variables to monitor organisational performance and correct deviations (Laguir et al., 2019). The second control system at is called Strategic Performance Control System and comprises of controls that monitor the current strategy of the organization and its performance by assessing whether strategic uncertainties have an impact on its mission and vision. In here, various social controls are utilised to delineate the strategic objectives of the organization, in line with formally communicated values and procedures (Simons, 1995) Moreover, technical controls in the form of monitoring the environment of the organization for uncertainties are present as well. Previous literature has suggested that control in this domain aid explicitly in managing strategic uncertainties. For example, interactively used tools are associated with communicating emergent uncertainties

that can invalidate current strategy (Tuomela, 2005). Examples of this practice are information exchange meetings that discuss these uncertainties and devise approaches to tackle these (Mundy, 2010). Here, managers utilise formal control tools to engage in regular discussions with their subordinates interactively, to exchange information for strategy and strategic innovation (Simons, 1995). At the same time, regular meetings with all organisational parts, mediated by the use of information exchange software, has the effect to communicate uncertainties and new strategy formulation. These are connected with PMS tools that aim at monitoring how key variables are associated with the success or invalidation of current strategy due to these uncertainties (Mundy, 2010). In different strategic considerations, uncertainty is also managed by being communicated via meetings with relevant operational managers and senior, to communicate emergent opportunities (Arjaliès & Mundy, 2013). At the same time, best practice can also be communicated with interactively used meetings to incorporate innovation new strategic directions based on emerging issues and competition. As a result, control tools utilised in strategic and operational performance systems, are directly associated with managing uncertainty, especially uncertainty connected with strategic opportunities. This has been suggested to directly influence performance measures (Widener, 2007).

The second set of control systems aim at controlling for organizational compliance at both operational and strategic levels. Both systems are governed by the notion of the risks to be avoided at both levels. On the operational level, Operational Boundary Control Systems are delineating the acceptable domain of action by employees. This acceptable domain of action is communicated through social controls, i.e. values and business conduct rules or it gets set through technical controls such as procedures and rules The source of information that these controls communicate derives from the organizations itself and the various stakeholders that exist in its domain such as regulators, the government, society and the industry that identifies the organization. Similarly, but at the strategic level of the organization, the Strategic Boundary Control Systems consist of controls delineating the acceptable domain of strategic opportunity seeking by the organization, similar to the initial idea of Simons (1995). Once again, various social and technical controls are utilised here and form a set that frames the limits for strategic innovation, project engagement and various activities that are associated with strategy innovation. Previous literature has shown that boundary controls, usually supported by communication of core values, are key in managing risk, as they are associated with

minimizing risk of employees engaging in activities that undermine organisational processes, or acceptable operations risks, such as financial risks to be avoided (Tuomela, 2005; Bedford, 2015). Examples include the communication of off-limit activities, sanctions on undesirable business conduct and enforcement agendas of strategic boundaries (Mundy, 2010). In managing specific strategies, and the risk behind not adhering to these strategies, boundary controls are explicitly found to be able to manage a variety of strategic risks (Arjaliès & Mundy, 2013). These authors provided evidence that risk, in the context of sustainability risk for example,was managed by boundary controls in the form established adherence to regulation, codes of conduct, ethics and best practice, as well as guidelines on accepted strategic activities and innovation. These stools were complemented by communicating mission and values of this strategy, in an effort to manage the risk of non-compliance with regulatory directives (Arjaliès & Mundy, 2013). As a result, control tools utilised in strategic and operational boundary systems, are directly associated with managing risks, especially the ones associated with undesirable activities, non-compliance and business conduct.

As was discussed above, formal control tools are utilised by managers at both organisational levels to aid in strategic attainment and formulation. However, at both he strategic and the operational level, informal controls are utilised to offer a different perspective at strategy and strategic goal attainment. Contrary to formal controls, "informal controls are defined as systems that foster an organizational climate through common values, beliefs and traditions that direct the bhavior of group members" (Laguir, 2019, p. 534). Informal processes, the constant free flow of information through all organizational members and departments, and flexibility provided to enhance decision-making effectiveness, make these tools key in fostering interactions between all organisational members. These interactions, in the form of meetings or information exchanges via software and so on, enhance organisational learning and decision-making in strategic goal attainment (Simons, 1995). It is also worth noting that these controls tools can take the form of technical as well as social control tools, depending on the needs and the deliberate design of the organisation (Laguir et al., 2019). These informal systems are less visible and are more likely to be designed in a deliberate fashion by all organisational members, to direct attention to organizational objectives in said members' area of activity (Laguier et al., 2019). At the same time, they are considered to be equally effective to formal systems (Langfield-Smith, 1997; Stacey, 2010).

All four control systems are represented by the middle circle of the diagram in Figure 2.3. The line that connects all four control systems emphasizes the aforementioned synergy of these systems. Indeed, and pointing out on the tension between performance and compliance as discussed above, each control system maybe associated to the controlling of performance and compliance to certain extends. In a sense, when a control system is used for performance purposes, then it can inform about the achievement of target setting in a department and promote accountability for the results of such a department, following the control for compliance. Synergy implies that similarly to the types of controls used in the four aforementioned control systems, because systems are constituted of controls, a tension can be created that requires balance (Simons, 1995) and controls at the strategic performance level can set the level of compliance required to both strategic and operational levels thus working in a complementary but opposing fashion. One control system can inform what other systems needs to control and vice versa at all organizational levels. This concludes the middle and central level of the role and function of the four control systems as revisited by Tessier and Otley (2012, p. 181) based on ideas borrowed from Simons' (1995) initial framework. Indeed, as Tessier & Otley (2012) state, "the revised framework includes all elements of Simons' (1995) original LOC framework, albeit sometimes in a different form".

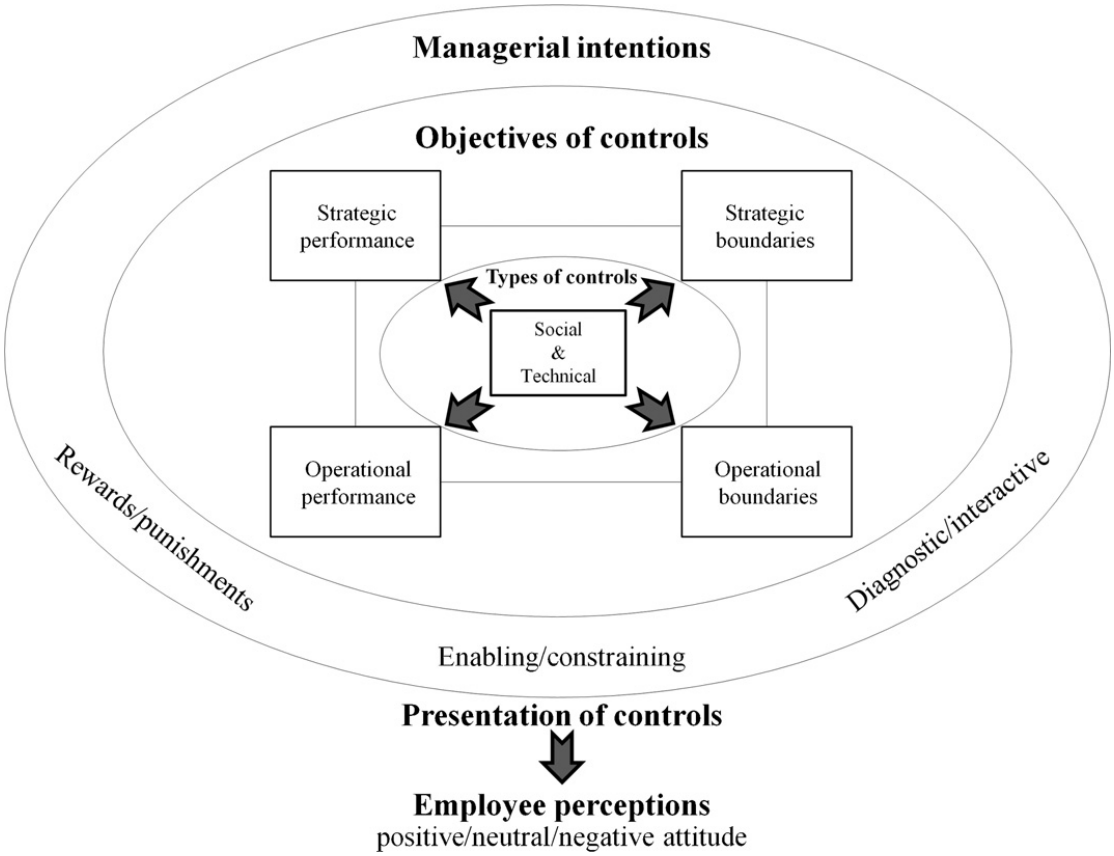


***Figure 2.3**: Revised Levers of Control Framework (Tessier & Otley, 2012, p. 173).*

After the controls have been designed, managers attach their intentions to these systems, and the subsequent controls comprising them, to make use of them. Managers express their intention into two areas. First of all, they choose which controls will be used promoting communication, learning and strategic innovation. Managers also choose which controls will be used to promote the monitoring of critical performance variables and deviances from the intended strategy. In other words, managers choose which controls are intended to be used interactively or diagnostically. Another area that represents the intentions of the managers in the design of control systems is the level of flexibility and predictability they choose to give to their controls. That is, they make a choice of which controls will behave as enabling or constraining controls. Following the consideration of these two intentions, managers also choose which aspects of performance or compliance they will reward or punish as dictated by the use and design of the different control systems. At this stage, tension is also created as some controls can be applied to exude compliance, while enabling organisational learning, or interactively while managing organisational performance. Moreover, rewards and punishments

can also apply to either compliance or performance related controls. That tension is created as a result of managerial decisions imposed upon the use of controls (Tessier & Otley, 2012). Finally, the design phase concludes with the control package being presented and imposed upon the employees. In the attempt of presenting the control package to employees, managers choose various ways of communication and proportions of the control to be presented. This is where there might be a gap between managerial intention and presentation. Tessier & Otley (2012), argue that managers do that because they want to keep their employees focused on specific elements of the systems and its purpose and ignore others that are not directly affecting them or are associated with their activities. In that way, managers "retain some level of flexibility as to how they use controls" (Tessier & Otley, 2012, p. 181). The final circle that encloses the control packages in Figure 2.3, including the aspect of the presentation of controls, is the graphical representation of the control systems as they are designed and used based on managerial intentions. This represents the domain within which managers have an influence upon their control systems, including their presentation choices about them.

The final aspect of the revisited framework has to do with the way employees perceive the controls or control systems imposed upon them and the attitudes they develop towards them when they are getting exposed to them. This has to do with the employee influence on the control systems and its separate consideration in the framework is emphasized by the arrow distinguishing the two areas or influence (i.e. managerial and employee) (Figure 2.3). This distinction is further strengthened by what the authors argue as a dynamic influence of employee's perception and attitudes towards controls. Indeed, the design and presentation of controls is not the only factor that shapes employee perceptions and attitudes. The employees cultural background, their social space and knowledge as well as their level of knowledge about controls will further shape their perceptions (Tessier & Otley, 2012). After this perception is formulated, employees develop a certain attitude towards control systems that can be defined as either positive, or negative and at times neutral. Irrespective of its academic-based usefulness, however, the revisited framework lacks field validity and needs to be tested in a study. What follows is a brief discussion on the insights this management control framework offers to the understanding or risk and uncertainty as they are handled by organizations in light of strategic implementation and innovation, strategic goal attainment and influence of employee behaviour.

3.4 Controlling for risk and uncertainty: usefulness of LoC theoretical components

To answer the research questions, this study will utilise Tessier & Otley's (2012) revised LoC framework. As a starting point, the LoC framework, in both its versions, aims at understanding how managers and organisations design control systems to help with strategy implementation and monitoring (Simons, 1995, Mundy, 2010). In the past, studies have utilised the LoC framework to explore the design, co-existence, balance, and tensions between different control systems, as part of this framework in various contexts (Mundy, 2010; Barros & Ferreira, 2022; Dávila et al. 2023). In brief, tensions refer to the contradictory purpose various control systems serve in a dynamic way, to control for contradicting aspects of strategy (Mundy, 2010), for example what Tessier & Otley (2012) call restraining versus enabling use of controls in their framework. The nature of contemporary risk management adopts the same view, controlling for risk via shielding against uncertain events, while, at the same time, utilising this uncertainty for opportunity-seeking, a dynamic contradiction that is the backbone of Simons' (1995) LoC and prevalent in the revised framework presented in section 3.3. Moreover, and with specific focus on performance measurement systems, the framework has the potential to explain the design and interplay of different control systems, and especially PMS systems and show their role and how these co-exist with other PMS and other control systems (Tuomela, 2005). Conclusively, at an initial level, the LoC framework has the potential to offer a rich conceptualisation of the use, design, and co-existence of controls and control systems in any context and offer insights of how competing elements of strategy can co-exist.

Furthermore, and with specific reference to risk and uncertainty as central concepts in this study, the LOC framework offers some additional prospects. In fact, a number of controls is associated with managing risk and uncertainty. In a clear connection to this study and the key components of contemporary risk management mentioned before, Simons (1995, p. 215) defines uncertainty as "the emerging threats and opportunities that could invalidate the assumptions upon which the current business strategy is based". This uncertainty refers to lack of information in realising current strategies (Widener, 2007). Moreover, risk is defined as "an unexpected event or set of conditions that significantly reduces the ability of managers to implement their intended business strategy" (Simons, 1995, p. 255). Evidently, the LOC framework, not only conceptualises the notions of risk and emergent risk (uncertainty) (Georgiou & Favotto, 2021) but it also shows how control systems are designed with a clear

focus of managing these two elements. In further supporting the discussions of the usefulness of the framework in managing risk and uncertainty, previous studies have supported its applications in the public sector as well. Notions and concepts of the framework have been used in previous studies to show how public sector entities control for risk associated with political regulations compliance (Modell, 2012), joint venture arrangements (Cäker & Siverbo, 2011) and create value (Höglund et al., 2020). Moreover, the framework provides invaluable evidence of the design and use of interactive control systems to manage uncertainty through information exchange, in the public sector context (Kominis & Dudau, 2012). Finally, similar studies have utilised parts of the framework to show how managers use information exchange systems to make sense of strategic uncertainties and how these systems co-exist with other communications channels in the private sector (Lewis et al., 2024). Conclusively, the LoC framework, has the potential to uncover the process by which control systems utilised for public sector risks, especially for managing emergent risks (Georgiou & Favotto, 2021).

Subsequently, as evidenced in this section, the LOC framework, as revised by Tessier & Otley in 2012, has the potential to offer rich conceptual context within which to address the research questions of this study and explore the various conceptual components this study is interested to within these research questions. In fact, previous studies have utilised the framework, mostly in its original form, to provide evidence of the use and practice of control systems, similar to what this study is aiming for. The framework can explore the nature and role of various control systems, unravel assumptions underlying their design and use, and provide insights regarding the role of controls in managing risk and uncertainly in dynamic contexts Following that, the notions of risk and uncertainty and how these are controlled for, is central to the framework (Widener, 2007). And as an additional note, and since contemporary risk management has become strategic (Andersen, 2016), the framework can also provide a clear understanding of how different strategies are controlled by organisations. These strategies vary and include strategies that emerged 2 decades later from Simons' original conceptualisation, for instance corporate social responsibility and sustainability strategies (Gond et al., 2012; Arjaliès & Mundy, 2013).

4 Research design

4.1 Introduction

In this chapter, the research design and its elements are outlined and justified. Section 4.2 outlines the research orientation and methodological assumptions underlying the selected research design. In section 4.3, the research design will be expanded upon by detailed descriptions and justifications. The site of study will then follow. Then, section 4.4 articulates the methods and practical details of data collection, followed by section 4.5 that presents the main data analysis. In this section, the main themes of data analysis will be introduced, which will later be discussed in the findings chapter. Finally, this chapter concludes with some ethical considerations informing this study, and the mechanisms utilised by the researcher to mitigate participant and other ethical risks.

4.2 Research orientation and methodological assumptions.

This study utilises a middle-range methodological approach to address its research questions and provide empirical evidence. A middle-range methodological orientation derives from Middle Range Thinking (Laughlin, 1995, 2004; Broadbent & Laughlin, 2008). This approach assumes that the social world and its nature derives from interpretive constructs and interactions between its social elements that understand and build these constructs. As a result, understanding these social constructs or part of them, cannot rely on a previously tested theory, but at the same time, it can be explained adequately by a theory without the need to build one through an interpretive approach (Broadbent & Laughlin, 2014). That is because accounting phenomena, and especially management control phenomena, are contingent to their situation, context, point in time, organisational needs and, as a social construct, they cannot be fully explained by a given theory (Broadbent & Laughlin, 2009, 2013). Moreover, its philosophical assumptions do not lie to the extremes of positivism/realism or pragmatism and ethnomethodology. A middle-range methodological approach, which reflects the ideas of Middle-Range Thinking (Broadbent & Laughlin, 1997), lies in the middle of the two and suggests that the phenomena under study cannot be completely explained and quantified by numbers, but at the same time, not a new theory is required to conceptualise them. Subsequently, the middle-range methodology suggests that in going into a field to gather

evidence to explain the social constructs of accounting, the researcher needs to pick a "skeletal" theory, that will be eventually "fleshed" out by the empirical evidence (Laughlin, 1995, 2004). To reflect this, the researcher identified a suitable theoretical framework and went into the field with that framework serving as starting point to understand the phenomenon under investigation. That chosen conceptual framework is the Levers of Control (Tessier & Otley, 2012). The purpose of this was to provide empirical evidence of an accounting phenomenon, but not to define it, in respect of its contingencies in providing empirical findings. As such, empirical data gave meaning, or flesh, to the theory and how this applies to the specific context of the study, that is, the context of the public sector. The events, structures and participant perceptions about risk management and the associated controls will be looked through the lens of a theory to ensure evidence robustness (Sutton & Staw, 1995). Subsequently, this theory, Simon's Levers of Control (1995) as revised by Tessier & Otley (2012), will be utilised as a starting point to understand the types and processes of control systems integrated in public sector risk management. This theory is used explore the controls used in the risk management process in the selected organisations, informed by a middle-range methodological approach (Broadbent & Laughlin, 1997; Laughlin, 1995, 2004). This kind of methodology is appropriate in studying accounting phenomena within their context and gaining robust insights for theory and practice (Broadbent & Laughlin, 1997). More details on the design protocols, methodological processes, methods utilised, and data collection and analysis protocols will be given in the sections that follow.

4.3 Research design outline

4.3.1 Research design

To answer the research questions, the current study will employs an interpretative qualitative case study design and orientation to inform data collection and analysis (Baxter & Jack, 2008; Yin, 2014). The main reason behind the choice of such a design, and reflecting on the purpose of the study, is because it offers a rich contextual understanding of processes and procedures of accounting phenomena (Mechant & Van der Stede, 2006; Lee et al., 2007; Parker, 2012), by interacting with actors in their environment at a close distance (Vaivio, 2008). As the author proposes, "in the single case study, the phenomenon of interest is examined in its detailed context, against a rich background of organizational processes, tensions and competing

sectional interests… this provides a plausible, contextually rich explanation of the research phenomenon that has theoretical value (Vaivio, 2008, p. 74), In fact, case studies offer such rich descriptions, that sometimes they can uncover stories and circumstances that may not have existed when initially designing a study (Lee & Humphrey, 2017). Moreover, and in relation to one of the contributions of the study, as discussed in the introduction chapter, a case study is relevant in advancing and refining theories (Vaivio, 2008). As such, the Tessier & Otley (2012) revised LoC theory, being utilised in a case study design, will offer insights on its application and critical evaluation (Vaivio, 2008), which is something Tessier & Otley (2012) suggested as future research. In general, a qualitative design, because it relies on appropriate data and theory to develop accounting concepts, principles and practices (Salmona et al., 2015), it offers avenues to show how accounting practices shape and are shaped by societal members, in an effort to gather empirics to better understand such accounting practices (de Villers et al., 2019). However, qualitative study designs suffer from a few drawbacks. For instance, qualitative accounting research has been criticized for offering low levels of generalisability, validity and reliability (Parker & Northcott, 2016). In fact, and since a qualitative case study design has the need for the researcher to enter the field and experience participant life and environments, rigour and reflexivity are in danger, as they heavily depend on the researcher's analytical and interpretation skills (Parker, 2012). In a similar vein, case studies, and single-case studies, have been criticized for not providing with adequate generalisability and theoretical relevance (Hägg and Hedlund, 1979). To address these issues, and to ensure qualitative case study design rigour, reflexivity, reliability, validity and generalisability, this study will employ a set of criteria. First of all, to address the issue with the validity and reliability of findings, this study will collect data from multiple sources, as it will be shown in the next sections of this chapter (Hoque et al., 2013; Yin, 2014). Moreover, and with specific reference to rigour and reflexivity, all findings will reflect the context studied, and arguments on these will be supported by the evidence drawn (Scapens, 2004). In fact, and to address the issues with the researcher's interpretation skills, clear steps will be taken to initialize, confirm and saturate the data from the participants of the study, following Broadbent & Laughlin's (1997) 3 steps of data collection that inform the middle-range methodological approach. In a nutshell, and as it will be expanded later in this chapter, based on these steps, data collection commences with collecting data from a few key participants and sources of a case study, then these data are confirmed by more participants, and they are later saturated and updated, if

needed, by the researcher's participation and observations in the field. Finally, to ensure generalisability, replicability, and validity, or as Parker & Northcott (2016, p. 1116) coin it "credibility and trustworthiness" in qualitative accounting research, this study's case study approach will follow Parker & Northcott's (2016) criteria in qualitative accounting research. As this study is interested in exploring the processes and practice of the phenomena under study, it will follow a "naturalistic generalising" direction (Parker & Northcott, 2016, p. 1114), that aims at uncovering "social forms, processes or meanings". This mode of generalising will be realised against the following criteria:

1. Sampling and case selection: "purposive sampling" to select a case that provides in-depth analysis of the phenomenon under study that has specific characteristics relating to such phenomenon (Parker & Northcott, 2016, p. 1116). The authors call this the "typical case" that offers an abundance of practical considerations that can be later picked up by future researchers, and policymakers. In doing so, clear cases of analysis need to be identified (Cooper & Morgan, 2008).
2. Field participation: To ensure credible results, the researcher needs to be part of the field, as it is the case for this study (Lukka & Modell, 2010).
3. Thick description of findings: the need to "understand and portray how and why actions take place the way they do, the processes and mechanisms involved and to understand how they occur in particular settings, including assessing the lived experiences of actors" when engaging in field work (Parker & Northcott, 2016, p. 1117). Interpretation of findings should also follow a set of criteria, for example, based on theory and themes (Cooper & Morgan, 2008).
4. Multiple sources of data: to enhance generalisability, the researcher should employ a variety of data sources that complement each other (Parker & Northcott, 2016).

These criteria will be later expanded upon in the methodological choices of this chapter, to show adherence.

It is also worth mentioning that a case study design is also helpful in bringing forth the similarities (literal replication) and differences (theoretical replication) of a studied phenomenon in its context, as this is reflected in the "concrete manifestation of the cases" (Yin, 2014, p. 136). Therefore, a case study is relevant to study a phenomenon in its context and

when this context possesses different logics of this phenomenon. Indeed, the phenomenon of management control as part of the risk management process in the public sector follows the same logic. As mentioned before, the way risk management is adopted, implemented, facilitated and practiced in various public sector entities around the world varies with context, external environment, regulatory oversight, expertise and politics for each public sector organisation, as well as their expectation on reaping the benefits from the adoption (Woods, 2009, 2010; Rocher, 2011; Collier & Woods, 2012; Palermo, 2014). Therefore, to enrich findings and cover all the possible theoretical propositions of this study, the most appropriate design would be a case study design. That is something that is required in management control for risk management research, to advance knowledge on practice (Bracci et al., 2022).

4.3.2 The case organisation

For this study, a single case study design investigating organisational practices in their context was selected (Stake, 1994; Yin, 2018). To select the case, a purposive qualitative sampling was executed with the aim to provide in-depth information about the phenomenon under study (Parker & Northcott, 2016). Indeed, since this study is interested in unravelling a rich description of the phenomenon of controlling for risk management, the researcher is interested in selecting a rich case setting, with a variety of sources of data, to produce rich results (Fossey et al., 2002). This exploratory approach has been advocated for accounting research (Parker et al., 1998; Malina et al., 2011) and has been applied into different accounting contexts (Anderson & Guilding, 2006). For all these reasons, a case organisation was selected for this study, that is a public sector organisation based in Greece. The primary reason for selecting this organization was its extensive use of management control systems, many of which are directly linked to risk management in daily operations (Gomm et al., 2000; Cooper & Morgan, 2008). Moreover, they also have a very sophisticated and complex risk management system, advocated by a risk management took that they have majorly developed and running themselves. These systems are responsible for helping the organisation with their responsibilities in managing and monitoring European Commission funds that are given to Greece to develop various infrastructures, specifically relating to transportation and the environment. Effectively, this organisation is responsible for managing and monitoring European Commission (EC) funds that are given to Greece to develop various types of infrastructures, mostly related to transportation and the environment. The funds derive from

the well-known Partnership Agreement for the Development Framework (PADF) that the European Commission runs every 7 years and utilises European Union funds, given to country members, to implement various infrastructural developments in their countries, which is part of the wider European Regional Development fund (European Commission, 2014). The funds for the 2014-2020 programme period that the case organisation managed, were 4.7 billion euros.

These developments have to do with modern transportation infrastructure, environmental and sustainability projects, projects for developing entrepreneurship, and projects to reduce unemployment, among others. Effectively, these funds are utilised for the development, prosperity, and modernisation of the country-members of the European Union. These funds are given to each country-member and are managed by relevant managing authorities, that are responsible for managing projects utilising these funds, in a respective area, for example, transportation infrastructure. Indeed, the case managing authority (MA) is working with various beneficiaries around Greece that eventually receive those funds, to materialise projects for road and railroad networks, airfields and ports, subways, and various projects to promote the environment and sustainability. In essence, the organisation is the managing authority of these funds, and this term will be used to refer to the case organisation from now on. Transportation projects are considered mega projects, while environmental and sustainability ones are considered of smaller capacity. Mega projects are classified as projects with a budget of over 50 million euros. The organisation has classified all projects as “praxis” or “ergo” and they are operating with a file for each of these, that includes all related contracts required to complete this “praxis” or “ergo” projects. We will refer to these as “projects” from now on. The way the materialisation process works is that the MA receives the funds from the European Union and then engages into a competition process to select suitable organisation from both the private and the public sector, to materialise these projects. Projects are advertised, beneficiaries apply, and if they meet specific criteria, after assessment, they are assigned the projects and they are allocated funds, via specific procedures, and in every stage of the project. Once project assignment is completed, each project is given to specific operators from the case organisation, to monitor their materialisation, from the initial stage to project completion. In essence, the organisation is the managing authority of these funds, and this term will be used to refer to the case organisation from now on. For the materialisation of all these projects,

European Commission funds are utilised, that are targeted at specific infrastructure based on the European Commission needs and these funds are running into rounds that the European Union calls programmes (European Commission, 2014). The projects for each funding period last from a few months to 7 years, which is effectively the completion period of each project. To account for delays, some projects may be given an extension for a maximum of 3 years after the funding programme ends. If a project is not completed within this timeline, the funds are either returned to the European Commission or are not given at all. During the period of the data collection, the organisation was managing funds from PADF 2014-2020 programme period and was trying to finalise projects for that period with a final deadline of December 2023. As such, data were collected for this period and not the new one, that of 2021-2027 that they were also preparing for at the point of data collection and was not in full effect yet or fully realised in terms of systems, regulation, funding or other procedures. The managing authority is also monitored by a Special Regulatory Support Agency (SRSA) in Greece, that overlooks all organisations that manage European Commission funds, like the case organisation, and the Greek Ministry of Development and Investments (for the 2014-2020 programme period). The purpose of the SRSA is to monitor legal, regulatory and other compliances of managing authorities, and to develop and monitor various governance systems for the same managing authorities.

The managing authority is divided into units that are responsible for managing funds and the organisation itself (Figure 3.4). Indeed, "Alpha" unit, is responsible for assessing and integrating projects for the two categories mentioned above: transportation and environment and sustainability. Each segment has its own Unit Alpha sub-unit. Effectively, there is a Unit Alpha that supervises one sub-unit Alpha for the transportation and one sub-unit Alpha for the environment and sustainability segments. After projects have been integrated into the programme, that is have met all the criteria to be funded from the EC funds, unit Alpha proceeds into integrating the projects under the organisation's supervision. At this point, the various units called Beta come into play, and they are given responsibility to monitor the accepted/integrated projects and the fund allocation. These units can be assigned many projects at the same time and are divided into 3 sub-units each, that are responsible for the materialisation of specific projects, based on structure and expertise. For instance, there is a different Beta unit for railroads, a different one for subways and a different Beta unit for

environmental projects. Each segment (transportation and environment and sustainability) has a divisional structure. In essence, Beta units are making sure that funds are used to complete the agreed projects that have been integrated by unit Alpha, in both transportation and the environment. Finally, the organisation has unit Gamma that is responsible for managing the organisation and its needs, including work support, human resource management, accounting and finance, regulatory compliance and all other supporting activities. Unit Gamma is effectively responsible for making sure all other units have what they need to complete their activities successfully and effectively. All these units are overlooked by their own supervisors, which are then supervised by a director for each segment. All of these are supervised by the director of the MA which is accountable to the ministry representative at each point in time (based on the one assigned by elections). At the heart of this structure, lies the risk management team that brings together representatives from all units and communicates information on risk and emergent risk to the senior management level, e.g. the director, to assist with programme and MA decision-making. As a result, the risk management team applies to all parts of the organisation, as it brings together everyone in the MA to discuss and manage risk, emergent risks, and operate their risk management tool. More information of how this team operates, will be provided in the finding section of the thesis. All this can be seen in Figure 3.4.

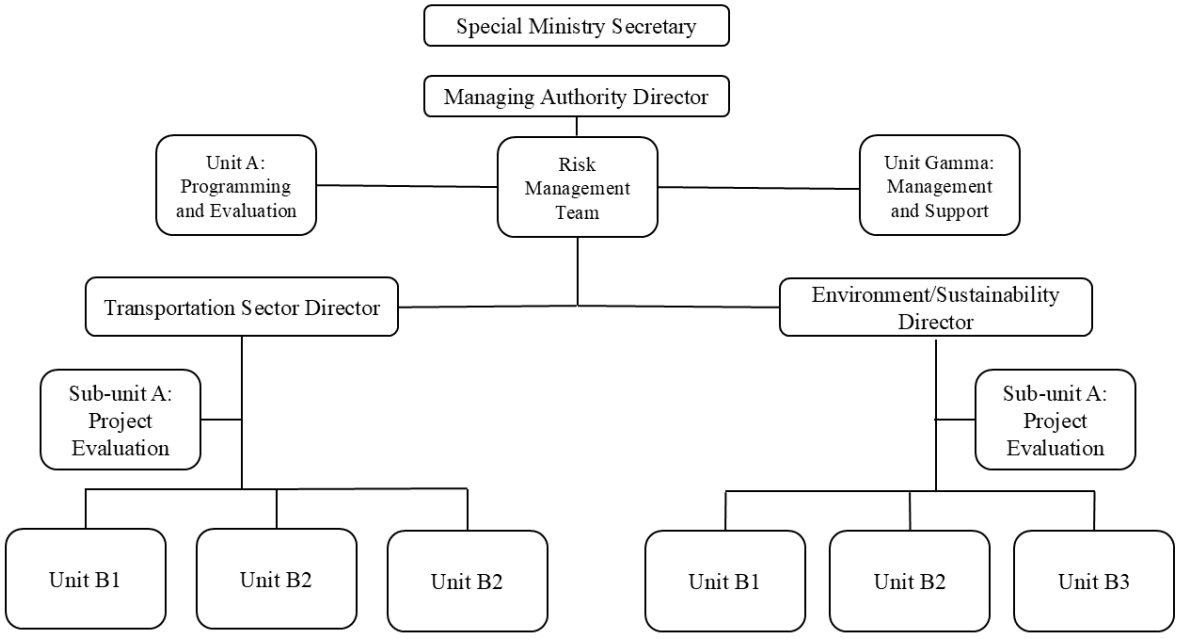


Figure 3.4 *Case study structure*

In managing all those projects, and the organisation itself, the MA, has developed a clear and sophisticated risk management system, reflected on a single risk management tool. That tool delineates the risks and uncertainties, the MA is exposed to, the domain from which these risks manifest and the organisational attention that each risk needs to be adhered to. In fact, and in communication with the European Commission and regulators, the case organisation has developed a system of categorising and ranking those risks. Moreover, this risk management tool has been designed to fit appropriately with other procedures and control systems within the organisation. There is also a specific risk management team that has been created to manage risk and uncertainty within the case MA. This team is associated with all organisation levels, and, at the same time, this team consists of representative from all organisational units. These members are there to represent their units and communicate unit risks and emergent risks, and they help communicate all relevant risks through the organisation. As a result, risk management and monitoring are done with the collaboration of all units. If changes are needed, for example due to a new regulation development, or due to a new development in a set of projects that was not identified before, this team communicates all changes to the units via their representatives. For instance, as a general indication, when risks are changing, either their nature, ranking or impact, the risk management tool, communicates these changes into the organisation to implement appropriate procedures and rules, where appropriate. Detailed information on this tool will be provided in the findings section.

4.4 Research methodology and methods

4.4.1 Research methods

Single case studies can provide generalisable findings (Yin, 2014). However, as mentioned before, it has been suggested that qualitative research in accounting, and case studies as well, have issues with low levels of generalisability (Parker, 2012). To enhance generalisability of findings and also adhere to the sampling direction that this study has taken, rich and varied sources of evidence were utilised (Parker & Northcott, 2016). In fact, and to collect these data, a mix of interviews, focus groups, observations and documentation analysis were utilised. Data were collected from July 2022 until October 2023. As per the methodology and to ensure generalisability (Parker & Northcott, 2016), all relevant participants that worked, participated and managed risk management tools, process and procedures, and also worked with various

projects, internal mechanisms and regulation, were identified in terms of sampling. All participants interviewed from the case organisation and the beneficiaries and SRSA were covering a significant sample to ensure data saturation (Dai et al., 2019; Hennink & Kaiser, 2022). For example, interviews and focus groups were conducted with all members of the risk management team of the organisation, who, at the same time, were representatives of all units of the organisation and they were aware of the processes and procedures, as well as attitudes towards these, from their units. At the same time, the SRSA representative was the head of supervision on all MA regulations and when this participant was asked for more contacts within the SRSA, she indicated that the researcher would hear the same information. Moreover, participants from the beneficiaries covered 3 out of 4 beneficiary organisations. Moreover, to further ensure data saturation and check that no more data were needed, the researcher engaged in coding, at third-order level, to check the data to see if there were any more codes or themes emerging. Indeed, after the last interviews with the gatekeepers and the director, no more new codes or themes emerged, which strengthened data saturation (Hennink & Kaiser, 2022).

To provide more transparency about the process of data collection, the whole process started with identifying the case organisation and initiating first contact with the QAO as they had some publicly available information for that. The QAO was then interested in this study, and we arranged an initial, unofficial meeting to discuss the study further and see options for data collection. After the meeting, they QAO expressed their interest and agreed to discuss this with the CRO, which was keen to arrange a single meeting with both to commence the study. Thus, in July 2022, the first meeting and interview with the two gatekeepers took place. At the same meeting, the gatekeepers provided the researcher with the main documents the organisation is utilising, that is the Risk Management Tool document and a list of MCS links that lead to the whole set of MCS documents and procedures as they appear in EC and Greek Government publicly available online domain and are utilised by the MA. These documents where analysed and served as naib discussion points at later stages. The CRO was then the facilitator of the rest of the process, as they engaged with their colleagues from the risk management team to initiate the first focus group, in September 2022, to present the study to the rest of the risk management team members and collect their initial input and ideas on the matter. At this stage, no other documents were collected, and the researcher made note of initial themes to be discussed later with all participants. After the initial focus group with all the participants, QAO and CRO

included, the data collection process continued with each participant invited to an individual meeting, to further discuss the risk management and control tools associated with their organisation and space of responsibility. If there were more than one participant in a team, such as the fraud risk management team, then a focus group was utilised. At this point, interviews and focus groups were intertwined with all the MA's participants. In these meetings, the collection of further relevant documents was conducted. At the same time, the elements of the risk management tool and MCS were further confirmed. As it will be further discussed in the observations section, within these initial interviews and focus groups, the researcher observed the operation of various systems such as the MCS, the Action Plan, the IIS via Zoom screen share on behalf of the participants. Relevant documents were also shared on these, were appropriate. Once a participant offered any of the above, data from documents and observations were analysed to be utilised in the next interviews. As a result, as data collection as going forward, data from one participant served as a starting point to engage into a conversation with the next participant. That was done to make sense of the whole risk management process and to also bring the research instrument at its final form. This process lasted until December 2022 Once participants started to be pilling up and more details were provided on the processes of the materialisation of projects, the researcher focused their attention on collecting data from the main organisations that materialise the MA's projects, that is, the beneficiaries. At this stage, the CRO was kind enough to share contact information for the MA's main beneficiaries for transportation projects. Due to the nature of the beneficiaries, no participants could be selected from the environment and sustainability area. The beneficiary contacts where then emailed and asked to participate in the study, many of which agreed to, via their representatives in key risk management positions. That happened in January 2023. Gathering data from beneficiaries was challenging at this stage, as they were experiencing high workloads and were not available on demand. The first interviews started in February 2023. At this stage, an interview was conducted with one beneficiary, with conversations on how how beneficiaries manage projects, as well as how this feeds back as a process or information to the MA. As more interviews and focus groups were conducted, that emerged as the main focus of discussion. During these interviews, and focus groups, where representatives were more than two, documents were shared, and procedures were showed that were relevant to managing project risk in conjunction with the case MA. For example, two participants from two large beneficiaries in Greece, offered guidance and documents to show how different regulation

applies managing and materialising transportation projects via utilising EC funds. Another participant indicated the process by which communication happens with the MA, via showing emails of how this happens on a continuous basis. At the same time, the researcher was going back and forth to beneficiaries and MA participants to finalise the data collection and check if any more participants were required to be utilised for data collection purposes. This process lasted until May 2023. Finally, to wrap up the whole process, and to confirm all information from previous data, a final focus group with the gatekeeps was conducted during the summer of 2023. This focus group served as a follow-up on questions not asked in the initial gatekeeper interview, due to the maturity of the data collection instrument at the time. At this focus group, the CRO offered additional information on risk management elements, such as team communications for various project elements, such as information shared with director and the relevant overlooking bodies, via sharing emails of conversations. At the same time, and as a last final interview, the researcher interviewed the director of the MA. This interview was done to confirm the process of risk management and management control at the strategic level, and it was impossible to do so at an earlier stage, as the director was just appointed a few months before that time. Conclusively, the data collection process was not a step-by-step sequence. The researcher collected and analysed data in various forms and avenues throughout the whole process of data collection. Initial data analysed from the first round of interviews with the MA participants, served as the basis of questions and discussion to the next interviews, and documents shared, or procedures observed, were confirmed with later participants. The same applied to discussion with beneficiaries.

4.4.2 Interviews

A total of 28 participants were asked to participate in this study. From these, only 21 ended up participating, due to workload reasons, which is consistent with the average participants to ensure data saturation, on top of the sampling elements that were discussed in the previous sub-section (Dai et al., 2019). From the case organisation, 15 participants were recruited, 12 from the risk management team, 1 from HR and 2 from the fraud team, and the director of the organisation. The other 5 were members of beneficiaries and 1 participant served as the representative of the SRSA. That sums up a total of 21 participants from the case MA, and other beneficiaries or overlooking bodies. More information on the particulars of the participants can be seen in Appendix 5 and 6. At an initial stage, participants were recruited

using their email address, which was found online, at the website of the organisation. However, this was done after initiating the study, via gatekeepers. To initiate the data collection, an interview with the chief risk officer (CRO) and the chief quality officer (QAO) were conducted, who were both members of the risk management team at the period of the study. These two participants served as the initial gatekeepers that helped secure access to the rest of the participants in this study. In these initial interviews, we discussed the purpose of the study, its parameters, and possible benefit for the organisation. Since these two participants were interested, they opened the gates to the rest of their team, by suggesting more participants, via a mass email, and also initiating the original focus group in September 2022. As a result, the study was communicated to more people, which were later recruited after they expressed interest. A total of 14 participants were interviewed after that. The gatekeepers were later kind enough to point the researcher to the direction of representatives from the beneficiaries and these were asked to participate in the study. As a result, 5 participants from 3 large beneficiaries participated in the study, 3 of which were interviewed and the other two were asked to join a focus group, representing 3 out of 4 main beneficiaries in transportation infrastructure. No beneficiaries from the environment and sustainable projects were interviewed, as the operators who monitor these projects were found adequate to provide information. That is because these beneficiaries do not have the knowledge and expertise to provide insights. Then, the SRSA director was also interviewed, to offer insights on the regulatory supervision of the case organisation, and any systems that they monitor that the case organisation has in place. Finally, in October 2023, the director of the organisation was interviewed. Subsequently, a total of 20 interviews, ranging from 30 minutes to 1 hour and 30 minutes, were conducted during the period of the study, with all these participants. All interviews were recorded.

The interview questions utilised in this study can be found in Appendix 2. These interview questions served as the basis of interviewing beneficiary participants as well, in a more open-ended fashion, to confirm the way their systems work and relate to the case organisation. It is also worth noting that these questions emerged after pilot interviews with the gatekeepers and the big focus group with all members of the risk management team. That was done to reflect the research questions better, and the context of the study, for better targeted questions. All interviews were conducted online via Zoom and were recorded and kept safe at the researcher's password protected University of Glasgow account. To ensure anonymity, all participants were

referred to as either with their main role, or with their main position or role in the unit they represented. For example, the chief risk officer, or a member of Unit Alpha, Beta or Gamma. In the case of beneficiaries, these were referred to as members of a specific beneficiary. All participants were provided with a participant information sheet and signed an informed consent.

4.4.3 Focus groups

Some of the participants, either because they did not want to participate alone, or because they were members of the same team, requested to provide their insights via focus groups. A total of 4 focus groups were conducted from September 2022, until May 2023. In these focus groups, a total of 21 participants participated, many of which were later interviewed individually or in smaller focus groups. To make matters clearer, the first focus group took place in July 2022, with the two gatekeepers, the chief risk officer and the chief quality officer. This initial focus group ignited the second big focus group with 7 participants from the case organisation, that was requested by the chief risk officer, to inform about the purpose and elements of the study and give chance to participants to express interest in participating in interviews. As such, a total of 7 participants were involved in the second focus group, which they all later ended up providing insights in individual interviews. One more focus group was conducted with the fraud risk team, which consisted of 2 participants, and one final focus group with the two gatekeepers, in October 2022 and July 2023 subsequently. Finally, 2 more participants participated in one focus group in February 2023, from one of the beneficiaries that construct subway infrastructure.

The focus group questions utilised in this study can be found in Appendix 2. These interview questions served as the basis of interviewing beneficiary participants as well, in a more open-ended fashion, to confirm the way their systems work and relate to the case organisation. All focus were conducted online via Zoom and were recorded and kept safe at the researcher's password protected University of Glasgow account. To ensure anonymity, all participants were referred to as either with their main role, or with their main position or role in the unit they represented. For example, the chief risk officer, or a member of Unit Alpha, Beta or Gamma. In the case of beneficiaries, these were referred to as members of a specific beneficiary. All

participants were provided with a participant information sheet and signed an informed consent. All focus groups were recorded.

4.4.4 Documentation analysis

The researcher identified all relevant documents that matched the study requirements and evidence needs (Bowen 2009). Initially, the case MA documents were collected, as the researcher was given access to these documents by the 2 gatekeepers. Then, as data collection unravelled, the researcher identified more documents and was also given access to others via various participants. Most of the PADF and EC documents were found online, if not provided by participants. A total of approximately 30 documents, totalling approximately 1580 pages, were identified and were included in the study. These documents included policies and procedures, the main management control systems of the organisation, regulatory and relevant law documents, organisational structure documents, and documents relating to policies and procedures from the PADF framework. Moreover, email correspondence was also fed as part of these documents, especially emails relating to correspondence from the CRO to the director and vice versa. However, these emails were mostly as part of the interview, they relate more to observations during the interview, and that is why the final document tally is approximate. After the documents were collected, they were scanned and analysed by the researcher to ensure authenticity, credibility, representativeness and meaning, always in line with the purpose of the study (Kridel, 2015). Respectively, to check that the documents were genuine, the researcher confirmed their credibility in the online sources to be formal and matching the organisations under study and confirmed all authenticity through oral participant confirmation or because they were sent to the researcher by the study's participants. The same process applied to ensure documentation credibility. Afterwards, to ensure the documents are representative of the phenomenon under study, the researcher selected all documents that were directly or indirectly connected with managing risk, its processes and regulation, as well as its conceptualisation within the organisation. Some documents matched risk management but were associated with other organisations and not the case study. As such, they were discarded. Finally, to ensure that the meaning of the documents was clear and understandable (Morgan, 2022), the content of all documents was discussed and confirmed by all participants, during both interviews and focus groups.

4.4.5 Observations

On top of interviews, focus groups and documents, the researcher also observed many processes and procedures in the organisation, related to managing risk or related to elements indirectly associated with risk management. For instance, at the beginning of the study, and specifically a few weeks after the focus group, the researcher took part as an observer in the annual risk management meeting of the risk management team, in October 2023. This meeting lasted for 1 hour and 3 minutes. In there, valuable insights were gathered as to what these participants discussed, and what is the purpose and content of this meeting of the risk management team. However, only this meeting was possible to observe, as the risk management team, due to workload mainly and the hectic time at the end of the programme period, did not manage to have another one. As a result, this meeting's contents and procedures, were later confirmed in the interviews and focus groups. Additional observations also occurred during the interviews and focus groups. For instance, during 4 of the interviews, the researcher was able to see how different policies work, and how different systems in the organisation work. In 3 the interviews with participants from the case organisation, the researcher was able to observe different mapping and oracle procedures that the case organisation, including elements of the overarching rule system of the organisation. These observations, due to the nature of data collection, occurred via Zoom screen share on behalf of the participants. For example, in an initial interview with an operator from transportation, a screen was shared to show input on the IIS. The participant shared their screen and logged in to the IIS system, specifically the fund absorption tables of the IIS, for every project they were managing. This vast set of tabs and tables showed information about fund absorption of projects, and the participant specifically filtered their projects. For these projects, a new tab was selected to show project maturity, completion, fund absorption and additional notes, as well as key attention areas that the participant needs to focus on. Effectively, this information shows the risk of non-completion for each project and was broken down into key project areas. In the notes, information was shared with beneficiaries, regarding the particulars of each project and the observation showed the tabs and notes of how this information was conveyed. That visualised how risk information, or information on emergent risks, is shared through the IIS to reflect the MCS, the communication of important project elements (and by extension, risks) via the IIS and how operators materialised the projects step-by-step, relying on information from the IIS

to make decisions to avoid or manage said risks. The observation showed how key information was included and communicated or visualised to the participants, from various project elements. In another interview, at the initial stage, a participant shared their screen to show a part of the Action Plan, a vast excel file, and the fields where each project was included, as well as its maturity and fund absorption state. In there, projects were flagged when their completion was of high risk to not be completed. Moreover, in the focus group with the fraud risk management team, a brief explanation was provided as to how fraud information flows from the public to the MA. The 2 participants shared a link via the Zoom chat box, and guided the researcher, while discussing the process, as to what steps can be followed, for anyone from the public, to report a fraud instance to the MA, relating to one of its projects. In another example, the SRSA participant was able to share slides and policy procedures related to the case organisation, including the risk management tool's initial conception. Via Zoom screen share again, the researcher was able to see policy procedures and how they worked on the initial stage of the formulation of the risk management tool, within the MCS, while describing the initial stages and misconceptions that occurred prior to its application. Finally, the beneficiaries also shared valuable details of their rules and procedures that they follow. In 1 focus group with one of the beneficiaries, emails and other correspondence was shared to check communication procedures with the case organisation. In there, it was visualised what information was important and how it was conveyed, usually in an unofficial manner, to the case MA, to trigger a discussion on project completion or stage action. The beneficiaries also shared laws and regulations, and sometimes, their own procedures, that showed how they work. For example, one beneficiary responsible of constructing road networks with EC funds, shared and commented on elements on a set of documents via Zoom, indicating their quality assurance system and how this works in materialising projects, with clear communication stages with the MA. Another participant from another beneficiary also shared elements and excerpts from law documents and discussed how all these apply to their organisation, and by extension, to the materialisation of projects overlooked by the case MA. All observations were conducted via Zoom, and any notes required were taken separately, or as part of the interview and focus group transcripts. These notes and transcripts were later checked to remove any identifiers.

4.4.6 Research methodology and data collection execution

Following the case study design approach, and the middle-range thinking methodology and generalisability assumptions mentioned previously in this chapter, a set of specific steps were followed in executing said methodology, as indicated in section 4.3.1. As Broadbent & Laughlin (1997, p. 627) suggest, the first step of this methodology is to develop "critical theorems" or the initial understanding of the case organisation, its background, and contextual considerations. For that reason, 2 semi-structured interviews were conducted with the 2 gatekeepers from the case organisation in July 2022. The purpose of identifying gatekeepers was to unlock access and availability to the rest of the organisation, especially in case of interest in the study (Parker et al., 1998). As discussed in the previous section, these gatekeepers were actually the Chief Risk Officer of the organisation, and the second gatekeeper was the Chief Quality Officer of the organisation. After these interviews, there was a focus group with 7 participants, including the CRO and QAO, that formed the risk management team of the organisation (some of them were absent due to work-related responsibilities, but were interviewed later on). The purpose of the interviews was to establish the context, operation, environment, and nature of services for the case organisation and to inform participants about the study. The researcher also wanted to confirm a set of publicly available documents that were found describing the case organisation. Moreover, participant observation occurred at one of the annual risk management meetings of the risk management team of the case organisation, where the researcher was allowed to participate and take notes. At this stage, the researcher used the LOC framework as a lens to understand processes and procedures, especially related to risk management, that applied to the case organisation. Semi-structured questions were used in both the initial interviews and focus groups, to establish an appropriate picture of how risk is managed, and how participants perceive it, at an initial stage.

Once the critical theorems were established, the researcher sought to test and confirm them through understanding participant perceptions on the processes associated with managing risk (Broadbent & Laughlin, 1997). Significant help was offered by the gatekeepers who provided valuable support in snowballing participants for interviews and focus groups throughout the organisation and affiliated organisations. As such, the researcher went over to conduct semi-

structured interviews with the rest of the participants of the risk management team, each of them being a member and a risk representative of every unit of the organisation. To ensure critical theorems are accurate and that they reflect participant perceptions, interview questions were revised from time to time, until their final version (Appendix 2). During interviews, some participants offered observation insights on how various IT systems and risk management processes and procedures operated. The participants often pointed out contacts and affiliates to beneficiaries that actually receive EC funds to materialise projects. Therefore, after half of the risk management team was interviewed, the researcher conducted semi-structured interviews and focus groups with participants from various beneficiary organisations as indicated in the beginning of this section. Critical theorems were confirmed by February 2023. As a way to close the data collection and conclude the study, in October 2023, a final focus group with the gatekeepers and a semi-structured interview with the Director of the organisation were conducted. Moreover, throughout the whole process of interviews, observations and focus groups, the researcher analysed documents relevant to the organisation and its procedures.

Finally, and following both the assumptions of middle-range methodology in providing multiple sources of data and to ensure credibility (validity of results) as a means to further enhance generalising, or in other words reaching robust conclusions (Parker & Northcott, 2016), the study also adopted a multi-voice approach to disseminating findings. Indeed, the findings of the study, were initially discussed by the researcher and its supervisors, following all research question and theoretical considerations. Furthermore, the researcher itself discussed the findings with the research participants constantly and especially the gatekeepers. For that matter, the final focus group with the gatekeepers involved presenting some preliminary findings of the study. Finally, the study results were presented to the participants in the form of a report and discussed with them. The researcher also received and collated feedback from various doctoral colloquiums, doctoral symposiums, and conferences throughout the execution of the research, and especially after findings were analysed.

4.5 Data analysis

Data for this study were analysed thematically (Braun & Clarke, 2023). Specifically, primary data from interviews, focus groups and observation notes were transcribed, analysed and themes were extracted from them. Secondary data from the documentation analysis were

subsequently analysed and fed into the ongoing thematic analysis process To analyse all the data that derived from all these sources, and identify overarching themes, the NVivo software was used.

All interviews and focus groups, upon participant consent, were recorded. The same applied to observations, however, the researcher was also allowed to take notes. These recordings were later transcribed to a word document each and fed to the data analysis software. The same applied to the observation notes.

To analyse the transcripts and produce data, the main steps of qualitative thematic analysis proposed by Braun & Clarke, 2006 were followed. The first step involved the researcher reading and re-reading the data, and noting down initial ideas, specially connected to the next steps of the thematic analysis, and the methodological considerations of the study. At this stage, the main critical theorems of the study were created, that later informed the themes of the data analysis (Broadbent & Laughlin, 1997). For that matter, and since the original interview and focus group questions were revised, initial interviews served as a starting point to realise these initial ideas. As such, the researcher followed the transcribe-as-you-go approach to establish ideas and directions of data, clearly connected to middle-range methodology and the underlying theory. Indeed, the first interviews and focus groups were transcribed directly after they occurred, to relate to research questions, theory and data requirements, and ensure subsequent interviews were revised to be appropriate. The second step involved an initial coding of the data at a first-order level. The researcher identified the initial codes as illustrated in Table 2.4 (Broadbent & Laughlin, 1997).

4.5.1 Development of codes

Project nature (main code): • Project nature • Project processes	This code was developed to group the main nature, components and characteristics of the projects the case organisation monitors and

• Targets	manages, as well as their main targets upon completion, to gain an initial idea of the nature of the organisation.
Risk management (main code): • Action Plan • Changes • Issued • Procedures • Total Quality Management • Uncertainty Management • ISS (integrated information system) • Management Control System	This code was developed to group the main constituencies of how the case organisation manages risk. That was aimed to gain an initial idea of how project and their risks, are fed into systems of the organisations to be understood and managed.
Risks (main code): • Organisational risks • Programme risks • Project risks • Uncertainty • Other risks	Following the first code in this table, this code grouped the main risks and uncertainties that the organisation is exposed to, that are either directly or indirectly connected with their projects and main operations.

Table 2.4: First-order coding codes

Following the generation of first-order coding, that aimed to develop an initial understanding of the data (Braun & Clarke, 2006), a second-order coding was developed, with an aim at putting all data into the perspective of risk management, risk controls, and the association between these and other control systems within the organisation. These codes are illustrated in Table 3.4.

Managing project risk	The purpose of all the categories on the left, was to group all relevant procedures of risk
Managing internal organisational risks	

Managing other risks	management as to how they are used to manage the various organisation risks and also clearly define and distinguish the systems, specifically control systems, that are outside of the scope of managing risks but are required to answer some specific research questions of this study.
Managing programme risks	
Managing other risks	
Managing other risks aspects	
Other control systems	

Table 3.4: Second-order coding codes.

Finally, and to reflect the theory and the theoretical considerations of the study, a final coding round was performed (Braun & Clarke, 2023). Codes were developed in reflection of Tessier & Otley's (2012) Levers of Control typology. These codes are presented in table 4.4. The codes are explicitly draw upon the 4 typologies of control systems as presented in chapter 2 of this thesis, including the concept of employee perceptions.

Operational Boundaries	Included elements in the transcripts of how control systems were used to delineate the acceptable domain of operations and risk and risk management, at the operational level, and included boundary controls that were not associated with risk per se.
Operational Performance	Included elements in the transcripts of how control systems were used to manage risk performance, at the operational level, and included performance controls that were not associated with risk per se.
Strategic Boundaries	Included elements in the transcripts of how control systems were used to delineate the

	acceptable domain of operations and risk and risk management, at the strategic level, and included boundary controls that were not associated with risk per se.
Strategic Performance	Included elements in the transcripts of how control systems were used to manage risk performance, at the strategic level, and included performance controls that were not associated with risk per se.
Employee Perception	All elements of how all MA employees perceived the systems in the previous parts of this table. This was backed up by perceptions from beneficiaries.

Table 4.4: Third-order coding codes.

Upon completion of coded and finalisation of the initial understanding of the data and their meanings (Braun & Clarke, 2006), the researcher went over all empirical materials to identify and review themes in the data. That was done with the creation of the initial thematic map, that was based majorly on the third-order coding and through utilising one of NVivo's function of cross-tabulating and cross-referencing codes. After all, most data in all codes were the same, but their connection were not yet clearly identified. The themes informing this study were initially brainstormed and later collated in a refined form, which is presented in Table 5.4.

4.5.2 Development of themes

Theme	**Description**

Strategy and risk at case study operations	Describes the main risk and uncertainty elements the organisation is exposed to, including the regulation that it adheres to.
Performance management: overarching performance management tools and risk integration.	Describes the main performance management tools in the case organisation and the way risk and uncertainty are integrated in terms of managing organisational performance. It includes elements of performance management at both strategic and operational levels.
Overarching management control system and risk integration	Describes the main control systems utilised by the case organisation and how these are integrating the notions of managing risk and uncertainty. It includes all control, as per Tessier & Otley (2012), that interact in the case organisation and complement performance management systems, to form the wider control framework of the case study.

Table 5.4: Final data themes

The final step of the thematic analysis was to present a report of the findings based on the data and deriving from undertaking the thematic analysis (Braun & Clarke, 2006), as it can be seen in Table 4.4. This report will be provided in the next chapter, where findings are presented. On a final note, and to adhere to the final criteria of Parker & Northcott (2016, p. 1117) on enhancing generalisability and credibility in findings, the study employed a rich description in data collection, analysis and presentation of findings. The two formers will be analysed here

and will be further supported by the findings section later one. As a result, for this study, data were collected and presented with an "underlying intention to understand and portray how and why actions take place the way they do, the processes and mechanisms involved and to understand how they occur in particular settings, including assessing the lived experience of the actors" (Parker & Northcott, 2016, p. 1117).

4.6 Ethical considerations

To collect data for this study, as indicated in the previous sections of the research design, participants were recruited. As a result, there was some risk involved. To minimise this risk, a few mechanisms were put in place. However, before unpacking this, it needs to be noted that this study was of low risk overall, majorly due to its nature. The data collected were only associated with specific risk management tools, that were associated with internal organisational procedures, without any connection to sensitive or personal organisational data. The people associated with these tools and procedures, are part of a wide network of participants within the Greek public sector and, together with the measures to be mentioned later on in this section, are hard to identify. Moreover, the researcher, during the data collection and contact with the study's participants, discussed and identified sensitive issues that were noted down and deleted from transcripts and any data sources. Finally, the only personal data that were used for this study was the participant contact details, for instance their names, positions and email or organisation phone numbers. These personal data were kept, and are kept, in a password protected drive provided by the University of Glasgow, in a password protected excel sheet.

The first, and most significant, risk identified for this study is risk to participants. That risk was associated with causing harm and infringing anonymity of participants, during the data collection process. However, this risk was mitigated in this research and minimised. The recruited participants that were all over the age of 18. To recruit these participants, an email was sent to the main gatekeepers of the organisation, in their publicly available email at the organisation's website. The same applied to the rest of the participants, as they were emailed to request participation consent. Initially, and to gain access in the case organisation, the gatekeepers were asked for consent, which were provided and evidenced through an email. Finally, although it never occurred in the data collection process, mechanisms were put in place

to minimise possible distress to participants, and shield against any emotional, psychological, health, education or other issue. In such a case, the participants were made aware that the interview can terminate at their convenience, organisational HS was advised, and participants were informed that they can choose whether to choose to continue the process or not. However, this never occurred in the study.

After access was secured with the case organisation, the researcher sought Ethical Approval from the College of Social Sciences at the University of Glasgow. The ethical approval was presented with all necessary evidence to commence the study and mitigate/minimise all possible risks. Final Ethical Approval was given to this study in June 2022 (Appendix 1). Data collection started in July 2023. To adhere to this ethical approval, certain procedures were followed throughout all interviews, focus groups and observations. Moreover, participant consent was sought when accessing organisational or other relevant documents, if not publicly available already. Every participant was emailed before the meeting with a copy of the relevant participant information sheet (Appendix 4) and specifics of their participation expectations. Then, a meeting date and time was arranged at the participants convenience. During the interaction with the participant, they were offered the relevant consent form or forms (Appendix 3), and they were given time to review, ask any questions they might have had and sign it. No data collection procedure commenced without a signed informed consent on behalf of the participants. As an extra measure, and to avoid any distress during the data collection process, participants were informed that they could stop the researched if a sensitive topic occurred and the researcher ensured this was not brought up again, or they were explicitly told that they could stop the interview at their convenience. Furthermore, and to minimise possible omissions to this, participants were given time to read their transcripts, when needed, to erase any information they did not want to be included in the data. Finally, to ensure confidentiality and enhance anonymity to the most possible extend (and participants were made aware of that), a few procedures were also followed. First, all data and participant identifiers were de-identified by a code and a pseudonym was allocated to each participant, for example, participant 1, CRO, director, unit member, among others. Moreover, participant data, which were all digital, as participants were explicitly told, was kept at a password protected cloud drive provided by the University of Glasgow. No one had access to this data, except the researcher and its supervisors, under confidentiality. Finally, as participants were made aware,

this study's findings will only be kept for future publication purposes as a result of the doctoral thesis of the researcher, for the organisation to access through and report that will be sent to all participants via their publicly available email, and that these is the only information that will be kept as a result of this study. At the end of the study, and upon doctoral degree completion, all data will be deleted as per University of Glasgow Policy.

The final risks that were identified in this study, were those associated with the researcher and any conflict arising from this study. For the former risk is low. That is because the researcher did not engage in any field work that required presence in Greece, as initially suggested in the ethical approval form. All data collection procedures took place via Zoom and exchange of emails. As such, researcher risk was low to none. The same applied to the conflict of the study. No incentives were given to participants to participate in the study, there was no relationship between the researcher and the participants throughout the study and there was no connection with the case organisation and the University of Glasgow at any point in time. Therefore, there was no risk of conflict that needed to be managed for this study.

5 Introducing the case organisation

5.1 Introduction

5.2 Case study profile

To provide the context of the study and make the findings more relatable, this chapter, will introduce the case organisation and its nature, operations, management tools and risk management framework. The case organisation that this study collected data from is a public sector organisation in Greece, that has a specific role: manage selected EC funds for a specific period, that target the materialisation of projects that aim at increasing the value and life quality of European citizens. In fact, the case organisation is part of a network of standalone organisations in Greece, that are all called MAs and are responsible for managing EC funds for a particular set of projects. For example, employability, urban development and cultural investment projects, among others. Going back to the case MA, the organisation specifically manages transportation infrastructure and environmental/sustainability projects that are utilising these EC funds and is responsible for the appropriate allocation and absorption of these funds, throughout the materialisation of their projects. The funds derive from the well-known Partnership Agreement for the Development Framework (PADF) that the European Commission runs every 7 years and utilises European Union funds, given to country members, to implement various infrastructural developments in their countries, which is part of the wider European Regional Development fund (European Commission, 2014). Effectively, these funds are utilised for the development, prosperity, and modernisation of the country-members of the European Union. These funds are given to each country-member and are managed by relevant managing authorities, that are responsible for managing projects utilising these funds, in a respective area, for example, transportation infrastructure. It is also worth mentions here that these funds need to be fully absorbed by the relevant countries. The funds for the 2014-2020 programme period that the case organisation managed, were 4.7 billion euros. The projects they materialised with these funds ranged from road and subway lines, airports, ports and railway lines (transportation) to composting units, fisheries and recycling units (environment and sustainability). The transportation projects are considered mega-projects, and the environment/sustainability small projects. The distinction has been made in light of the funds

they use, with the former utilising millions of pounds per project, compared to the latter. For instance, transportation projects are considered mega projects, while environmental and sustainability ones are considered of smaller capacity. Mega projects are classified as projects with a budget of over 50 million euros. The funds that the case MA managed during the data collection were these from the EC fund PADF round of 2014-2020 and there were currently at the end of the funding programme period, plus 3 years that were allowed by the EC. In the effort to manage these funds, the case MA is supervised by several bodies, that is the SRSA, responsible for providing the rules of operations for all the MAs. Hence, the purpose of the SRSA is to monitor legal, regulatory and other compliances of managing authorities, and to develop and monitor various governance systems for the same managing authorities. And, at the same time, the case organisation is supervised by the European Commission and its regulations, as well as the relevant Ministry at the time. At the time of data collection, this was the Ministry of Development and Investments.

5.3 Case study operations

Once the funds are received, or made available to the MA, the process of materialisation of project starts. Initially, the MA engages in the identification of projects that are suitable to be developed for Greece, utilising these funds. The projects are selected by the MA, or the ministry, and are aiming at meeting the main EC targets that the funds have been given for. To materialise these projects, and since the MA does not have the capability or responsibility to do so, beneficiaries that will materialise these projects need to be identified. Hence, projects are advertised by the MA via relevant avenues (such as online websites or via competition procedures of the Ministry) and are made known to potential beneficiaries. Then, the process requires the beneficiaries to apply, and provide all the necessary documentation and assurances that not only they are capable of materialising the projects, but that they also will do so within the specific funding programme period. To provide assurances, the case MA engages into further checks, to assess the credibility of each beneficiary. Once an appropriate beneficiary is selected, the competition closes, and the materialisation of the projects starts. Once project assignment is completed, each project is given to specific operators from the case MA, to monitor their materialisation, from the initial stage to project completion. Initially, these operators set up the requirements for the project commencement and make sure that there is a clear plan for fund absorption, completion deadlines and any relevant assurances that need to

be in place e.g. risk management reports, environmental capability reports and so on. Effectiveley, the operators make sure that all parts of the project are set from the beginning in a detailed plan. That is because they need to establish a set of assurances for absorbing all available funds. For that matter, if projects are completed on time, and all funds are absorbed, then the MA is considered to be successful, and the EC is provided with assurance that they can handle projects in future funding rounds. In the case where projects are not completed within their timelines, the funds are either returned to the European Commission or are not given at all. There is also the case where projects might be either not completed on time, or they fail to materialise halfway through. In that case, the money is returned, and the cost is assumed by the Greek Government. In the case of no-fund absorption or no adherence to relevant regulation, the EC has the authority to reduce or deny funds in future periods. As a result, the case MA needs to not only select appropriate beneficiaries that meet specific criteria, but its operators need to make sure that project materialisation is as planned to avoid any fund absorption issues. For that matter, however, there is no mechanism within the case organisation that aligns these results with a clear reward or punishment mechanism.

5.4 Case study operations' management

To run their operations, the case MA utilises a specific structure and management tools. First, the MA is divided into units that are responsible for managing funds and the organisation itself (Figure 3.4). Indeed, "Alpha" unit, is responsible for assessing and integrating projects for the two project categories mentioned above: transportation and environment/sustainability. Unit Alpha is responsible for selecting projects, advertising them and selecting beneficiaries that meet the specific criteria mentioned before, i.e. certain capabilities of materialising each project. Each segment of the MA has its own Unit Alpha sub-unit. Effectively, there is a Unit Alpha that supervises one sub-unit Alpha for the transportation and one sub-unit Alpha for the environment and sustainability segments. After projects have been integrated into the programme, that is have met all the criteria to be funded from the EC funds, unit Alpha proceeds into integrating the projects under the organisation's supervision. At this point, the various units called Beta come into play, and they are given responsibility to monitor the accepted/integrated projects and the fund allocation. Operators work within these units and are assigned specific projects each. These units can be assigned many projects at the same time and are divided into 3 sub-units each, that are responsible for the materialisation of specific

projects, based on structure and expertise. For instance, there is a different Beta unit for railroads, a different one for subways and a different Beta unit for environmental projects. Each segment (transportation and environment and sustainability) has a divisional structure. In essence, Beta units are making sure that funds are used to complete the agreed projects that have been integrated by unit Alpha, in both transportation and the environment. Finally, the organisation has unit Gamma that is responsible for managing the organisation and its needs, including work support, human resource management, accounting and finance, regulatory compliance and all other supporting activities. Unit Gamma is effectively responsible for making sure all other units have what they need to complete their activities successfully and effectively. All these units are overlooked by their own supervisors, which are then supervised by a director for each segment. All of these are supervised by the director of the MA which is accountable to the ministry representative at each point in time (based on the one assigned by elections). All this can be seen in Figure 3.4

To manage their funding programme, and effectively to materialise their projects, the MA utilises a set of sophisticated tools that govern their whole operations. The purpose of this section is not to provide details of these tools, but to describe them in brief. More details of these tools will be provided in the findings section. To manage their operation, they MA is adhering to a very detailed and sophisticated Management Control System (MCS) that delineates the rules for all their operations. These rules reflect both EC and Greek regulation in the usage of EC funds. In fact, this tool, devised and supervised by the SRSA, provides rules, procedures and support to all MA operations, from project integration to project completion. In there, the steps to integrate projects are provided, the rules of selecting beneficiaries, and the relevant procedures, as well as the formal collaborations with beneficiaries and how these need to be done. Other elements of the system also include anti-fraud and anti-corruption mechanisms. Indeed, the MCS covers the whole range of processes and procedures that the MA needs to follow to materialise all their projects, with an aim at absorbing all EC funds and adhering to all relevant rules and regulations. In fact, rules and regulations are often referenced in the MCS. The purpose of the MCS is to make sure EC funds are not lost, by dictating the rules by which projects need to be materialised to do so. Conclusively, the MCS is the rules of the game. Withing the MCS, lies a very sophisticated risk management tool that the MA is utilising. On top of everything else, the MCS requires all MAs to run a specified risk

management framework, that adheres to this risk management tool. However, the MCS provides the basics of this tool, as every case MA is given flexibility to utilise it as per their needs. The risk management tool that the MA is utilizing is reflected by a set of risk identified, with clear risk management and monitoring tools devised by the MA. Effectively, the risk management tool of the MA sets the risk management framework of the organisation, as it includes all their identified and unknown risks (defined as uknown events and given attention to), together with all the details of their nature and the mechanisms in place to manage these. This tool is adhered to and updated regularly, according to the relevant needs of the case MA at that point in time. As part of their wider risk management framework, the MA has also created a specific team that works with this risk management tool, to monitor it, manage it and update it where appropriate. Within this team, representatives from all units of the organisation have been appointed to be part of the team. Their responsibilities are to manage and update the risk management tool, communicate risk and emergent risks, devise and discuss mechanisms for risk mitigation, and also communicate relevant updates to the tool and risk management mechanisms to all their respective units. The risk management team is supervised by the CRO of the MA, which is accountable to the director of the MA, that supervises all MA operations.

Apart from the MCS, which is the key tool the MA utilises to manage their operations, they also have other tools to complement it. For instance, the MA has developed and utilised a clear, ISO-reflecting, internal quality assurance and audit system. Effectively, this system is following trails and is making sure that the MCS and all rules and regulations that govern it, are adhered to. At the same time, this quality assurance system is checking if all procedures of the MCS are followed appropriately by the MA. This system, supervised by a quality assurance officer, is not mandatory to be utilised by the MA, however, they do so in order to ensure high quality of project materialisation, and insurance against external audits. Moreover, the MA is also utilising an online oracle system, called the IIS that aims at collecting and presenting all information about the life of the MA projects, from selection, competition, integration, materialisation and completion. Effectively, this system includes all relevant project and funding information, in adherence to the MCS, that helps the MA, and its operators have real-time information and monitoring of all of their projects. However, when information in this oracle system is incomplete, the case MA is utilising another tool, called the Action Plan. This tool has the same information that the IIS includes, but they also populate it with information

that the IIS cannot convey. These two mechanisms are the core of the MA operations as they are used to monitor and materialise projects throughout the funding programmes. For instance, at the beginning of the programme, projects are selected and integrated through information conveyed by the IIS. As the programme period matures, the IIS and the Action Plan are advised to check completion of ongoing projects. At the end of the programme period, the Action Plan is utilised to see fund absorption and re-allocated funds to more viable projects and avoid loss of funds. Throughout the programme period, both tools are utilised to check fund absorption to integrate new projects.

5.5 Case study justification

The primary reason for selecting this organization was its extensive use of management control systems, many of which are directly linked to risk management in daily operations (Gomm et al., 2000; Cooper & Morgan, 2008). In fact, the case study, as discussed above, has a clear, sophisticated and extensive risk management framework, that is also monitored and audited regularly. They also have the flexibility to tune it for their own needs and reflect their operations where required, in order to ensure effectiveness. At the same time, the key officers of this system, the Chief risk officer and the Quality assurance officer are very keen and proud of not only maintaining but evolving this system, as a model for the Greek PSO. This will be evident later when more discussion will be offered on this, when findings are presented. That means that, in terms of risk management and controls, the case organisation has a rich exposure to maintaining and utilising them, making it an appropriate case study candidate. All these are reflected to the creating and maintenance of a a very sophisticated and complex risk management system, advocated by a risk management tool that they have majorly developed and running themselves. These systems are responsible for helping the organisation with their responsibilities in managing and monitoring European Commission funds that are given to Greece to develop various infrastructures, specifically relating to transportation and the environment. Conclusively, and in relation to the selected research design orientation of the study, as discussed in the previous chapter, the selected case study has the potential to offer a rich understanding of the processes of the integration of risk management and management control in the context of the public sector.

6 Findings

6.1 Introduction

This chapter discusses the main findings of the study in light of the theoretical lens utilised to explore the phenomenon under study. To begin with, section 6.2 introduces the case study and focuses on its operations, on its main risk profile constituencies, as well as the strategic orientation that this case study possesses, with a clear connection to managing organisational risks. Then, sections 6.3 to 6.6 present the main findings of the study. These sections are structured in such a way as to present the levels of the Tessier & Otley (2012) LoC framework as presented in the theoretical chapter, and as these are transformed to apply to the controls, control systems and all other revised LoC framework elements that the case MA is utilising.

6.2 Managing authority operations and strategic considerations

6.2.1 Operations

As indicated in the research design chapter, the case MA is effectively supervising how the consecutive PADF programme is executed and materialised in the specific area of transportation and environment and sustainability. To expand on the research design chapter, the MA is divided into units that a part of them is responsible for managing funds and the rest are responsible for managing the organisation itself. For that matter, the first unit, unit Alpha, is responsible for assessing and integrating projects for the two categories mentioned above: transportation and environment and sustainability. Project integration works in steps. The first step is for the MA to advertise projects that the EC PADF programme is required to fund. This advertisement is done within Greece and to Greek beneficiaries that can materialise these projects such as subway and road developers, for mega projects, and municipalities and smaller local authorities in Greece, that usually materialise environment and sustainability projects. This is where Unit A comes in to overlook this advertisement and, following the appropriate rules and procedures, and integration criteria, assess the capabilities of any beneficiary and assess suitability for materialising projects. Effectively, beneficiaries compete for advertised projects, and the most capable ones are given the responsibility to materialise a given project. Once projects are integrated and included in the programme, they are indeed ready to be

materialised. As a next step, and depending on their nature, these projects are later sent to the supervisors of the materialising units of the MA. As such, there are various units called Beta units that are responsible for monitoring the fund allocation and making sure that funds are used to complete the agreed projects that have been integrated by unit Alpha, in both transportation and the environment/sustainability. In these units, projects are given to specific operators from unit supervisors, and these operators are responsible for monitoring and managing their materialisation. Finally, the organisation has unit Gamma which is responsible for managing the organisation and its needs, including work support, human resource management, accounting and finance, regulatory compliance, and all other supporting activities. Unit Gamma is effectively responsible for making sure all other units have what they need to complete their activities successfully and effectively. At the top of the MA, there is a director that overlooks the whole PADF programme and works with all units and their supervisors to ensure the programme is running smoothly. All these procedures are overlooked by the SRSA who are responsible for setting and regulating the main rules and procedures required to materialise all EC funded projects. At the time of data collection, the MA was also overlooked and supervised by the relevant ministry to which it belongs to, the Ministry of Development and Investments. This ministry overlooks the MA and their operations, as well as their EC funding spending, staff allocation and management and also their adherence to European and Greek law regarding project materialisation and spending.

6.2.2 Strategic profile

The main target of the managing authority is to fully absorb the European Commission funds for the programme period, or not to lose any funds, and materialise projects with these funds, within agreed timelines and by the end of the PADF programme period. The fund target, for the programme 2014-2020, was 4.7 billion euros that needed to be absorbed and expenditured during the programme duration or at a maximum of 3 years after the end of the programme, for projects that faced challenges in materialising. This translates into meeting targets in not only integrating appropriate projects, but also making sure that projects that have entered the programme and have begun materialising, are finished on time and with the appropriate funds. This can be distinguished into targets that reflect the main target at two levels:

- Operational: main target is to materialise projects at a specific predetermined timeline, and at the predetermined budget.
- Strategic level: successfully close the programme with all predetermined funds absorbed. Absorbed funds are different than integrated funds (funds projected and agreed upon, but not absorbed yet, not caused an expenditure in the project).

These targets, clearly set by the case MA, as directly associated with risks. As the CRO established in the first initial interview:

> *"What we call risk, is anything that can pose, rather, create losses, in the achievement, the basic achievement, the main objective of the managing authority, which is not to have a loss of fund at the end of the programme period. That's it. In other words, we see everything based on this. At the end of the programme period, the final report we will submit to the European Commission must show that we have sufficient material to cover all the budget allocated to the country for transport and the environment. That later translates into project deadline targets, to avoid loss of project funds. So, everything goes through that prism".*

Moreover, the programme has European Commission dictated targets, connected with allocating funds, that have to do with what the projects will meet if they materialise, for example, social targets for kilometres to serve specific number of citizens or reduce distance times, number of citizens served by a new water supply and sewage system, or recycling time per ton for a recycling system.

6.3 Managing strategy and risk: integration of management control and risk management

6.3.1 MA risk profile: the centrality and procedures of the risk management tool

That main target mentioned in sub-section 5.2.2, and the relevant targets at both levels, are associated with all relevant risks that can affect it, as all participants indicated during the interviews and focus groups. Thus, the managing authority is exposed to any risks or uncertainty that can affect these targets and risk management within the organisation is associated with managing all these risks and uncertainties. As a result, the main risk/uncertainty is reflected to the attainment or not of these targets. These risks are later translated to reflect project risk, that include any event that can hinder the complete materialisation of a project, and in turn, can lead to loss of funds, and eventually missing the main targets of the MA. Again, at both levels, the MA is exposed to a set of risks that have been classified according to the organisational needs. The organisation, as dictated by the European Commission Management and Control System (MCS), is responsible for building and maintaining a risk management tool that delineates the risks of the managing authority, and the programme, as these can affect the targets mentioned in the previous paragraph. Despite being dictated, however, the managing authority has the flexibility to apply the risk management tool as per its needs and risk/uncertainty exposure. In turn, the MA takes this tool that has been populated, and transforms it according to its needs, by populating it with additional risks that they deem appropriate to their operations. Moreover, this risk management tool delineates the mitigating mechanisms for each risk category. In an effort to keep the tool up to date and relevant to their project and operations, risks are identified and set by the manging authority, and specifically by the risk management team of the organisation and serve as the main risk and uncertainty categories that can affect the organisation and the programme, and by extension, the aforementioned targets. According to the tool document provided by the head of quality assurance, risk and uncertainty are classified into four categories: programme risks, organisational management and operations risks, non-compliance beneficiary obligation risks and political and economic risks. Therefore, the risk management tool serves as a technical control tool within the MA that delineates the acceptable risk appetite of the organisation, and the mechanisms put in place to mitigate those risks, as a rule of thumb. The latest version of the risks that were included in the most recent revision of the risk management tool, was

accessed in the document that represented the 3rd review, and revision, of the latest version of the risk management tool, by the MA, in 2021. These risks are broken down into further categories as seen in Table 6.5. All these risks apply equally to both mega and smaller projects.

Risk category	Risk	Risk origin	Risk description	Risk effect	Risk probability	Risk level
Programme risks	Delay in programme funding completion	External	Any delay in completing the programme from delays in receiving funds	N/A	N/A	N/A
	Delay in completing the programme commitments	External	Delay in completing commitments of the programme as received by the managing authority.	N/A	N/A	N/A
	No normal flow of funds from the MA	Internal	This risk has to do with delays of funds flows from the MA in terms of delaying processes and procedures for releasing funds to beneficiaries.	Significant	Almost never	Medium
	Delay in specialising political sectors	External	Delay in realising and finalising strategic objectives and requirements from various governmental bodies, that delineate the needs for road and environmental infrastructures.	Low	Almost never	Low
	Failure to meet internal deadlines and quantitative programme targets	Internal	Describes all elements that might delay the meeting of the main targets of the MA that might lead to delay in project payments or loss of funding due to fiscal corrections.	Significant	Sometimes	High
MA operations and management risks	Staff shortage	Internal	Failure to cover critical staff positions to make sure the MA works on projects as intended to.	Critical	Sometimes	Maximum
	Delays in project fund invitations	Internal	Delays to publish project invitations.	Limited/Insignificant	Almost never	Low

Risk category	Risk	Risk origin	Risk description	Risk effect	Risk probability	Risk level
	Deadline non-compliance	Internal	Failure to meet deadlines in project selection, integration, contract amendments and other changes in projects.	Significant	Rarely	High
	Failure to systematically monitor beneficiaries	Internal	Failure to closely and systematically monitor beneficiaries that might lead to loss of funds due to delays in fund absorption.	Significant	Sometimes	High
	Failure to systematically tackle fraud incidents	Internal	Failure to detect and manage fraud risk in assessment and section of projects, materialisation of projects, accreditation and payments, and selection of technical support intermediaries (for the purposes of managing the MA). Includes any failure to manage fraud.	Significant	Sometimes	High
	Emergency events/ pandemic	External	Any emergent event or situation that might hinder the smooth operation of the MA and its beneficiaries.	Significant	Rarely	High
Risks of beneficiary non-compliance	Non-compliance with the national laws for public contracts	External	The beneficiary fails to comply with the law of public contracts in Greece. That might lead to non-selective expenditure and loss of funds.	Significant	Sometimes	High
	Inadequate management of projects	External	Materialisation of projects that differs from pre-approved and agreed way of materialisation, as described in the selection and materialisation criteria.	Significant	Sometimes	High
	Failure to meet deadlines according to fund agreements	External	Beneficiary failure to meet project completion and management deadlines,	Limited/In significant	Sometimes	Medium

Risk category	Risk	Risk origin	Risk description	Risk effect	Risk probability	Risk level
			including failure to manage emerging problems.			
Political and Economic Risk	Changes in the legal and normative frameworks	External	Failure of project materialisation to meet legal and normative framework criteria, or constant changes to these legal frameworks.	Significant	Sometimes	High
	Delays or changes to the planning/materialisation from the central management	External	Delays in decision-making from the central management that overlooks the MA.	Significant	Sometimes	High
	Restrictions from changes in the relevant financial system laws and regulations	External	Difficulties in undertaking or materialising projects due to fiscal changes that might affect the MA or the beneficiaries.	Critical	Rarely	High

Table 6.5: Risks in the case organisation

As shown in Table 6.5, these risks are also classified into levels, depending on their effect on the risk of losing programme funds. Indeed, the organisation, especially the risk management team, with their expertise, have projected these estimates of these levels, presented in Table 7.5 and Table 8.5. These risks and the metrics of their impact have also been discussed and agreed upon with the procedure compliance department of the Ministry. Table 7.5 describes the probability of a risk and Table 8.5 shows the levels of risk and their effect. The MA classifies risks based on intensity and probability of happening. Historic risks take higher probability, as they have been known before, and their impact is more or less assessed. The classification is made with combining probability, and impact and effect on loss of funds. These tables are a replica of how these exist in the risk management tool of the case study. Originally, the main risks of the MA were identified and established at the strategic level, with discussions between the director and the CRO and CQO and the SRSA. That happened in the mid-2010s, when they were negotiating the introduction of the risk management framework in all managing authorities, as part of their operations. Thes risks were fed to the MA via the creation of the risk probability and impact tables as seem above (Tables 7.5 and 8.5). Back then, which continues to this day, the risk management team was established, to overlook the risk management framework of the case study. As such, representatives from all Units came into play to represent risk management in their respective units. And the risk management team was finally formed. Within its role, the probabilities and impact of risk and uncertainty are discussed, majorly in a bottom-up fashion. For instance, when the risks were initially established, the risk representatives took this information and communicated it with their respective teams. Within these teams, these risks were monitored in projects by operators of Beta units, and internal risks by other units such as Unit Gamma and Alpha sub-units. As the projects and the MA were operating, these risks were evaluated on how they applied to instances, for example, different transportation and sustainability projects. Then, within these project teams, the impact of risk was evaluated on whether and how it applies to different situations. After the completion of projects, for example, operators came to talks with their risk representative which established the new risk evaluations and impacts to be fed to the table. And this is done by discussions with the risk management team. The same process applies to emergent risks. However, this time, an evaluation occurs at the operational levels, fed into the risk management team, and a new risk is included in the tables, with clear probability, to be monitored by the MA. Finally, the MA, usually at the strategic level and with the help of the

CRO and the Director, utilise these evaluations to discuss risk management processes at the strategic level. Here, discussion with the SRSA and other MAs is crucial, in sharing the case MAs experience and create sector-wide risk evaluation and monitoring. However, how this works, is outside of the scope of this study. It is also worth noting here that, on many occasions, and in direct relation to the nature of the projects, these probability and impact tables might not be followed. In the case of some operators, risks are set for their projects and are displayed against a specific probability and impact. However, the nature of their projects, and the workloads this entails, especially in major transportation mega projects, they do not fully utilise this evaluation and monitoring method. As one of the operators in major road projects discussed in one of the interviews:

> *"So here we have this famous risk management tool of the programme, which, however, is not fed as it should by the progress of the implementation of operations. That is one point. And also, it is not always fuelled by all the developments of the external environment…So me, what do I do? I try to cover these two pieces (risk monitoring and evaluation) on my own, and in my own field. In the projects I have, I have made a tool makes a financial evaluation of the prospective contractors. That is, when someone wins a job on a project, I need to know if that contractor is capable of getting the project done. And this check is done both initially and intermittently. Because a company's financial conditions change. The other thing I do is the policy and legislation part. Because there are constant developments... These laws create new risks. We have a new set of risks because of these laws. This new set, then, is so large and broad that it even changes the form of the contracts we are going to award. The changes are not small. They are changes at a structural level. This is the one part, then, the institutional, of the external environment, that describes a set of dangers. In a second environment, I have made an application in an excel. This tool is activated when something happens. That is, for example, in the legislation there is a procedure for amending the contract. The contractor may, for example, request an extension. And we say, why is he asking for an extension? What are the reasons? So, I read the justification and questions start to arise. We ask the beneficiary and the contractor to clarify the case and, having in mind other information on the financial standing of the contractor and changes in the legal framework".*

As a result, these tables, are somewhat of a box-ticking, directions setting exercise, that aims at creating space for regulatory and internal legitimacy. They exist, but at the operational level, especially for mega projects that are challenging and multi-faceted, operators evaluate and monitor risks that might be outside of the scope of these tables but at least directed from these.

The higher the probability of occurrence, the higher the classification, The higher the impact in the loss of funds, the higher the impact classification. For uncertainty, the same applies, as the MA classifies it with probabilities and impact again. The risks, probabilities and effect have been determined by the risk management team within the case MA. This team is responsible for establishing these risks, re-evaluating the tool with an additional risk category that may derive from an emergent risk, and check the effects and probabilities of these happening throughout the programme period. If changes apply within projects throughout each programme year, for example new regulation or new project and environmental influences, operators feed this into this risk management team, and they then discuss and re-evaluate probabilities and risk effect. As such, to evaluate the risk management tool to reflect updated circumstances, the risk management team engages into interactively used meetings. Once risk and their effect/probability are identified, then mitigating mechanisms are put or updated in the tool, if mitigating mechanisms already exist. In the case of an emergent risk, they monitor it, discuss it with the SRSA at the strategic level, and if it becomes a known risk, it enters the tool with its own set of characteristics. Since this process is used to manage risks and emergent risks in particular, more information will be given on how this works in the later sections. In there, the process will be unravelled as to how the risks in the risk management tool work and how they are updated if necessary. The CRO was clear in unravelling this process:

> *"Absolutely. Every review we do... Rather, every risk assessment done predicts a review next year. So, as a risk manager, I must, at some point in time, in a year's time, or sooner I can do it, if I believe that there is something extraordinary and whatever, to convene this risk management team for a meeting. We get together, and we formulate an agenda of issues… The other part is that we take the tool line and brainstorm there the whole team thinks and brings everyone from his team about the existing risks. And then we say, in these fields that he has set us a tool initially,*

something new has emerged. And if we have a whole new area of risk that has appeared to us. So, we are having this open debate. We identify something, we try to put it, first of all, into our existing tool. In other words, we have a central guidance from SRSA, the which has forged the first tool, and has distributed it. Which has told us, but please do not abuse it in the sense of making a huge spread to this tool".

Risk probability	**Percentage**
Almost never	0.00% - 1.00%
Rarely	1.1% - 5.00%
Sometimes	5.1% - 10.00%
Frequently	Greater than 10.00%

Table 7.5: Risk probability

	Risk effect				
		Limited	Low	Significant	Critical
Probability	Frequently	Medium	High	Maximum	Maximum
	Sometimes	Medium	Medium	High	Maximum

	Rarely	Low	Medium	High	High
	Almost never	Low	Low	Medium	Medium

Table 8.5: Risk levels based on probability and effect

6.3.2 Unravelling risk and uncertainty: some examples

During the interviews, especially with project operators, it was shown how risks in the previous section are manifesting within projects in more detail. For example, when discussing beneficiary risks, one of the operators of environmental projects indicated that these projects are materialised by small municipalities around Greece that work under understaffed conditions. Usually, one or two beneficiary operators are responsible for materialising a plethora of small environmental projects. That represents a beneficiary risk and is closely connected to the specific risk that the MA has identified as the beneficiaries inadequately managing their programme. To further support this, the same environmental operator indicated that some municipalities:

> *"They don't have two projects each (the municipality operators), they have too many. Even for procurement for these projects, and even if they can do it, it takes a lot of effort and time. For use, risk management is a big deal in these projects, because there is a workload of employees they cannot cope with and do the proper supervision and monitoring of the whole project".*

The said risk causes delays in project completion, and it occurs frequently with a critical impact. However, as most mega-project operators indicated, this is not the case in transportation beneficiaries, as they are well-established private sector companies, most of the time, that have abundant experience and are monitored by Greek law, and fiscal regulation. For these beneficiaries, the risk is different and has to do with delays from processes of integrating projects, or even lawfully challenging this integration after it has been approved. These risks represent low probability, and they have low impact. For instance, there might be a beneficiary that lost the assignment of a project to another, and the former can challenge this decision of

the MA in court. This cannot be predicted in every project integration, and it is an event that is known, but not known when it will apply, and causes delay to the project completion, even at the initial pre-materialisation stages. This risk is two-fold and has to do with the MA response times and the beneficiary management.

Furthermore, there are examples of programme risks. The CRO, at the initial interview for this study, indicated that any risk consists of programme risk as long as it has the potential to result in loss of funds. And then went over to indicate:

> *"When are funds lost? When projects are not materialised on time. Or when the beneficiary of a project fails to comply with the rules of completion, or regulation and so on. Or when the MA materialises projects without considering the EC funding requirements for projects, e.g. development and infrastructure for sustainability".*

All these represent risks associated with the programme, they reflect the risk of delay in funding completion, and they can hinder the main objective of the programme. They are also high probability, and significant to critical impact risks.

Another set of examples has to do with risks associated with the MA and its operations. For instance, an example of risks that are associated with the failure to monitor beneficiaries and its operations, is the process of failing to comply with the rules for responding to beneficiary changes in project materialisation, and also delays in reporting back to the beneficiary when operators engage in on-site verifications to check the progress of said projects. As the CRO and many project operators indicated, the rules applying to the MA are that there should be 20 days in responding to an on-site verification, with a report that shows all findings. However, due to understaff conditions, and work overload of many operators, the target of 20 days is usually not met, causing further delays in materialising projects. Speaking of understaff conditions, a risk clearly identified within the MA tool, in currently manifests as there are a lot of places that cannot be filled, and many operators undertake more project monitoring than expected, causing work overloads and delays.

The notion of emergent risks was devised and included in the risk tool of the MA, when the outbreak of Covid19 happened in 2020. In there, with a clear influence by the pandemic, the

MA decided to include the notion of emergent events and pandemics, as a clear identification of uncertain events that might hinder the programme and the MA's operations. These risks represent a low probability, and an unknown impact level, that needs to be assessed upon exposure. These emergent risks are also connected with political and economic risks that manifest in the external environment of the organisation. For instance, when referring to the Covid19, one project operator indicated:

> *"The last few years, we have also seen a lot of external risks. And we have begun to see them more seriously, because, even starting from Covid19, we have influence of these risks. And, in a recent talk with the risk management team, we have discussed for risks associated with the supply chain of projects, and the increase of material prices that is a by-product of these supply chain risks".*

These risks are but some examples of how the MA sees and classifies risks and uncertainty. More details on ow these risks manifest themselves will be given in later section of this chapter, when a discussion will be held on the processes by which they are managed.

6.4 Managing risk at the operational level: PMS centrality and complementary control systems

6.4.1 Managing risk and uncertainty at the operational level

6.4.1.1 Managing operational performance: risk at the heart of performance management

For the case MA, performance management systems are at the heart of managing projects and the programme as a whole. They are the key systems to manage funds and project performance, internal operations performance, as well as gather information for corrective action. At the same time, many of these controls are also utilised to make sense of emergent risks. Risk is at the heart of this performance management system at both the strategic and the operational levels. At the operational level, operational performance control systems are associated with the assessment and monitoring of key success variables of operations, that are connected with meeting strategy and strategic objectives (Tessier & Otley, 2012). Here, diagnostic controls are central, complemented by "values and organisational symbols" that promote organisational

performance, and procedures that evaluate that performance (Tessier & Otley, 2012, p. 180). As it will be seen in this section, the case organisation utilises all these at the operational level. For that matter, the primary and key performance target of the MA is to complete projects in the agreed timelines, with the agreed budgets. That also needs to be in line with all EC and Greek Regulation. This is broken down into a few main Key Performance Indicators (KPIs) that govern performance measurement at the case organisation: project timeline KPIs, project budget KPIs and compliance KPIs (both to law and MCS). The first KPIs are reflecting the project completion targets and are usually agreed yearly, depending on the stages of a project. KPIs on budget are concerned with meeting targets of EC fund absorption, which is usually agreed and communicated on a yearly basis, depending on the stage of each project. The main KPI is also to absorb as much as possible EC funds for all projects. Finally, compliance KPIs have to do with a variety of compliance requirements, from all operational boundaries, that have to do with the MCS, law and regulation, project compliance i.e., provide the correct and necessary documentation for each stage of the project, or EC fund targets for project inclusion, response time targets from the project operators to IIS communications and agreements, and regulatory standards and targets that need to be met for each project. All the KPIs, are monitored and reach back to the main targets of the MA and the programme they operated at the time of data collection. These KPIs, critical for the completion of projects and the programme itself, are associated with the risk of project and programme failures if not met. As such, the systems operate with risk being their central concept of attention and these KPIs, as it will be shown below, serve as risk KPIs at the same time.

6.4.1.2 On-site verifications

The managing authority is required, as per the rules reflected on the MCS, to engage in on-site verifications for each project, on regular intervals agreed by the MCS for each project, usually every 3-6 months. These verifications are also called physical object confirmation visits, as they serve as a tool for a real-time checking of the progress of a project, while it is being materialised. At this level, on-site verifications serve as a technical control, used diagnostically, in a constraining manner. That is because, and during an on-site verification, project operators (the ones responsible to carry out this verification) can confirm the project elements and technicalities of the project, and thus check if and how a said project is progressing and planned, based on meeting the KPIs discussed above. Moreover, on-site verifiers can informally

communicate with beneficiaries, and sometimes sub-contractors, about all elements of attention for the project. Especially in environmental and sustainability projects, and to reduce delays and support project completion (due to the nature of beneficiaries and project), operators go an extra mile to work with sub-contractors in these instances, to support them with regulation, information, and anything they need to complete the project. This informal communication is also used interactively and in an enabling way to identify not only the nature of an emergent issues (emergent risk), but also see how it manifests and discuss problems and mechanisms to solve it and avoid delays.

During an on-site verification, and due to the closer communication and the ability to take a closer look at the project itself and a meet with the beneficiaries and sub-contractors, project operators get a better idea of the issues that manifest in it, and they can also see elements that cannot be identified in the formal communications between the MA and the beneficiaries. As one of the project operators identified:

> *"But, it (the on-site verifications) is a way, for better or worse, in the projects, if you do not go on the spot, you will not understand. It makes a very big difference... The progress of the economic object of a project is important, but the physical object also has its own value. Plus, the fact that I have had a lot of conversations… One time, we might come across people in materialization who although they have taken the money of completion of a project stage, they do not leave and create issues with the construction sites. This might not be visible through official papers and communications. So, on the spot, you learn things. You see a great deal, and I don't know whether the system wants it, but personal contacts with the project and the beneficiaries and the construction site and so on are very important. That is, trust is something that has been built with a lot of effort, we usually change the projects so that they are not the same and you get stagnant, but you can take the projects with the same people, because we have enough leeway, with some of these people, to call at 11 o'clock in the evening or on a weekend, and tell them that some payments have to be made. To clear things up. And they have cleared up for many instances. So, it is very important that sometimes this does not replace but complements all the systems that we operate and use this personal contact".*

As seen in how the participant above perceives on-site verifications, they are very important in unravelling all the details of a project, especially the ones that are not clear or cannot be agreed or identified through a formal interaction. These details have to do with technicalities, the site environment of the project, how emergent risks manifest and every issue or element of the project and how a project progresses. In that respect, on site verifications work in two ways. The first is diagnostically to verify that all elements of the project, especially at the stage where it is being physically built, are progressing as planned, and following the regulation and IIS set targets for completion and fund absorption. On the other hand, on-site verifications are also used interactively to identify and report emergent risks that were either not their pre-materialisation or manifested during materialisation and were reported by the beneficiary through their integrated information oracle system (IIS), but without a clear understanding. That is because the IIS cannot always include all the details of an emergent project issue, due to the limitation of the information provided. Instead, the IIS actually triggers the on-site verification and communication with beneficiaries, as it will also be shown later on. If an emergent issue is persistent, then the MA can classify it as risk. In a feedback procedure, operators check these emergent risks, and then they communicate it with the risk management team of the MA, at the meetings and to their superiors, for discussion, assessment, inclusion and mitigation mechanisms. As such, feedback from on-site verifications can travel up to the strategic level to inform strategy and revisit the risk management agenda, if risk or other elements of emergent risks persist, for example, a new regulation. For instance, the integrated information system that the MA and the beneficiaries use to formally communicate, includes all information on the schedule of the on-site verifications when they are due and where they are done. Once an on-site verification is complete, an operator creates a report to the IIS, no later than 20 days after the verification, which is the main response target for every operator post-verification. This report includes information on the post-verification findings and procedures agreed to continue the project, if an issue arises. This serves as a control utilised diagnostically, and as an interactive control tool to enhance organisational learning on project risks, at both organisational levels. This report also serves as a corrective action mechanism for the beneficiary to follow and for the operators to look at, as it analyses their performance on responding to on-site verification. For that matter, through the ISS, operators can check how their own delays might affect the project completion and discuss options to reduce the report delays, if possible. This was something, as the CRO indicated, that is done in the regular risk

management meetings, as the whole team discusses holistic information on delays from all project operators.

Especially for environment and sustainability projects that include more uncertainty, mainly due to the EC general targets and the nature and experience/expertise of beneficiaries, operators at these projects use on-site verifications, complemented by meetings and other informal means, to confirm the project and the targets of absorption, but also to see how the project progresses and to identify emergent risks. An operator of such projects framed the importance of this by saying:

> *"So, I happened to see work in a small municipality up the mountains, a rural village, where they had done a small composting plant using EC funds. When we went to see the project, they showed us composting. That is, they had bought and installed all the pieces for composting. But they didn't operate it! It was very clear that they were not operating the unit, because firstly there was no material, and the unit was very remote. Then, the employees were just two, and they went there because the headquarters were elsewhere and they went there three times a week to check, so there was no material to run the composting unit. So, while the expenditure has been made correctly for this project, in terms of effectiveness, to implement it, the answer we got, we were told, that okay we took it as a pilot, to see how it works and did not implement it. As a result, this expenditure would not have a direct impact on the environment and residents. This has been an uncertainty".*

As seen above, this uncertainty, this emergent risk, was manifested itself in the project and was only evident when the said operator engaged in on-site verification. At this stage, and through utilising the concept of on-site verifications, risk and emergent risk are the central reason why these verifications are utilised.

In essence, on-site verifications are a way to confirm and manage the performance of each project, and its main targets and completion dates, and elements of physical substance that are connected to funds and any other relevant element that needs to be completed. That way, operators can engage in managing said performance and trigger corrective action when needed. Moreover, on-site verifications serve as a real-time observation and assessment of any risk or

emergent risk that manifests into a project. Evidently, operators visit project construction sites to check many project elements, including fund utilisation and that funds are sued where it has been agreed to, project maturity to ensure completion in time and how the regulation has been applied to each project. That way, the operator can confirm progress and report issues. These issues, these risks, will eventually lead to project delays and under-absorption of funds. Therefore, the operator, by checking these issues, can create report that serves as a tool to guide the beneficiary to take corrective action and mitigate said risks and emergent risks. Therefore, the on-site verification tool is used both diagnostically and interactively to manage performance, and, at the same time, is integrated as a mechanism to manage known and emergent risks.

6.4.1.3 Oracle system (IIS)

At the same time, and at the operational level, another mechanism of performance is associated with monitoring the performance of the beneficiaries and works very similarly with on-site verifications. But the key mechanism here is not the on-site visits, but an oracle system. This tool is a sector-wide Integrated Information System (IIS) oracle system, utilised by the MA, that aims at formally communicating all necessary information for the completion of projects, and information for strategic decision-making. The IIS is an integrated information system that has been implemented and utilised by all managing authorities managing EC funds. It is a tool for managing the programme, and it translates the sections of the MCS into key sections for information exchange and control. In this system, the managing authority and the beneficiaries input real-time information for the progress of their projects. Information included in this system relates to any part of a project such as

- Information for the assessment criteria of a project.
- Information on the integration criteria of a project.
- Information on project or sub-contract modifications and extensions.
- Information about completion deadlines and fund absorption.

This information helps the managing authority monitor each project specifically, see how they are progressing and why there are any delays. They can also monitor changes in projects and

have real-time information about elements of a projects that were not known before the materialisation of a project. In essence, this system acts as an information providing tool for monitoring, decision-making and communication with all key stakeholders, i.e., the managing authority, the beneficiaries, and the overlooking authority of the ministry, at both organisational levels and for all the stages and needs of a project. In fact, information exchange occurs for projects throughout the whole process of integrating and materialising projects.

At the operational level, the main target that beneficiaries need to meet, and is embedded in the IIS, is the timeline of completion of a project. This needs to be agreed with the MA at an initial stage, and then beneficiaries break it down into critical targets (completion of technical reports, supplying of equipment and other elements of projects as per project completion requirements) for the project success, which are risk targets, because if they are met, they mitigate the risks associated with delays from non-compliance to EC and Greek laws, or non-compliance with technical components, for example materials and IT monitoring systems in projects, among others. When issues with compliance arise, and to be proactive against new laws, the risk management team utilises their regular meetings as an interactive control tool, to make sense of new regulation and revise their attention to where the beneficiaries need to focus on complying, and as a result, where the MA needs to monitor their performance. Indeed, as observed in one of these meetings, the team at the time, discussed the effect and impact of new laws and discussed clear mechanisms to adhere to these laws. As observed by the researcher, at the end of one of the risk management meetings in November 2022, the team brainstormed one of the new laws, to show how these affect their current risks and how these laws might affect the new PADF programme of 2021-2027. The discussion was wrapped around what points might be taken from these laws, what the organisation might need to do and with which bodies they will need to talk with to include this risk, and how this will affect operations and projects, even current ones. The discussion was also around the main elements of the cycle of a specific mega-project and how these laws will affect it and how new elements of this law might affect the actions that need to be taken for the team such as new law items that need more training. Possible controls were also discussed, but not brainstormed. The team discussed that there are issues with the new laws, but when discussed in upper or external bodies for solutions, they need to show not only solutions but how to implement that and associated controls/processes.

Conclusively, the ISS, at the operational level, serves as a technical control tool, used diagnostically in a constraining manner. That is because it communicates the critical targets mentioned above from the beneficiaries to the MA. The beneficiaries are required by the MCS to input all relevant information for these targets, so they can be visible by the MA. Then, the MA takes corrective action if a target is off and raises an alarm of either delay or non-compliance. This is where risk management

IIS also works to monitor internal MA performance. This oracle includes information on how the MA responds to laws and regulations, especially new ones. It shows if they are up to date with new laws about public contracts, with Human Resources (HR) and other laws that might affect their operations and any other relevant information that might affect organisational operations and performance. For example, unit Gamma, goes and checks the HR results of the MA per year to see personnel and personnel related information, to see if they are over or understaffed. Accordingly, they take action to ask for procurement of staff through the Ministry. But, as all participants working with or for Unit Gamma indicated, this is something they do not have a lot of influence on, as the staff movement in their area is dictated by external factors, for example, political changes, needs of other public sector entities, especially other programme MAs, needs of the Ministry, public spending. One of the main operators of Unit Gamma, in clear reference to this and how it is affected by the consecutive political environments on the country, referred to how the 2023 national elections delayed their recruitment of staff in meeting various operational needs:

> *"The concept of the elections in Greece has the following consequences. On the one hand, because we have a political supervisor who is the body supervising the managing authority, who is politically appointed, as recently, because it was election period, he told us that personally, they are no longer signing any staff movements, as it would be a risk for them. So, in this part, especially in the part of unit Gamma, which is support and operation of what we need assignments for consultants, for operation, for equipment and so on at the time, we must move quickly if we want these before the elections. For about four months, and because now the elections are by proportional representation and it is estimated by the whole world that we will not have a self-sufficient government, we will go to a second election. So, because of this election process, we will not have signatures for the processes to recruit new*

personnel and consultants to cover our needs for about 4 months. They will sign, before the elections, on accession issues, but they will not sign on assignments. And then, if the political person who oversees us changes, again there is a period until that person is informed, talks to his advisers and so on. And really, especially for 2023, this is catastrophic, given that it is the last year of the PADF 2014-2020 program period, and we are 1.5-1.8 billion behind in spending. And, of course, this does not only exist for us, but there is also an issue some of the beneficiaries. If, for example, the governor or the president, whoever needs to agree, does not want, or politicize or on the matter and delays, will be a period when we will not have signatures for the relevant procedures in the projects, for things to move forward".

Speaking of Unit Gamma and with relation to law and regulation performance of the MA, this unit is responsible for regulation application in the MA, and to search law and regulation via various legal documents and a database they have, to see law updates and communicate these with other MA units to ensure compliance and avoid risks. During Covid19, this team was responsible for monitoring the workplace regulation imposed nationally by the pandemic, and the rules that were devised by the MA. They then communicated it with all units and operators to ensure compliance, via meetings and emails, and to avoid risks. If there is a personnel shortage, they also follow legal recruitment law to recruit staff from other public sector entities, or externally, or through other MAs. The way this work is that they see staff needs, devise a report, send this report to the Ministry and the public body responsible for staff recruitment and allocation, and they ask for staff. But this is the only thing they can do, as they cannot recruit, and there are staff shortages in the Greek public sector anyways. Therefore, to solve this issue, MA staff usually utilise goodwill and extra personal effort to ensure that work is not delayed. Unit Gamma also pulls IIS reports that have to do with response rate and times of all personnel, to see deviations, why these deviations occur, and discuss improvements, usually with operators and unit managers.

Another example of the use of IIS to monitor MA compliance and performance when the IIS shows all relevant dates where an item has been inputted by the beneficiary and the date the project operator responded to it. The IIS also includes the targets and responses that need to be met through the timeline of a project, and raises alarms, usually in a yellow indication, if an action has not been completed by the project operator, in the agreed time. This directly reflects

risk. In essence, if these targets are not met for the project, then there will be delays and a risk of the project is not completed in time. Therefore, the IIS is used diagnostically to emerge these targets and point them out when they are overdue, to avoid delays. For instance, one of the project operators, when showing how the IIS operates in one of the Zoom interviews with the researcher, commented:

> *"So, there you have it, what you see is a reference to a very specific railway project, which is the signaling of the Athens-Thessaloniki-Promachonas railway axis... Old project, and problematic on too many levels. As you can see in the maturity report that the ISS provides, it gives you group data on the act, on the deadlines for the project decisions... Here the program is divided into deadlines to act, financial, tracking data, all these, into a table. For example, here, it monitors obligations. It also tells you if any checks have been carried out, if we have found findings, at what level it is assessed that the project should be monitored. This project, let's say, comes out with the tracking code, like a project status that we operators put into the program. To have an image, in the maturity report there is also the memorandum and how it works and what parameters it evaluates to categorize the projects. It tells you, say, the evaluation result field comes out of the previous slip put in by the operator. The MIS tells you what it is looking at; in order to get the result, it gets in the report. Therein lies the synopsis. If you've included a search of a lot of projects, you'll see a more general report of the projects you've taken. Which of these are to be monitored, which are to be completed, which are on intense monitoring. The latter are at risk and need monitoring, or they need a surveillance decision, which means that the project is placed in a regime of increased monitoring, because it has been identified in the maturity report that the project is in danger of not being finished and not being completed in time. Another field of maturity report tells you that, in the financial data of the project, there is a difference in costs. The project has received money, and no expenses have been declared, why? It is a matter of giving money to the beneficiary in projects and not declaring costs. The maturity report pulls that out too".*

Evidently, the IIS can produce reports for all these data, on top of fiscal and their completion data of the projects. The IIS then classifies projects that need more attention and need to show a progress report. It points out the projects which have delayed processes and require attention

for the operator to pick up on. Effectively the ISS shows the maturity of projects and hence how these progress in relation to project targets. If the project processes and agreements, documents and signatures are in line, then the IIS shows no crucial attention to the project. Moreover, the IIS, depending on operator needs, can provide multiple reports on many aspects of one or multiple projects and the MA uses it to see how targets are met. For example, the IIS compiles a maturity report as discussed by the operator above. This is a report with updates for the results of the units, new targets if needed and so on. It's an update to show the whole performance of the MA and individual units, and what else needed to be included as target.

The IIS also includes, reflecting the rules of MCS, all the dates and milestones that have been agreed by the beneficiary, for all stages of project integration and materialisation. If there is a delay, the IIS raises and alarm and operators chase the beneficiaries for details on the delays, supportive documents and a solution to the problem, to avoid further delays. When a project has issues that need attention, i.e., extra documents, legal attention, issues with sub-contracts or any other element that might cause delay, the operators, through the IIS, put the project under surveillance and they make IIS dictations to the beneficiaries to respond to delays and provide necessary documents, assign a sub-contractor, and so on depending on the issues that causes delay. In the rare case there is no resolution to the project issues, for example non-appropriate spending, then the project is terminated. But this is not usual to the mega projects due to their nature and the nature of the beneficiaries, and it is slightly more prevalent to environmental and sustainability projects. However, as it will be discussed later on, the operators utilise the social control of personal effort time to avoid these issues from the project assessment stage already.

To make matters clearer, project completion targets are inputted on the IIS as per agreement with operators and the agreed materialisation timelines. If a project is delayed, the IIS includes all delays and new completion dates or future ones, including full justification on these delays (regulatory documentation, technical reports etc). As such, the IIS is utilised as full performance management tool (both for MA as a whole and for risk management).

Some representative examples are as follows:

1. 500 meter or more road or train tunnel, need to adhere to specific standards and parameters, regulated Greek law and Independent Authority of Tunnels in Greece. This needs to be communicated to the managing authority by IIS to see that these have been met as targets for the relevant project to continue.
2. Most of the beneficiary participants engage in excel targets for projects, to include targets that need to be met for projects i.e., risk management folder, risk assessment, technical targets, EC targets and so on. These are communicated with the MA via IIS.
3. A beneficiary (Creta) also indicated that they do on-site confirmation these visits in conjunction with other auditors from the Ministry of Development and Investments, to ensure compliance with the MA. Results of these are communicated with the MA via the IIS.
4. Specifically, for mega projects, and especially these mega projects on the subway networks in Greece, technical reports need to be completed pre-materialisation – technical reports before the project starts need to include all technical information and the feasibility and technical elements of the project. In one of the beneficiaries that materialises subway networks, they work with a Building Information System (BIM) real-time monitoring systems that show how these technical report elements are set in the project, in real-time. If something changes in this system, there is a red flag raised by the BIM system that shows the need to intervene and solve an issue. For example, when a new subway line was faced with a large, unexpected void when digging a tunnel, the BIM system raised the alarm. Then, this triggered a process of technical meetings with project managers and mechanics to develop a response, this response was later agreed upon by senior management and communicated and agreed with the MA via IIS. MA and mechanics did an on-site verification and agreed on solutions. BIM serves diagnostically for the beneficiary, and thorough that, the MA knows and works similarly to confirm the issues and work on an agreement, via meetings and IIS information input.

Moreover, and to communicate emergent risks, the beneficiary, as required by law and the MCS, has a close relationship with the sub-contractors. As a first point, if an emergent risk rises during the materialisation of a project, both mega project and smaller size (usually environmental and sustainability projects), all beneficiaries discuss this with the sub-

contractors and relevant mechanics and project managers to see what it is, how it affects the completion of the project, and what mechanisms can be put in place to mitigate this. This later feeds to the MA through meetings, emails, and informal discussions, and via IIS. As a result, in that case, MA uses IIS and these meetings and discussions with the beneficiaries interactively, as well as diagnostically. IIS is the final formal system that is used for this communication, and for approving the project changes that need to be made to tackle any emergent issues. Therefore, the IIS also works interactively to communicate uncertainty in implementing projects and monitoring beneficiary performance. Here, the IIS is utilised interactively to make sense of emergent risks. In addition to that, the MA also utilises meetings interactively. Most project operators, when they need more information, or more regulatory compliance in the IIS forms submitted by the beneficiaries, to reduce response time, they do not directly refuse a beneficiary IIS request. Instead, they engage in informal meetings, emails and telephone calls to solve the issue, help the beneficiary submit what they needed to submit at the IIS and then accept the request, to save time. Especially in environmental and sustainability projects, small projects, the operators utilise these meetings with both the beneficiaries and the sub-contractors, mainly because the beneficiaries are small organisations and municipalities without technical expertise and structure, compared to beneficiaries that materialise mega-projects. Compared to transportation operators (which manage fund for mega projects), and mainly due to this distinction between beneficiaries, environment and sustainability operators have a closer relationship with beneficiaries, engage into more detailed meetings and on-site verification, and sometimes have the need to engage with sub-contractors (something that is not the case in transportation, they are strict there and they expect beneficiaries to communicate with sub-contractors and raise any issues). In these, meetings and discussions are used interactively to try and understand an emergent issue and support all parties as much they can for the project to move forward and on time. To demonstrate this process, an operator for a new subway line in Athens commented on an issue they had with digging the ground for the subway line. In this line, they usually find electricity cables and other underground networks such as waters:

> *"In order for the project to go ahead and find a way to complete the project, and to avoid losing funds from the country, many times, the national treasury is forced to pay money due to the delay of the project ... Because it is not their fault that the*

previous contractor did not do the groundwork for the next one to continue. Either it is the fault of the electricity provider, that has not gone to tell them where the cables are in the ground, or the water supply company, that has not indicated where the pipeline is or does not know how to find it. We have something like that. We have been looking for 2 years to find a pipeline. All this, however, does not pass through the hands of the MA. At most, we have to collect all of them (these parties), press them by phone every week for updates, and then secure resources from the national treasury to make up for this delay. Because the contractor asks for arrears."

6.4.1.4 Managing performance: risk management team meetings

Another technical control tool for managing performance is the meetings held from the risk management team on a regular basis. For instance, there is a meeting with the risk management team at frequent intervals (3-4 times) throughout the year, and more frequent intervals at the end of the programme period. This team consists of people that each represents their unit and is chaired by the CRO. Each member is responsible for risk at their own unit, and if something arises within their unit, they report it back to the risk management meeting, both for identification and to devise mechanisms in place to managed said risk. For example, in these meetings, among others, they see how the MA and project operators responded to one main target: responding to beneficiaries. That includes responding to pre-approvals, extensions, regulation checking, capabilities of beneficiaries, and all relevant approvals and confirmations that the MA needs to give for all project and sub-contract elements and modifications. It applies to all relevant checks and confirmations the MA needs to give for all stages of project life, from competition, to assessment, materialisation, and closure. That was 20 days during the 2014-2020 programme period, according to the MCS. As such, in one of these risk management meetings, they discussed reasons behind these delays, and ways to manage them and mitigate, with an aim at improving these responses. In essence, delaying these responses was a risk to the project, as it would delay the project materialisation. Most common reasons for delays were then recorded into a table and related back to mitigation and how to reduce these. Some participants indicated that one way to solve this is to ask the SRSA to revise MCS respond targets to more days, but that has not been implemented yet, and the same response target still applies. The same applies for court appeals target is 30 days, and the 60 days that is the target

for assessing project to include in the programme and providing a response. The IIS shows these targets and how each unit has performed in meeting these targets.

Another example of how the risk management team works is on the internal level. During the first year of the programme, in 2014, the units of the organisation were merged into one. This was something they were not expecting to happen, and it was mostly due to political pressures and the aftermath of the 2008 crisis which brought about economic measures in the Greek public sector, and the need to manage spending more efficiently. At that time, because the MA was not prepared, they did not effectively implement the merger and they experienced issue in operations and internal spending, as their main issue was that they did not have enough personnel to operate projects. As a result, they decided to get more prepared against such external uncertainties and, through creating the emergent events-pandemic risk category in the risk tool, they devised a way to measure the impact of possible organisational re-arrangements to mitigate possible issues. In 2021, the MA was broken down into two parts again, transportation and environment, and they were aware of the personnel shortage issues before hand. The team met to see and discuss unit needs and they devised a plan and a report to the Ministry to ask for personnel through legal public sector channels, and also ask for an external accounting consultant as the internal accountants were not enough. To understand this uncertainty, they devised a new risk category, measured for impact, and to mitigate it, they followed the legal route devised by the Greek Law for public sector recruitment.

Finally, and with the CRO being keen to that, the risk management team, in their meetings, brainstorms new risks that might have emerged from the operation of the different units that operate in the MA. As such, each unit representative that has been delegated to the risk management team, bring emergent risks to the to be discussed on how they affect internal operations, project development, materialisation and closure, external environment and so on, and they discuss how they can affect the programme. These risks derive from monitoring of the market, fiscal results and capabilities of sub-contractors, and monitoring the environment in general, through publicly available reports, stakeholder analysis, new technologies and laws in making material. The operators usually check for the effect of external events in the market, such as the most recent war in Ukraine that affected prices of materials, the effect of Covid19 on supply chains for project materials and equipment, as well as annual reports, or any other any publicly available information, to ensure compliance with laws and regulation and also

work to understand emergent risks and how they can affect projects, even before these projects are assessed and integrated into the programme. If an emergent risk is qualifying to affect the main targets of the MA, then it is brought to the attention of the SRSA to see how it can fit the risk management tool so it will be updated accordingly. If an emergent risk is not that impactful or is very contingent to a specific unit, then they discuss ways to manage it in that unit. To demonstrate with an example, and during the October 2022 risk management meeting, the team brainstormed a risk in that way. The meeting started with the agenda and people started talking about KPIs for the expenses that reflect one of the new laws. The team started by discussing what they do or do not do for their risks already and discussed some omissions they were having in their KPIs and targets. For instance, new law required the target of an operator to respond to a project expense sheet is 20 days. In general, all the participants in this meeting were discussing how this law affects their areas and different projects as well as they have been doing until now as a starting point to incorporate the new law and show how the new risks by the law are currently affecting the targets and the project cycles of the projects. In this conversation, the team discussed the update of the risk tool but agreed that was not necessary as it was difficult. However, they would create a report from their oracle system to show the progress and reports affecting their risks. They felt the update of the tool was not necessary at the moment. However, the changes will apply in practice to reflect the new law. The team also discussed the effects of the risks and the rest of the agenda risks for the new programme period as well. The new programme is also introducing a new oracle system.

Therefore, the risk management meetings serve as a technical control tool at the operational level, to manage MA performance in all levels of performance, internal of project performance. In these meetings, which are used diagnostically, the team identifies performance that is directly associated with project risks and discusses options to manage and mitigate those risks, effectively taking corrective action. Moreover, as indicated in the previous section, these meetings are also utilised interactively and in an enabling way, to induce learning of emergent risks, devise procedures to manage internal performance and monitor beneficiaries. That helps in reducing delays and is connected with one of the main MA targets, not meet the criteria to absorb all EC funds. This tool is designed with risk being at its heart, as moth of this process is associated with understanding performance and takin corrective action in an effort to reduce

risk associated with delays and EC fund absorption, as these are reflected into various organisational, programme and regulatory compliance key performance variables.

6.4.1.5 Organisational values

At the operational level of the MA, there is a social control that is utilised in an enabling way, when it comes to managing performance. All operators, as the majority of participants indicated in their interviews, when they need to save time, they go an extra mile to work with the beneficiaries to personally solve project issues that arise in all stages of project materialisation. That is a value that has been running throughout all members of the managing authority and for all elements of their work. Greek sense of honour (a cultural thing in Greece) and personal interest of each project operator. In essence, operators devise ways to constantly communicate with beneficiaries before a project stage documentation is applied, majorly through IIS, and before a project stage starts (from approval, invitation, pre-approval, materialisation, project and sub-contract modification and so on). In there, they utilise meetings, emails, phone calls and any personal/ informal means available to be proactive towards submitting forms that are complete, so as not to cause delays. These technical controls, used interactively, aim at communicating known risks and managing, mitigating them before documentation is formally uploaded to the system, and also communicate uncertainty, in a sense that they identify issues beforehand, that might not be known and if they arise in the project processes, they will delay the process, and endanger the main targets of the project: finish on time and with the EC fund absorption required. However, as a few participants indicated, because this is a process that is not recorded in the IIS, some might not want it, because it is not a recognised effort, and they end up not being motivated to engage with it.

6.4.1.6 Action Plan

To further manage the programme performance, at both operational and strategic levels, the managing authority is utilising an Action Plan, effectively a vast excel map, that produces information about the current state of the programme, its multiple projects, and effectively the level of EC fund absorption at any given time. In the action plan, there is information about projects (critical, non-critical, phasing), there is information about EC funding rolling and absorption and there is particular about how these funds are expensed by projects. This action

plan is devised at the end of every year and populated with all elements of all current MA projects, is consulted at the end of the year to see project progress and is a requirement from all authorities that monitor the managing authority and is updated every 2-3 months according to how project materialisation is maturing. As described by the director of the managing authority:

> *"The action plan, in practice, gives us a picture of all our projects, based on financial figures that related to the economy and the absorption of EC funds."*

Every 6 months, and with the interaction between operators, unit supervisors, the CRO and the director of the MA, this excel map is prepared, and updated, to show the level of maturity of all projects, both in the transport infrastructure and the environment and sustainability areas. This map aims at showing how projects have progressed, what funds they have absorbed and what funds they still need to absorb from the programme. And this map goes to every level of detail and every level of sub-contract for all active projects. It also shows the level of criticality of projects. The projects are classified as projects that are doing well, have absorbed most funds and they will be done by the end of the programme period, and projects that have not adequately absorbed funds. The latter are later classified as critical, meaning that they need to be focused upon for completion, non-critical, indicating that they can move to the next programme period round of funds, and dead, indicating projects that can't be completed within the programme deadline. An operator working for environmental projects summarised the action plan as follows:

> *"The action plan ... The risk management team and action plan are different from each other. Quite simply, conclusions do emerge from the action plan. How we work is as follows. Instructions and the basic file of the action plan are sent by the coordination service in the operational programmes, that is, to us. This thing goes down the project level and reaches the units and the project operators, that is, it reaches the last level of management, each operator completes the picture of his project in cooperation with the implementing body, or knowing for himself what condition each operator is in. All this information is collected, after the whole file has*

been completed, this now single file for the programme is created, which is discussed by the superiors with each other, and sent in response to the special coordination service. And that's where the whole picture that I'm explaining to you comes from. That is, which projects will be closed, which will not be closed, which will be phased, and so on. From there, indeed, the action plan is a tool to show you if the program is at risk."

In conjunction with the Quality Assurance System (QAS) of the organisation, this action plan is also used as map to show the basic KPIs that need to be met by the QAS. For that matter, to manage the operations of the MA, there is also a non-regulated, Quality Assurance System, that the managing authority has voluntarily implemented and adheres to. Product of the austerity measures of the post-2008 crisis, the Quality Assurance System (QAS) of the MA was first devised in 2011, to prove that they are capable of carrying out their responsibilities as an authority, which is the materialisation of the EC co-funded projects. This system is running as compulsory from 2011, but is now voluntary, still applied and used by the MA and overlooked by a Quality Assurance Officer (QAO) that is also a member of the risk management team of the MA. This QAS has also based its principles on the ISO 31000. In essence, the QAS is a system that ensures compliance with the MCS and all its rules and procedures that the MA and the MA units need to follow. As a result, the QAS delineates the rules and procedures that need to be followed by the MA, to adhere to the MCS. That is done to ensure compliance, but also to protect the MA against an issue that can be found by an external audit. However, the MA and the QAS team, has taken this system as step forward to include operational and communication procedures to be followed and adhered to, additional to the MCS procedures, that help the general cause of the QAS. The QAO is also ensuring that the QAS is running as intended, by carrying our internal audits at regular intervals throughout the year, ensuring compliance with the ISO principles and also making sure that if an issue arises to the system or the following of the MCS, then corrective action is taken. This corrective action is instilled by reports and the QAO monitoring the issues, how it manifests, how it is resolved and the implementation of its resolution, through a report by the MA unit that dd not comply.

The QAS also serves as a critical performance target management system at both the operational and the strategic level, with targets agreed at the strategic level. As the QAO indicated:

> *"A process we do within ISO, we did at least till recently…Because now we are in a very transitional time. We had a meeting of unit supervisors, in my presence as a quality assurance officer, and we did the so-called ISO system review, in which we discussed what has been done in the past period in the managing authority, what changes have been made and set goals for the future. The near future. The objectives and responsibilities of the units. That is, we were discussing... All absorptions and what interests the programmes is what work we deliver, how much this project will cost, what costs it will have, and so on. We do these figures in the so-called action plan, which every managing authority has, for the future. What it will give, for example, next year, in terms of expenditure and so on. We, in the review, had dealt with more strategic level style KPIs. That is, let's say that in 2022 we want 20 project integrations, we want to have no exclusions in terms of timetables. Because, in these procedures, there are also tight time limits. That you must get the proposal, and within 60 days decide, based on the papers, whether this proposal will go ahead or not. You can't keep it indefinitely".*

As such, the whole QAS serves as both a strategic and operational level tool to monitor MCS compliance and ensure strategic cohesion and performance management at both strategic and operational levels. Key Performance Indicators (KPIs) are set at the strategic level, are then communicated to the operational level and unit supervisors and project operators, and then the MA monitors their performance on projects, on a yearly basis. As such, this tool also serves as setting the required KPI levels to mitigate the risk of a project falling out of EC funds or timelines. The above tools, the action plan and the QAS, are interdependent and complementary in managing organisational operations, strategic objectives and risk. The next part of this section will present how this happens in the case MA with particular emphasis to the overarching research questions of the study.

Going back to the action plan, this map serves as a tool for monitoring, learning and decision-making for the programme, at both operational and strategic levels. The action plan also

complements the IIS as it provides more accurate and recent information about all projects, and also this information is inputted by employees who monitor projects. The action plan is more recent and more focused towards specific project aspects that need attention, e.g., absorbed funds, than the IIS which includes any piece of information about all project, for example it shows the general budgets for all projects and not in each project in detail. As one of the participants indicated:

> *"The Action Plan is something else. All these are linked, but the action plan is not done through ISS. It is done every six months, to capture the picture of the projects, based on what contracts they have, whether they have contracts, whether they are going to be auctioned immediately, what expenses they have, how far they have progressed. Whether the projects will be closed and how they will be closed, according to specific rules that the NSS (special coordination service) has tied to us. This is how we structure the action plan. The risk management team and action plan are different from each other. Quite simply, conclusions do emerge from the action plan. How we work is as follows. Instructions and the basic file of the action plan are sent by the coordination service in the operational programs, that is, to us. This thing goes down a level and reaches the units and the project operators, that is, it reaches the last level of management. Each operator completes the picture of his project in cooperation with the implementing body, or knowing for himself what condition each operator is in. All this information is collected after the whole file has been completed, in a single file. Tis ingle file for the program is created, which is discussed by the superiors with each other, and sent in response to the special coordination service".*

At the operational level, the action plan shows absorption targets for individual projects and the programme as a whole. It is used to manage performance in EC funding absorption and used diagnostically to see how all projects are doing in meeting their fund absorption and if not, the MA takes corrective action by allocating funds to more suitable or more mature projects, or anywhere that can be founded to absorb funds and not lose them, or phase projects to next periods (deadline last year of programme +3). Effectively, it manages risk by showing which projects have high risk of not being completed according to how much they have absorbed in funds and mitigates the risk of EC fund loss. The same applies for the deadlines. The Action Plan works the same with deadlines. Moreover, the action plan includes the funding

absorption of projects. In there, the MA looks at how programmes have absorbed funds, usually yearly. Or each year, at the beginning, the MA sets targets for the absorption of each project in the action plan, and then, they see how these targets are met at the end of the year, why and why not, and they devise mechanisms to mitigate risks as before (fund movement to other projects, phasing etc). The action plan itself classifies all projects based on a variety of categories, finally reflecting the main KPIs of the projects i.e., completion date and absorption, regulatory compliance. Based on that and based on if projects are missing signed sub-contracts, or if they have progress issues and so on, the Action Plan classifies projects as completed (or close to completion), incomplete and needs attention on one of its elements, and phasing to be completed in the next programme period, part funded from current period and part-funded from next one. The action plans also serve as a diagnostic tool to raise alarms with projects i.e., there might be projects that have not been assigned a sub-contractor yet, while they should have started in the current year, and they need attention. That way, the MA and operators in particular, chase these projects, at the operational level.

Effectively, the Action Plan, complemented by the QAS, serves as a risk performance management tool as it delineates all critical targets of the projects and how these are met, in an effort to manage risks associated with project completion. This vast excel map, shows the key areas of project completion that serve as a technical control tool used diagnostically, to monitor risk associated with project completion, and effectively, absorption of EC funds. As a result, risk is central in the operation of the Action Plan and it is a system that monitors standalone risk performance, part of the wider framework of performance management within the case MA.

6.4.2 Managing risk and uncertainty: controls complementing performance management

6.4.2.1 Overarching management control framework.

The overarching rules of operation and control that the managing authority needs to adhere to, is a set of rules and procedures imposed by the European Commission, embedded into Greek law regarding organisations managing European Commission funds and overlooked by the SRSA. This system is called the Management and Control System (MCS), and it is the backbone of rules and procedures that need to be followed by the managing authority, in

monitoring and managing the materialisation of various projects utilising European Commission funds. The term "Management Control System" is the exact term utilised by the case organisation and the SRSA, which is a direct translation from Greek and the term used by the managing authority. According to the European Commission and the Greek law manuals as of 2019, this MCS for the 2014-2020 programmes is defined as:

> *"The ensemble of management rules, that exist in co-dependency, are formed with specific organisational structure and develop individual activities with an objective purpose to correctly manage the European Commission funds (with economy, efficiency and effectiveness".*

These rules are divided into 9 areas that delineate the acceptable domain of action to manage the programme. Table 9.5 describes these areas in more detail, as these were found in the documents of the MCS, provided by the QAO at the first interview.

Area 1	Selection and approval of projects. This area of the MCS delineates the processes that need to be followed to evaluate and select projects. In here, the methodology, steps that need to be, criteria for selection, invitation of beneficiaries are drawn. Moreover, this section delineates all the approval criteria and steps that need to be followed to implement these criteria.
Area 2	This area of the MCS tool is associated with establishing the appropriate monitoring and verification of projects. In here, monitoring process and procedures of projects and fund

	allocation are drawn. That includes rules on project declaration procedures for beneficiary invitations, monitoring of project contracts and sub-contract regulatory commitments, on-site verification rules and procedures, modification of project and sub-contracts, project completion rules and procedures, monitoring of long-term commitments of the beneficiaries (post project completion), and any rules of fund recalling, if necessary.
Area 3	Area 3 delineates the control, fiscal correction and recovery of control bodies. This area does not apply to the managing authority, but to the governing bodies of the Greek national authorities regarding their fund participation in programme if needed. In here, auditing procedures for fund, procedures to recall funds if they are not abiding by the rules, and rules to report of irregularities, are set.
Area 4	In here, the rules and procedures of fund flow are set, including how project funding is allocated and how the payments of this funding from the European Fund are made.

Area 5	Area 5 delineates the key elements of the MCS application and monitoring in the Greek context. In a nutshell, it shows how the MCS should be applied to the SRSA and the Greek National Coordination Authority. That aims at monitoring the correct application of the MCS and its improvement through feedback and corrective actions, which are also reflected in this section.
Area 6	Area 6 delineates the rules of the assignment and monitoring of middle bodies that are overlooking the managing authority (and, in fact, all other managing authorities that monitor EC funds). In here, the assignment and monitoring steps and procedures that need to be followed are discussed, to provide the grounds for when the managing of European Commission funds are given to middle bodies to be managed, instead of the managing authority.
Area 7	Area 7 of the MCS is associated with the rules and procedures of how each programme should be monitored by the MAs. Programme monitoring should be done in a coordinated fashion, by the monitoring commission for the programme. That commission is usually from the relevant ministry that overlooks the MA, in

	conjunction with the SRSA for the MCS. In here, rules are provided for the support steps that need to be followed to inform this commission by managing authorities. programme commission reporting procedures are also set in this section of the MCS.
Area 8	Area 8 of the MCS is associated with the rules and procedures for payment applications, annual transactions, and statement of management for the EC funds. These rules and procedures are associated with setting up, certification and submission steps and procedures for EC funds, setting up, certification and submission steps of managing authority accounts. All the above payment rules ned to adhere to accepted accounting rules, management and adherence of all managing authority funds, accounts and transactions according to accounting regulation. Steps to report all the above to the EC to show how the funds were utilised to materialise projects are also clearly set here.
Area 9	The last area of the MCS is associated with the setting up of the Risk Management procedures for all MAs. In here, all risk

	management procedures are set, including processes and steps to manage fraud risks, with a clear definition of the two main fraud risk categories: indication and suspicion of fraud, and how to proceed with each category when it appears. In that case, later on, confronting complaint procedures are delineated. The key element here is that this part of the MCS sets the processes, procedures and definitions of risk for all MAs. It also delineates the risk tool that needs to be used by every managing authority.

Table 9.5: Areas of MCS rules and descriptions.

Indeed, this system delineates all procedures that need to be followed by the case organisation for the whole life cycle of a project and serves as a boundary control system at both organisational levels. At the operational level, this system delineates all procedures that need to be followed from before the integration of a project, the integration procedures and what projects can be funded, how these projects are monitored and how they should be signed off when completed. A core rule in this system is the requirement for all European commission's fund managing organisations to implement and run a fully functional risk management system, as described in the previous section. Each of these organisations can implement a risk management system as per their needs, however, as the rules are flexible towards that. Within these rules, this operational boundary system, risk management, is integrated as a separate technical control, delineating the risk management procedures that the MA needs to follow. The MCS is used to manage the whole programme, including risks and uncertainty, at all organisational levels, and delineates the normative framework by which all procedures for project materialisation should work. As the CAO established in the initial interview:

"It is essentially a management and control package. It was originally a set of procedures, ranging from planning to the completion of some actions of the program, and it had detailed procedures, and it still has. It has been modified in many places, but it is dynamic this system, modified in its implementation just fine. So, this system told us how we would do our job. That is, how will we finance projects? Planning must be made. We need to issue invitations, which in detail now will have to ask for some things, very analytically. 20 things to ask for. What does the beneficiary do? When he sends us a missing sentence, what do we do and how do we respond to him? When we lack some important things, we reject it. When we lack someone, we can make up for, we ask for a supplementary act. Then its implementation begins. When do we do the on-the-spot verifications, to see the on-the-spot checks on the project and/or on the project files, how it will be recorded, say, in the beneficiary's offices. Such things are covered by the management and control system".

The MCS is utilised at both strategic and operational levels of the MA to serve as a boundary control system to manage strategy. At the operational level, boundary controls are setting the acceptable domain of employee action, as reflected in risks to be avoided (Tessier & Otley, 2012). For operations, or the actual materialisation of projects, the MCS delineates the acceptable domain of action and the domain of activity that needs to be there when selecting, materialising and closing/finalising/delivering projects, including fund movement if projects do not go well. These steps include various technicalities that need to be adhered to such as: fund absorption reports than need to be produced at regular intervals, sub-contract change reports where needed, fund flow reports, agreements for project stages between the beneficiary and the managing authority, and selection criteria of projects. The MCS also includes, as stated before, the rules for pre-approval on project pre-integration. The MCS states that the integrated information system that supports project monitoring, needs to have the most accurate, complete, relevant, and updated information for all projects managed by the managing authority at a given point in time. As one operator described:

"Look, the IIS information system is made to capture all management. That is, its structure, each element essentially, is reflection of the MCS. So that's where all the processes are captured. Therefore, an effort has been made by those who have set up the program, to set up the procedures and commitments that exist from the MCS.

Commitments, for example, when an update comes in that the 20 days someone had to give an auction pre-approval or something like that has been exceeded".

The MCS has risk management as central to its effect. All the processes and procedures agreed in the MCS have a single aim: to mitigate risks associated with delays and under-absorption of funds. All procedures are set to offer the optimal way operators and the MA need to work with beneficiaries and regulators, in order to ensure appropriate completion of projects. This MCS system, as mentioned before, is not designed by the managing authority, but is imposed to it and they have to follow it in their projects and fund management, or even the internal operations of the organisation. The core rules of the MCS are presented as follows:

1. All communications for the projects need to be there and occur via an integrated information system (IIS). That includes communication between the managing authority and the beneficiaries for all steps of the project materialisation: from announcement, to assessment, to assignment, to materialisation and to closure of project and sub-contracts.
2. Risks arising through these steps are communicated via the IIS in all project steps. The way it works is that the beneficiary that has received the funds to materialise the project, uploads information for completion of project stages. If a new risk or something that has not been confronted before in a project, arises, this is also communicated via the IIS, though a specific function called "modification of sub-contract". In there, the beneficiary suggests that there will be a delay in the project, justifies the delay, and provides all relevant information. The managing authority sees that and decides what to do with the project. If they agree with the delay and they find the justification sufficient, then they give their green light for the project to continue. If not, they discuss options to make changes. IIS then ranks projects according to risks from higher to lower.
3. If any development has been uploaded in the IIS by the beneficiary, the MCS requires 20 days for the managing authority to respond.
4. The managing authority, needs to operate a clear, detailed, and operational risk management system and tool, as dictated by the MCS.

For example, within the MCS, there is set of rules that are followed for communication purposes between the managing authority and the beneficiaries, is at the stage of pre-approval of the project. Once a project has been assigned to a beneficiary, and before it is initiated, the managing authority meets with said beneficiary to confirm capabilities, or both the beneficiary and the sub-contractors, to agree and check that these capabilities match the criteria of Greek and EU law, and that all parties are capable of completing the project in the required timelines. Effectively, this works as a pre-initiation risk identification and assessment, according to MCS. In this situation, the IIS and informal meetings are utilised. The aim of this process is to ensure all risks are identified, to the most possible extend, and that the beneficiary and the sub-contractors they have assigned can finish the project. Beneficiaries are providing all necessary information in the IIS or are checked fiscally, and sub-contractor fiscal capabilities are also confirmed. All this information flows through the IIS. Thus, a technical control is utilised here to diagnose the requirements of a project, against specific criteria. This is another example of how a technical risk control is associated with the overarching control infrastructure of the case organisation. As a member of Unit Gamma summarised:

> *"There are also reports within the IIS. There is an executive report, which results by cross-checking the IIS for example the end date of a project given by the beneficiary, what percentage of expenditure has been spent from what they are supposed to consume over time... And depending on this, the project is classified if it is in the phase of completion, if a monitoring report of the operation should be made and documents with corrective measures should be made to the beneficiary. Or, it has some categories, let's say, that classify the works, and depending on them, we also take corresponding actions towards the beneficiary. In other words, it classifies projects based on their completion. For example, some projects haven't even signed a contract".*

Moreover, the managing authority is utilising communications with beneficiaries, at the operational level, as an additional operational boundary tool, to also check that they follow the required regulation for each project. At this point, the IIS is utilised interactively to point out adherence inefficiencies. Another operator also commented:

"Yes. In all management programs we work through the IIS. Everything passes through the IIS. There is, let's say, the request for project tender documents, which the beneficiary submits there, we fill in the appropriate lists, we see if they comply with EU and national legislation, we give a decision of pre-approval, and then it is approved by the financial committee by the municipality, which then goes to posts the summary of the result and start the tender process".

Another example of the above, depicting a fraction of the risk management rules in the MCS, and showing how the aforementioned risk, consideration occurs, is the way the fraud risk management team operates in managing risk and uncertainty, specifically associated with fraud. All fraud risk management procedures that the MA needs to follow, come from the MCS. It is a process that is provided by the MCS by the PADF program for 2014-2020, and, based on this process, the MA has formed a team, with an appointed fraud risk management officer responsible for fraud issues and they have also appointed a team, with which they cooperate with each other because, according to the MCS, there is a tool they need to follow. This tool, an excel with many levels, follows the process of implementing projects, from proposal, evaluation, integration, tendering, contract and so on, with many questions, where the fraud risk management team has worked it out, and they have rated the risks they have identified, they have identified the measures to mitigate them, and they have assessed any residual fraud risks. Despite views from the fraud risk management team describing this as static, it is something that, essentially, includes the entire management function and all the procedures for monitoring and implementing projects, and, when a case of fraud arises, a recorded complaint for example, they manage by coming back and evaluating their tool again, to see how it behaved in that case or if they need to add a measure or modify an element at this tool. This is the basic process, which is utilized interactively. And the other thing that differentiates risk management and fraud risk management is that, in the case of the latter, it exists through the websites of all EC funding MA programs and anyone is given the opportunity, if they want anonymously, to submit a complaint about anything that concerns the organization, and the projects and organizations around it, and this needs to be registered and then processed. In giving exact details on the process and anti-fraud risk management procedures, one of the participants commented:

"What do we mean by fraud? First, we need to define the levels. First, it is an irregularity, which may have occurred, that may or may not have violated the law. We are not authorized to determine whether it constitutes fraud. We hardly examine whether there is evidence of fraud, according to the procedures by which we will explain, and these are then forwarded to the national transparency authority followed by public prosecutorial proceedings. Which will conclude whether this indication constitutes fraud. And before we go any further, let's identify the difference between irregularity and indication of fraud. The key difference is when there seems to be intention. Where there appears to be an intention for the irregularity committed, this may be an indication of fraud. If there is no intention and a simple mistake was made, obviously, it is a simple irregularity. This is the separation. Therefore, to conclude that something is fraudulent, it has the procedures of the prosecutors of the courts, and investigations, of which we are not competent, who are a more administrative and administrative service, who can examine such a case of fraud or irregularity. With the data we have, we make an initial assessment of this data, and conclude, which we pass on to the competent authority".

For that matter, there are several procedures and rules created by the fraud risk management team to address fraud risk. For example, there is an appropriate and detailed description of project elements and procedures, to not allow for lack of evidence when they investigate a fraud claim. The second element is that they have created an easy and well accessed fraud complaint system to enhance transparency and create an easy ground for anyone to file in a complaint. That in turn creates a feedback system of not only solving fraud when it happens, but also updating systems and the fraud risk tool, to decrease the risk of fraud in the future. That is done by running the fraud risk tool again, to see how it works, update procedures and re-visit risks. For internal fraud risk, all employees follow the rules of external bodies such as Transparency International and the Greek law. All employees have signed forms that they have no conflicts of interest with any of the project they monitor, and the sub-contractors have signed good faith contracts with beneficiaries that they will not engage in fraud in any moment of project materialisation. These are a few procedures that are followed at the strategic level to ensure compliance and to not deviate from law and regulation, and create credibility and conformity, to avoid loss of funds. Unfortunately, although the fraud risk tool was described well by the

fraud risk management team at our focus group, they did not allow access to it. All the above apply for all project, mega or small, at the MA. As evidenced from this example, the same technical controls, associated with known and emergent risks, as described at the end of the previous paragraph, are exactly utilised by the MA, for fraud management. In the end, if the fraud risk tool needs to be updated, the SRSA will be informed through a meeting and take all necessary actions.

Conclusively, the MCS, and the way it is designed and implemented-followed by the organisation, is majorly a technical control system that delineates the acceptable route of action and procedures for all elements of managing projects, at both organisational levels, utilised in a constraining way. At the operational level, the managing authority utilises the MCS in a constraining way, and it is a technical control that is also associated with providing the rules of conduct, if a new risk arises in a project. As such, the MCS controls for risk through its main operations and delineating risks and optimal action for emergent risks, mainly attending to reducing risks and emergent associated with project delays.

As an additional boundary technical control at the operational level, again utilised in a constraining way, all processes of projects and sub-contracts need to adhere to National and EU regulations, especially rules and regulations associated with the PADF. For example, projects need to adhere to the widely recognised Greek Law 4412 for public contracts. This is Greek National Law, that reflects the EU law, and delineates the acceptable domain of activities, procedures and rules to be followed, by beneficiaries who undertake public funded projects. This law covers regulation that needs to be followed from the competition, pre-approval, integration, materialisation and closure of project and sub-contracts. This law is mainly associated with the selection of sub-contracts by the beneficiaries and applies to these sub-contractors. This law also dictates that all projects, irrespective of budget (mega-projects or smaller ones) need to have a folder associated with managing risks, and this is how risk is reflected within this boundary control. This law is not strictly adhering to the managing authority, but more to beneficiaries. However, the managing authority needs to monitor the application of this law to all relevant projects and sub-contracts, to avoid risk of delays and loss of funds. The same applies to other regulation that needs to be adhered to by beneficiaries that undertake projects with funds managed by the case MA. For instance, there is law 4270, another Greek National Law, that demands for fiscal frameworks to be implemented and

applied to private organisations that undertake EC funded projects in Greece, according to instruction 2011/85/EE reflecting the EEL 306/41 framework. Effectively, this is a fiscal framework that needs to be implemented, adhered to and audited, as applied to firms and organisations that materialise public contracts in Greece. Another regulation is how beneficiaries adhere to the PADF framework for the selectivity criteria of projects. For example, during the competition for a project, a beneficiary or sub-contractor will be assigned a project. If a certain beneficiary is not happy with the process, they can use the court appeal authority, to appeal for the criteria of assigning the project to other beneficiaries, or on the grounds of any misconduct during that process. To avoid issues with project delays due to that, the managing authority, in collaboration with the ministry and the Greek regulatory bodies, reduced the process to a few weeks from a few months, to reduce delays, but some projects are still not resolved in time. This is an example of adherence to the law, and communicate or co-implement changes, to mitigate risks that cause project delays.

Other examples of laws and regulations that need to be monitored by the MA are the Environmental Impact Assessment and Waste Management law for public contracts. Especially for projects in transportation infrastructure and networks, such as subways and trains, environmental reports need to be presented on these as a pre-requisite for such a project to be eligible for EC funding. Deviations on these need to be communicated with the managing authority as per MCS and through IIS. Moreover, when a project encounters archaeology, a key and core known risk by the managing authority due to the geography and history of Greece, or expropriation of land, certain Greek national laws need to be adhered to. For example, if archaeology appears during the materialisation of a project, e.g., a subway project, or a new building project, then there are certain procedures that need to be followed, negatively affecting the project timelines (and cannot be worked around). The first instance is that the Ministry of Culture needs to intervene and follow a set of procedures and rules to analyse the site, and assess and excavate the artifacts, before the project continues. Similarly, for expropriation needs of a land, there is a ground composition risk that might apply. In that scenario, Greek law dictates that based on composition classifications, different depths of foundations need to be constructed, sometimes not initially assessed by the mechanics before the project was materialised. All these delays the projects, but they need to be legally overcome for the projects to continue. However, the beneficiaries not only need to communicate these via an Integrated

Information System (IIS) and other informal meetings but also seek approval from the managing authority to proceed (delays justified through IIS). In additions, and specifically for mega-projects in transportation (over 50 or 75 million euros) a 150 pages report need to be presented to show adherence to specific assessments – fiscal capabilities of beneficiaries, risk assessment, project planning and operationalisation, and technical pre-materialisation assessment. Effectively, this process ensures a smooth materialisation of these projects and shows what known risks are there and how they can be mitigated. Finally, and during the pandemic of Covid19, adherence to Greek Health Ministry workplace regulations was pursued, which were communicated to all the units of the managing authority, to ensure compliance, from the internal management unit, Unit Gamma. These rules were later implemented to the managing authority operations and delineated working rules, from how to work from home, to how to enter the building, how to arrange employee movement office spaces to adhere to social-distancing, reliance and operation of working from home software to full transparency from working from home to ensure people are working e.g., transparent tasks completed, and deadlines met.

In general, project changes that adhere to these two laws, especially in law 4412, can affect the deadlines, materialisation, and closure of all EC funded programmes, and they need to be communicated with the managing authority to agree upon, make funding release decisions, and see law compliance. Not doing so, embeds a risk of not only not completing projects, but also completing projects that might not adhere to the EC framework, resulting in loss of funds, both for these projects and for the national treasury (wrong-funded projects will be given less funds in the future, or money for incomplete projects as per final deadlines, might need to be returned from national funds). All the above regulations, and specifically for project element requirements, are utilized by the managing authority as a boundary technical control tool, at the operational level. In this tool, risk is central, as reflected in the non-compliance of project elements, with relevant laws. As such, risks and uncertainty are not separate with rules and regulations, they are the second side of the same coin. In essence, these rules for every aspect of project materialisation and operation, need to be adhered to for the smooth completion of projects and to not lose funds, through delays of non-compliance. Since the MA needs to monitor regulation and how this applies to beneficiaries, a mix of technical controls are utilised here, one used diagnostically and one interactively, to manage risk and uncertainty,

consecutively. As seen above, adherence to regulation is monitored from the MA via an oracle information system. In there, the law and regulation, in terms of deadlines, criteria for selection, fund absorption, among others, is checked to be as required, and this tool is used diagnostically and in a constraining way. Moreover, when it comes to delays or issues with projects, the MA, utilises interactive informal meetings, to discuss the issue with the beneficiaries and agree on a course of action, to avoid materialisation delays. Indeed, this technical controls, used in an enabling way, as indicated by the MCS, is the constant communication between the managing authority and the beneficiaries, majorly occurring though the IIS, and sometimes through informal meetings (these meetings are not regulated by MCS, but utilised by managing authority and beneficiaries interactively, as an operational performance control). For that matter, interviews with all beneficiaries (and with all project operators) revealed that the MCS has a clear and detailed procedure of how to communicate project delays, needs for extension and any issue with the projects, through IIS inputs. Effectively, if a delay happens to a project due to a known risks that has arisen but at a different level than expected, or due to another emergent risk, the beneficiary is obligated to communicate by inputting this information to the IIS in a timely fashion, justify this delay with description, legal or technical documents, and wait for the managing authority to review and authorise this delay. If the managing authority agrees, then the project continues. In the rare event they do not, then funding release might be delayed or even stopped. But that is rare, as most common and known risks have been assessed in the pre-materialisation phase, and if a project is at the stage of being materialised, then the funds have been assessed to be put into a project that meets all the necessary criteria. In more detail, the IIS communication process works as follows:

1. The beneficiary initiates an informal communication (telephone call, email, or meeting) with the manging authority, and the subsequent project operator, to discuss the issue, and agree on next steps.
2. All information about the issue that delays the project, or a sub-contract is uploaded into the IIS.
3. If further information is required by the managing authority, then they make a request to the beneficiary, through the IIS.
4. Solution is provided, delay agreed, and the managing authority gives the green light (pre-approval) for the project to continue.

If a sub-contract of a project needs to be modified for any reason, then the same procedure is followed. Risk and emergent risks are communicated via a combination of technical formal and informal controls.

Finally, to make sure that they monitor how the organisation is performing against all MCS rules, regulation and procedures, they have designed an internal audit system to ensure compliance. According to the ISO that they need to adhere to, there is an internal verification team within the MA that audits all procedures and organisational aspects, as they are dictated by the MCS and the EC and Greek regulation. This team is accountable to the QAO with written reports. This audit is to check performance against regulation, MCS, and any other operational other requirements. That way, they try to shield against issues and also make sure that if an external audit for all these occurs, all systems and procedures meet the legal and regulatory criteria. If an internal or external audit finds an issue within the MA, then there is a report initiated to the QAO and the team, then this team dictates solutions and monitors steps for implementing this solution, usually through reports. Effectively, this system works as a performance management tool and a way to manage operational performance of the MA, when it comes to their operations.

Conclusively, the MA, at the operational level, utilises a boundary control system that comprises of a mix of technical controls, which are all utilised both in an enabling and a constraining way and either diagnostically or interactively. All these technical controls comprise the boundary control system of the case organisation, associated with managing operational activities. Within each control, as described above, risk is central and clearly connected to, as part of the wider boundary control system. Risk and emergent risk are not independent from this infrastructure, but rather included in this infrastructure. For instance, the IIS inputs to diagnose risks associated with the materialisation of a project, are used both to ensure compliance with law and regulation, and, at the same time, to ensure the beneficiaries are performing as required. The same applies to the interactive use of meetings to discuss emergent risks. Using this control, the MA is trying to understand compliance with law and regulation, and also make sense of emergent risks and how beneficiaries are performing in mitigating them. All the above, are complemented with an internal audit procedure to ensure compliance.

6.5 Managing risk at the strategic level: PMS and complementary control systems

6.5.1 Strategic performance management

6.5.1.1 Action Plan at the strategic level

As mentioned before, the main tool to monitor programme performance and risk management at the strategic level, is the action plan. In the interview with the director of the MA about the action plan, he commented:

> *"The action plan, in practice, gives me a picture of the projects, based on financial and fund absorption data. So, looking at the action plan, we can understand whether a programme area is going well, and depending on how things are going there, in terms of absorption and economic progress, we can take corrective action. Let's say that we need to do more transportation projects, bring them into the program, or some road projects get them out of the program because they have a high risk of not being completed and as a result funds are lost. In any case, we can say that this is the programme, these are transport projects, and we cannot integrate these projects, but we can integrate them into the environment, and we are doing that in practice. So, part of the doubt we have and the risk of completing transport projects, and meeting the EC fund budget, we can balance it with environmental projects. It is something we do, especially at the end of the programme period. This is a monitoring tool that helps us manage the situation as well as the risk".*

In essence, at the strategic level, the action plan is a risk monitoring tool that shows the level of completion and EC fund absorption of all projects at the MA. Using that tool, they can re-arrange funds, or integrate new funds when they can, to ensure that EC funds poured into the programme are not lost. At regular intervals, and especially at the end of the programme where they need to close it with the highest EC fund absorption possible, the action plan serves as a risk mapping tool, in a sense that it shows, which projects have a high risk of not being completed. By populating this action plan excel with their own forecasts about projects and specific unofficial data they find useful for completion (e.g., completion dates, absorbed funds) from the projects, complemented by IIS official data when needed, the MA is monitoring the

risk of all it projects being completed or not. For example, if a project is under-absorbing funds, is at the end of the programme period (last 12 months) and to be completed and absorb all funds it needs more than 12 months of materialisation, then this project has a high risk of not being completed. Information like that is inputted by the MA in the action plan. If changes are made and funds are re-allocated, the action plan is revisited and updated, as well. Then, the programme might be revised as well. As the QAO indicated:

> *"All absorptions and what interests the programmes is what work we deliver, how much this project will cost, what costs it will have, and so on. We do these figures in the so-called action plan, which every managing authority has, for the future. What will the programme return, in terms of fund absorption, for example, next year, in terms of expenditure and so on. We, in the review, had dealt with more administrative style KPIs. That is, let's say that in 2022 we want 20 project inclusions, we want to have no exclusions in terms of timetables. Because, in these procedures, there are also tight time limits. Then, and within 60 days, we decide based on criteria, whether this proposal will go ahead or not, and the programmed be revised. You can't keep it indefinitely".*

Equally, for uncertainty monitoring, the action plan is used as a tool to identify issues with projects that have not being picked up by that time, or by their operators. For example, at the last 12 months of the programme, a new regulation about public projects changes. This has not been yet incorporated in the projects, but it might have an impact on the MA projects. The director meets with the relevant units and unit Gamma representatives, to discuss the effect of this new regulation and assess the impact on projects in the action plan, and finally decide on the level of risk these projects affected have, in order to be completed. All this is done at the strategic level and with meetings with the different project monitoring units at the MA, to make sense of this uncertainty. Therefore, at the strategic level, the action plan is used diagnostically as a technical strategic performance control system.

Another example of monitoring uncertainty through the Action Plan comes from the operation of a horizontal team within the MA, that overlooks the programme, and specifically the spending of the programme and its projects and works closely with Unit A and the programme director, to propose and make strategic decision about the programme. This horizontal team

overlooks the programme at strategic level, and they utilise both the action plan and information from the IIS to see deviation of budgets for the whole programme, with an aim at monitoring the performance of the programme and the MA, toward the main target which is to absorb all EC funds. To describe this, a member of this team commented:

> *"Another big part of my team has to do with the public investment program, that is, with the financing of projects. Without money, the programme doesn't go ahead. We already sometimes have some obstacles that we get a little stuck not having a normal flow of funding. Because whatever we do, we do it with national resources first, and then we ask for funding from the European Union and the PADF program. So, if the Bank of Greece doesn't have enough money to give the money immediately, payments for the projects are frozen."*

Therefore, in this horizontal team, they do this check to see the usage of funding, and if needed, they re-allocate funds to projects. For example, if they see that a project, through the action plan, does not absorb as intended, they re-allocate the fund to another less risky and more compatible programme, that has a better chance to absorb these funds. This is done in an effort no to lose EC funds. This is also communicated to all project operators, and how changes will be made in fund allocated to their projects, if affected, so that they have a greater picture of the programme, conform to the greater strategic target of the programme which is the EC fund absorption, and in an effort to make their work more interesting and meaningful. To support this effort, this horizontal team is also utilising IIS reports. As the member of this team indicated:

> *"Moreover, in this team, we do, with many of my colleagues, a great number of reports. That is, the IIS is a tool that has a lot of information in it and, with the right questions, gives you correspondingly many answers for the greater picture of the projects. So, we work with all reports, whether they are large/executive at the strategic level or smaller, project, accordingly. And you see progress every 15 days every time. That is, you can enter the IIS and see every 15 days how a project is progressing. So, we are also putting out a trend, which has to do with fund dynamics".*

These reports serve as a tool to monitor fund absorption in projects and, in conjunction with the action plan, at strategic level, they monitor fund absorption and are used to re-allocate funds to more efficient and less risky projects. For example, they see the trend of transportation mega project funds, and they check the trend for environmental and sustainability projects. Given that both areas need to absorb EC funds on a 50-50 basis, if transportation has a lot of projects that have covered 50% of funds, then they look to see how the environment is doing to meet this quota. That is another case of re-allocating funds. So, the horizontal strategic team, checks the action plan and IIS reports to see project maturity, and fund absorption. Then, it proposes changes to fund allocation, after discussing with project operators and their supervisors, and the programme director. Finally, re-allocation of funds is done to meet either the 50-50 quota between transportation and environment and sustainability projects, or based on meeting the main programme target, that is, to absorb all EC funding. As the participant from the horizontal team described, summarising all their work at the end of the current programme, to support all the above descriptions:

> *"We have agreed that in order for the programme to be completed as intended, we need to absorb 800 million, which I have broken into quarters, if at the end of September when we made a request, I see that I have fallen far off the forecast we had made, the phone calls begin, the issues begin... What problem do we have in the project? Is it political? Is it economical? It is the contractor's and substitution; Need to do something fast? Do we want a revised arrangement with a sub-contractor of a project, that changes the contract a bit, so you have to pre-approve the contract and some changes? So here, every quarter, internally, the whole MA, we look at the goals of the quarter with what we achieved. And what went wrong. Which, I had done at the strategic level."*

It is evident that this process, followed by the horizontal team that overlooks funds absorption, is used as a strategic performance management technical control tool, to monitor the uncertainty of the organisation. As such, risk is reflected within the existence of this team and their operations and monitored and managed through information gathered from the action plan and the ISS. In line with programme and project completion, this team also uses this procedure and monitoring, to address the risk of under-absorbing of EC funds, by monitoring the projects that have a high risk of not being completed, discussing re-allocation fund arrangements,

setting the main strategic objectives of the MA and making sure all employees know how their work fits with that, and, when risks emerge, monitor the environment of the organisation to address uncertainties and mitigate their impact, especially in projects that are under-absorbing.

Furthermore, at the strategic level, unit A monitors the whole programme for strategy implementation and uncertainty, with a clear focus on managing risk. The main goal of unit A is for the programme to close securely. In that respect, they see the risk at programme level, and not at project level that most operators do. The tools they use to monitor uncertainty and its impact on the programme are the programme itself and its characteristics/updates and external environment, the assessment report of the programme, which is done every year by the EC and by Greek external audits, and the possibilities they have, to revise the programme, if needed. To monitor the programme, unit A reflects the programme progress against the MCS and its updates and making sure that the programme follows any new MCS developments, especially at programme and project assessment and integration levels. They also monitor the programme progress through yearly reports from the EC, the IIS and the Ministry, regarding programme assessment. In particular, unit A draws various reports from IIS, wholistically for all projects, to check integration criteria, project maturity and progress and expenditure reports. This is done to see the extend of deviations from programme targets.

Speaking of targets, unit A, as well as project operators, usually check the completion and main target of the MA, against all targets mentioned in the operational level, which include the EC targets for programme inclusion. For example, there are EC targets for transportation projects, such targets for projects to reduce miles, reduce transportation time and so on, which are cleared and communicated via the EC policy. They serve as targets to be met during the project assessment process. These targets are in IIS as criteria for when projects are assessed for integration. There are also EC targets for environmental projects such as, reduce CO2 emissions, and so on, that need to be adhered to by the programme and its projects. For instance, in the case of the environment, the agreement documents provide targets for transportation and environmental projects (Greek Ministry of Development and Competition, 2014). Found in the Greek ministry document, these targets refer to complete systems of recovery and disposal of garbage, a completion of a proper and effective network to manage industrial, sanitary and

other dangerous substances that can harm the environment, as well as other bio-waste. In the case of transportation, targets range from completion of proper and effective road networks to avoid accidents and support transportation of vital roadworks or connect all islands with airport bases for the convenience of citizens. These are but a few targets that need to be complete in both transportation and the environment/sustainability. Any project that does not contribute to these targets, cannot be funded by EC funds. Indeed, these are general targets provided by the EC, and they need to be adhered to when a new project is integrated, while they reflect the national circumstances and needs. However, the fact that they are general means that the environmental assessors and operators need to specific projects to include. But, due to the generality of the targets, there is uncertainty involved in a sense that some projects might not be clear as to where they fit these targets, and delays occur. On the one hand, with meetings and personal involvement, operators try to reduce this uncertainty and see the dimensions of the project to fit better with these targets. On the other hand, unit A, at the strategic level, sees the programme holistically and how different project and programme targets are met at a given point in time, to assess accurate and efficient completion of the programme, and to absorb all funds within the programme period. If the programme picture is showing insufficient completion of the programme, the horizontal team, Unit A, the CRO and the director and their teams, in collaboration, as mentioned above, re-allocate funds to projects have the potential to absorb all EC funds and, in an effort, to successfully terminate the programme within the deadlines from EC. These EC targets serve as a guiding tool to re-allocate funds to projects that are capable of meeting those targets. As such, these targets, at the strategic level, serve as a tool to monitor programme performance, and, at the same time, as a mechanism that delineates the appropriate course of action when revising the MA strategy and programme update (tension between performance and compliance).

Finally, unit A also refers to the action plan to see how the programme is maturing in terms of project completion and EC fund absorption. If there is a development that the MA cannot adhere to, or is not inscribed in the current law, regulation and MCS procedures, unit A goes back to SRSA, the ministry and EC to ask for a revision of the programme. For example, there might be a new forecast for projects at programme level at a specific point in time. The case of Covid19 is also another example that affected the programme, as it delayed the projects due to the need to re-arrange the workplace and the ways of working from home. In that case, unit A

went back to the ministry to ask for extensions or discussed these issues with the EC to identify solutions. Other examples include the recent Covid19 pandemic, where the project delays were evident. In discussion with the MA, and other MAs, the Ministry of Development and Investments offered legal extensions to sub-contractors, and in conjunction with the EC, to allow for workplace changes. Or, and since each programme is at least 7 years in length, sometimes EC targets for projects, e.g., environmental targets, change due to advancements in legislation or technology. Finally, and at project level, unit A sees the action plan and how projects are absorbing funds. If there is an issue with absorption, then they take corrective action to re-allocate funds. As the representative of unit A, the participant commented on the interview:

> *"… (the programme) is very much lacking in terms of expenditure, we have too many integrations and these have already reached 9 billion euros from a programme of 4.652 billion euros, but our expenditure is still at 3.4 billion euros. In other words, we have a shortfall of around 1.2 billion euros in expenditure. And we are now trying to see how to close the program with this problem. What are we trying to do? We are trying, for example, to bring projects that have expenditure into the programme as new inclusions. This means that the programme is being reviewed. In other words, the programme is also being revised strategically, i.e., some initial objectives have not been achieved, particularly on the transportation area, so I am looking to bring in other projects which may not be of the same logic, energy projects for example, or urban regeneration projects, so that we can get some costs so that the programme can be closed. Otherwise, the program loses resources".*

This is sensed by unit A, brought to the attention of the director ad discussed at strategic level, discussed with EC, and a programme revision is made, changing the project assessment and integration criteria. If issues like that arise, then the MA suggests, to their overlooking bodies, programme revisions or changes in the rules of the programme. Any programme part can be revised, however, the MA trends to not revise the programme unless necessary, since it is a very bureaucratic and time-consuming procedure and might negatively affect the programme as a whole and its main targets. It is evident that through this monitoring, unit A is also, in parallel, monitoring programme risks.

6.5.1.2 Post-completion on-site verifications

At the strategic level, and to make sure that previous projects are fulfilling their obligations and the requirements for which they were funded with, the MA is engaging in post-completion on-site verification. This technical control tool is utilised diagnostically at the operational level to ensure project compliance, and, at the same time, interactively at the strategic level, to inform future strategy for the current or upcoming rounds of PDF EC funds when materialising projects, and diagnostically, to show how the long-term strategies of the programme are met. The way these verifications work is that the MA, and in the first 5 years of a programme, and its projects, being completed, needs to verify its projects, using a sampling method, by going on-site to check the operation of the project, to check that the long-term obligations of the project are met. These long-term obligations, according to the CRO are:

> *"…observing the long-term obligations is basically that the ownership of the project has not changed, and that no interventions have been made within it in the next five years. Interventions that change its functionality and perfection. There's a process for that".*

In essence, and to ensure that their long-term strategic goals are met, i.e., use public EC funds for the befit of society and to increase societal value, the MA, at the strategic level, utilises this on-site verification, after 5 years of the completion of the programme and hence its projects, interactively, to monitor long-term strategic performance and uncertainty. This usually informs the preparation of a new programme period. During the interviews for this study, and during 2023 specifically, the MA was at the end of the 2014-2020 programme (plus 3 years to complete as per EC). At this stage, they were preparing to close the programme and to welcome and start the new PADF programme, that of 2020-27, for similar projects. Reflecting on that, and as asked by the EC, the MA prepared a report assessing their beneficiaries, in terms of their capabilities in materialising projects, based on previous years' engagement with them. This report covered beneficiary readiness and leadership capabilities, fiscal results and adherence to law and regulation if needed, and also systems utilising to manage risks, among other. This report was sent to the EC, in preparation of the new programme period. At the operational level, the MA made sense, through this report, about the capabilities of their beneficiaries, and the risk of them completing projects.

6.5.2 Managing risk and uncertainty at the strategic level: Controls complementing strategic performance management

6.5.2.1 MCS at the strategic level

The MCS is also utilised at the strategic level, as a technical tool at the strategic level of the case organisation. At this level, boundary controls are utilised to inform the acceptable domain of opportunity-seeking by managers and employees (Tessier & Otley, 2012). Indeed, MCS, as a requirement to be implemented in all Greek MAs, includes all rules and procedures indicated in previous sections, given by EC as a cofounded programmes regulation, and adapted to meet the needs of Greece, also embedded into Greek Law. As part of MCS, the same applies to risk management that also included rules for risk management and anti-fraud risk. At an initial stage, around mid-2010s, the SRSA got this tool from EC, that was updated to require procedures for risk and anti-fraud risk management. The SRSA then took this tool, adapted it to the Greek needs and the MA needs, and dictated its implementation to all MA, following an initial brainstorming meeting with all MAs to discuss and identify risks, mitigating mechanisms and implementation, as an initial stage. The final product was an excel, very similar (almost identical) to the one the MA uses now. Moreover, the SRSA, and to reflect MCS, dictates the creation and commitment to a risk management team that handles risks within all MAs, and the case organisation as well. This team is required to be overlooked by one superior, the CRO in the case organisation, and they are responsible for running the risk management tool (seeing how risks manifest, manage current and identified risks, identify and discuss emergent risks, new risk management mechanisms) and they report back to SRSA to show how this risk tool conforms with the required application/implementation, and also inform the SRSA of new emergent risks that have not been identified before. The SRSA then discusses/brainstorms, with the MA, other MAs (usually represented by their CRO and risk management team members) and within their team, to see how they can frame and manage these emergent risks, and they feed this back to the MAs, or the MAs for which these risks are relevant (not all MAs are of the same nature, due to the projects they manage), or according to each MA needs. Indeed, the participant from SRSA indicated that some emergent risks are brainstormed because they apply to multiple MAs. The same applies if an initially identified risk (when the tool was implemented) does not apply anymore. Finally, as a second alternative to this discussion, and to recognise the needs of each MA, and the characteristics of each programme

each MA manages, they have been given freedom by the SRSA to add emergent risks to the tool, as per their needs and circumstances. The SRSA representative, reflecting on this, commented:

> *"The MA, and each MA, has autonomy in enriching the risk management tool according to their needs and the capacities of their beneficiaries. For instance, the MA we discuss, has a lot mature and well-experienced and capable beneficiaries that might not need the monitoring and capacity building of other MAs that we work with, that collaborate with small municipalities. That creates the ground for a different approach to managing risks".*

Furthermore, in the discussion of new risks, there are two pathways as well. Initially, the case MA or other MAs, usually identify a problem with the programmes/project materialisation/law and so on. Then, they discuss this problem with the SRSA, and they brainstorm, together, to identify a solution. If the solution is plausible, the SRSA, in conjunction with the MA, implement it. If there is no plausible solution, then this new problem is identified as a new risk (emergent risks) and the SRSA, in discussion with the MAs, discuss and implement mitigating mechanisms and they impose these mechanisms to the MAs, after including the risk to the general risk tool, and the MCS (as risk or procedure when needed). As an example to this, the SRSA representative indicated:

> *"At some point it became an issue from an external audit, from the audit authority, that in public procurement, we should have in our system, in addition to public contractors, contractors we call sub-contractors. Because MAs needed to ensure that certain things respect the national framework for public procurement. That is, that a person who gets a contract is not allowed in some strange way, to assign this contract to someone else, who would not normally be able to get the work done".*

This is an example of an issue that emerged within MA projects and was not included in the MCS before, through a mitigating mechanism. This example represents an emergent risk. Triggered by that, the SRSA representative commented on how the process worked to fix the issue:

"So, this led us to incorporate, within the MCS rules, when an MA beneficiary signs a contract with a contractor, it needs to declare the sub-contractors as well. We made a new template, that is, we introduced it in the MCS, and we instructed the managing authorities, when they will do the so-called on-the-spot verifications, which are random, to confirm on the spot, that the sub-contractors declared by the beneficiary are the ones who are actually in the project. This was an intervention that came to resolve a risk of illegality in the award of a public contract, discovered by a problem uncovered by an external audit. In other words, an audit authority went to an audit and found that there was no such record of the contractor in the project. It was an issue, so to speak, that needed to be addressed at the level of anti-fraud. We adapted this to our MCS system, we resolved this issue, but we did not recognize this as a new risk that needs other measures to be assimilated. That's what I want to tell you. That there was a problem, we solved it by integrating it into the MCS, so, one might say, we reduced the risk that sub-contracts were not legally awarded to contractors. We took one measure, that is".

Evidently, at the strategic level, the notion of risk management is not just a standalone rule, but a central consideration within the MCS. On the one hand, the risk management rules in the MCS themselves, serve as a technical, constraining control mechanism, at the operational level. At the same time, formal meetings, as described above, are utilised by the MA and the superior authorities, to make sense and embed emergent risks, into the MA operations. As such, these meetings serve as a technical control, in an interactive way and enabling way. Moreover, this technical control is utilised to manage the tension between compliance of MA to the risk management tool, and performance in managing risk and adhering to rules. This tension within this control unravels when the MA needs to not only comply to the above rules about the risk management and anti-fraud tools in the MCS, but they also need to report back on the correct and appropriate application of these tools, to the SRSA. The SRSA overlooks the application of the MCS, and the risk management and anti-fraud tools as well, utilising the feedback and feed-forward process for emergent risks, by discussing with MAs. They then audit the MAs for these applications as well, to make sure they are working as intended, to ensure no issues are identified that can be picked up by an external auditor. In this process, MAs are given freedom to adjust their risk and anti-fraud risk tools, according to their needs, to the greatest extend.

This freedom is distinguished between two things: if the emergent risks identified from an MA that apply to all MAs horizontally, then they are discussed with the SRSA and SRSA in turn discusses them with other MAs and updates the tool. As the SRSA representative indicated:

> *"For instance, the case MA we discuss, comes to us and says that they have implemented a new risk to their risk management tool, that might be specific and concerns other MAs as well. Then, we as the overlooking body, we see and discuss how this applies to other MAs, and this exists as a process, that is not that systematic, however".*

Then, institutionally, the SRSA updates the MCS section for risk management accordingly, and if another element of the MCS needs to change because of this risk, this changes too. For example, if a new emergent risk causes delays to projects, then a new MA response time is added, less days for example, to mitigate this risk. Changes in the risk tool might affect other MCS areas that need to be updated by the SRSA. Before any new risk, or emergent risk, is discussed with the SRSA, the case MA utilises an enabling technical control, interactively, at the strategic level, to discuss project risks. Effectively, the CRO calls the appointed risk management team if new risk arises to discuss assessment, impact, inclusion, and mitigation mechanisms. Through this, and with data from the IIS they see in which programme targets they had been exposed to emergent risks, due to lack of meeting these targets, they discuss these, justify them, discuss and bring to the attention of all units, get feedback, and shield for the future in terms of either implementing new mechanisms, or inputting these risks in the current risk management classification to be mitigated with current mechanisms, or both. For example, when a change in one of the laws they need to adhere to occurs, both at project and at organisational levels, Unit Gamma delegates communicate this to the rest of the units for consideration, unit then update beneficiaries accordingly. This rule, an internal organisation rule, applies to any change that happens, and then is transmitted for discussion in the risk management meeting, internally, and with the SRSA.

As a final example, there are key risk management procedures, adhering to the MCS, when the MA operates under conditions of staff shortage. The MA, at the point in time when the interviews took place and in general, are understaffed, suffering from the whole issue with the Greek public sector having staff shortages and low staff movement. The MA, supported by unit

Gamma, in an effort to change strategy to mitigate that, utilised the social controls and the responsibility and extra work its employees put to the job and daily tasks (social control in operational performance). However, as indicated before and by all Unit Gamma participants, this is something they cannot control. Therefore, at a strategic level and to solve this, they only have to follow the Greek public sector procedures. One procedure is to create an invite to other MAs to ask for an internal move of staff. But that is also very difficult, as most MAs in Greece are understaffed. The other avenue is to ask for the relevant public sector hiring authority, formally, to ask for external vacancies, or for movements of staff from other public sector entities. However, this has also been challenging, especially after the Greek crisis and the austerity measures. Public sector budgets are very low and there are no margins to hire additional staff in most public sector entities, thus the MA is still understaffed. In general, this is something outside of the control of the MA and they cannot do anything to increase staff mobility. They have to rely on these procedures.

6.5.2.2 Risk mindset as a strategic social control

According to the SRSA participant, implementing the procedures to monitor, update and modernise the MCS regularly, as per the previous sub-section, is very new to Greek public sector and the MAs. This was only started to be implemented in mid 2010s. Before, all MA mindsets were not risk management oriented, and they overlooked this process, deeming it non-mandatory. However, as a new implosion of risk management started at that time, with the need to implement risk management as per EC regulation and requirements, for the cofounded EU programmes, more and more MAs started to have a risk management awareness and mindset in implementing procedures and thinking more and more risk-wise. For now, this mindset, due to being developed recently, has created the grounds for risk management implementation and procedures, as indicated in the previous section, but, as the SRSA participant indicated, these procedures need to be updated and become more sophisticated. Moreover, and with that mindset, risk management tool updates are usually done yearly, and they adhere to the MCS. Updating the risk management tool and the risks included, needed to be agreed by the risk management team, discussed with SRSA, and also adhere to the relevant laws.

To reflect this risk-oriented mindset, the MA has designed a social control, a second one within the strategic domain of strategic controls, utilised in an enabling way. As an organisation, they are very keen on applying and disseminating all values and routines associated with reflecting the notion of risk and risk management within the organisation with a strategic objective to mitigate known risks and manage emergent ones (uncertainty). This social control is directly associated with risk and that way, risk is integrated with a standalone tool within the general organisational control framework. At the strategic level, and with the encouragement of the director, the MA values the notion of risk and uncertainty and its effect on their programme, and, as the director commented, whatever they do to manage their programme and daily project monitoring, entails the final objective of managing risk. Directed from the top level, the MA is engaging in a form of strategic risk management, in a sense that they not only focus on mitigating risk and uncertainty in every decision, but they also, especially the operators within their units, monitor the external environment of the projects (beneficiaries, fiscal health of sub-contractors, supply chains for project material, political environment and changes, war and other phenomena) to identify emergent risks and incorporate them into their projects and decisions for the programme, and discard if any are irrelevant, to meet exactly that: their strategic objectives and the main strategic risk objective, which is to mitigate all risks associated with their man targets. These targets associated with this are clear: absorb all EC funds and within the deadlines required (end of programme). This whole concept is translated into a perception that is infused at the lower levels of the MA. A participant, when shared their experience in entering that team as a risk management representative, commented:

> *"While in the beginning, before I joined the team, I had an opinion that this would not be something great, it is something typical that we have to do, I have started to feel that it has a significance and mainly, it is something interesting that has measurable consequences. They are some tangible and measurable pieces in risk management. That is, the fact that you take data from, say, the ISS for the evaluations that you have failures, and you see, let's say, that we made 100 project inclusions and in 3 we were out of time. To see the reason why the time was far off, what was wrong with us being off? What was this workflow that we followed and went off limits? It may be the fault of the operator; it may be something that refers to another team within the organization. But, in anyway, you see, you have tangible things, and it*

matters, and it also matters that you can have a picture of the service, how it is progressing, that is, its pace. And to go back and do some corrections".

To further recognise the existence of this social control, it was mentioned a lot by many participants of how it unravelled during the Covid19 outbreak. During that time, the MA and the risk management team were faced with an uncertain working environment that reduced the quality of their operations and their work conditions changed drastically in a few months. Working from home, meeting online, monitoring projects online (and meeting with beneficiaries) were among the key elements of operations that changed a lot, and the MA operators and management were challenged as they needed to adapt fast to make the necessary changes to adhere to the Greek law regarding workplace Covid19 restrictions. That endangered the completion of projects, as it pushed back timelines for completion and MA response times through IIS. Through that situation, they developed a mindset that aims at adjusting to continuously changing conditions, both for their work and for their project monitoring. Through enhanced collaborations, automated systems like the IIS and structured procedures and rules for workplace adjustments, the MA has learned to adapt to changes in their external environment. This mindset reflected the social control used for performance management at the operational level as instilled by the strategic level senior management.

At the programme/strategic level, the director and the directors of units have developed a mindset that goes deep into risk management. In essence, whatever day-to-day business they complete, all decisions about projects they take or all decisions that they take to make changes in the MA to ensure compliance with laws, the MCS and with meeting their main targets, is based on not only managing and mitigating risks, but also including any risks, known or emergent, in the procedures and decisions they make, and the associated procedures they follow. As such, risk and emergent risks is integrated as part of the wider organisational culture, for that matter, starts at the strategic senior level of the organisation. In support of that, and to borrow the exact words of the director of the MA:

"Look, risk management is something we do on a daily basis, even if we frame it or not. For that matter, we have a series of projects for which we need to make decisions. And this reflects a series of decisions we need to make, always weighing the cost and benefit, but also the risk of each decision. The programme consists of a set of projects.

We must select specific projects and discard some other. All of our decisions, in practice, embedded and reflect the notion of risk, and we definitely consider that risk when we decide about a project or set of projects, through selecting the avenue that maximises benefit and minimises costs".

Moreover, the MA and its main senior level managers, value the meaningful application of the risk management tool from the MCS to the organisation. The chief quality assurance officer, complemented by similar perceptions of all other participants and the CRO, indicated that the MA doesn't just want to implement the basics of the risk management tool. They want to make a substantial, meaningful and progressive-improvement oriented contribution. This is reflected to reports to governing bodies and other utilisations of the system, including making their own prototype system (SRSA rep indicated so as well). For the MA, implementing the risk management tool is more than a checklist to adhere to the MCS and EC rules and regulation. Especially the CRO, QAO and many participants take pride in this. For instance, when talking about the Covid19 approach they followed, the CRO commented:

"Here I want to say this: when in January 2020 I took over this (risk management) team, it was in the middle of the crisis with Covid19. And I said: let's meet a little bit about Covid19. And we started managing it. We started talking to SRSA and they told us there was no official management for this process as it was new to them too, and we had to rely on our own capabilities. And a few months later, we received a directive from the European Central Committee. We had to adjust fast... And we adapted through a series of procedures. This team, the risk management team, is great! That is, it has very good colleagues, without degrading the rest of our colleagues, that gives me huge confidence that the do the best we can, and it is evident. I mean, the QAO said to me looks, after a few months that we had started looking into the Covid19 issue and devised how to manage it, a series of points come from the audit of the European Commission, as guidelines, like what we did".

And that also reflected to the operators at the time:

"There is also a part of these teams, and this is something personal I want to share, that being part of them gives a sense being a part of your job. More active. It is not

that I go in, do my job and leave, mechanically. Your interest in your job is augmented. This risk management team has a high meaning. And in that team, you can see the way of operations of your unit, for example. And that is very important".

Moreover, the CRO and QAO mindsets are persistent with the implementation and correct use of all procedures that lead to meeting organisational, programme, EC and project materialisation targets and they are trying to instil this to all that their teams do. This norm exudes the belief that corrects procedures and correct implementation of risk management tools, will lead to meeting all targets of the MA. Finally, this is a social control that exists at both organisational levels, manages the tension between performance and compliance, as it will be shown in the next section of this chapter on performance.

To further analyse the components of this social control, an example of the Covid19 pandemic would be useful here. This social control discussed in the paragraph above, was extended to manage the crisis of Covid19 in 2020. During that time, all organisational members were very keen and very proactive in applying any required regulation and to mitigate all Covid19 associated risks. That was the general mindset as confirmed by all participants. The MA members valued the concept of readiness and proactivity since the early stages of the pandemic. That was exuded by a mentality of being prepared, implementing new rules and regulation correctly and on time and work efficiently and properly from home. That way, they extended the use of this social control to an emergent risk situation, the Covid19 pandemic, to manage this situation and to ensure all rules and regulations are adhered to. Again, the notion of risk was integrated here not separately from the tool, but as the second side of the same coin: embedded in the organisational culture as a risk-oriented mindset (emergent risk in that case) to ensure proactivity and to reduce the risk of the organisation delaying its operations, and by extension its projects, due to delays in non-compliance with the relevant rules and regulations. For instance, Unit Gamma updated themselves with the new law that applied to the workplace, to working from home to the beneficiaries in sites and so on. Then, Unit Gamma delegated communicated law and law changes to all units. If this unit was uncertain about a regulation or how it applied, they referred back to the relevant authorities for clarification, to ensure compliance, via a meeting, or a formal procedure.

This social control that delineates the risk mindset at the strategic level, is also transferred at the operational level of the MA and serves as a tool to manage project risks and emergent risks on a daily basis. As such, project operators always monitor projects and solve their issues always projecting their risk elements and antecedents.

6.5.2.3 Web of meetings: discussing and framing uncertainty

As an additional control tool at the strategic level, the director has also instilled an open discussion with his unit managers and the CRO and QAO to make sense of the projects, discuss and resolve issues about projects, internal organisational affairs and changes, new regulation applications and everything that might put the programme at risk. The director also indicated that there is an abundance of meetings with the EC, the ministry, the regulatory and legal overlooking bodies, the different MA units and the beneficiaries, to discuss issues with projects and ensure compliance. This stream of meetings starts from meetings with beneficiaries and continues to a stream of meetings and information exchange up to the Ministry and EC body level. In essence, these meetings serve as a mechanism to discuss current issues, develop mechanism and also make sense of emergent issues that may arise in projects or withing the organisation. That way, and in adherence with law and regulation, the MA is attempting to keep their operations on track, and their projects on track, to avoid delays, operational challenges and any obstacle that might cause a delay to the projects, or an under-absorption of EC funds. Referring to the meetings, the director pointed out:

> *"This obviously happens at regular intervals. There we deal with issues of mutual information exchange and issues of dealing with things that are horizontal, not just about projects. And they are also discussed with the unit supervisors. And at the level of supervisors and then at unit level. That is, I do not only talk to the head of the unit. Very often there are meetings with the whole of the unit and all the colleagues, both the supervisor and the executives, and we discuss all our issues."*

At the same interview, the director gave an example of how these meetings applied to the Covid19 management, when he was asked to provide an example:

"Yes, we discuss all arising issues. From daily work, to projects, and how the MA works, everything. And the issue of Covid, which we dealt with very well. And all this, after all, is also a matter of risk. It is the risk in the projects, it is also the risk of being left without people, or of the staff getting sick (during the Covid10 pandemic). All this involves the concept of managing the organisation and the programme and managing risk in parallel".

These meetings spread to the operational level as well, when needed. For example, at the final meeting with the QAO, and when asked about strategic level communications, she commented:

"...just to say that in a meeting we with an external body, they also put the dimension of risk analysis in the projects as well. I mean, no matter how big and small they are, okay, we're not talking about very small ones under 5 million... We had a meeting with a representative from there for the ports, for example, and he said that within both the feasibility studies and what is required for the preparation of projects, that there should also be a risk analysis for the projects, which is the first time that they have mentioned it to us a little more structured".

Similarly, another transportation project operator, when talking about her unit, commented:

"In our unit especially, we have very regular meetings to prepare and see what we have every month, or every week and so on. First of all, every week, a weekly schedule is completed by the supervisor, who has spoken with us about what needs to be done during this week, and accordingly we send to the office of the special secretary. He collates all this and discusses with unit A, which is for evaluation and planning for the whole program, and from there planning is done for the next 15 days."

This example shows that when a meeting is done with any member of the operational units and project monitoring units, it triggers a continuous web of meetings with other units and the director. Every unit supervisor goes and discusses issues with their project operators and the latter, in turn, discuss these with the beneficiaries responsible for materialising the project. The idea is to make sense of current and emergent issues in the programme, and then to find an approach to a solution. Once this is done, then meetings happen again at the opposite direction,

from the operational level, feeding back the director, to make decisions. Conclusively, these meetings are used interactively by the director and serve as a technical control tool at the strategic level, to understand and manage strategic uncertainty and make relevant decisions. These meetings are also imprinted into organisational culture and are valued for managing risk and uncertainty, at all levels. Therefore, they also serve as a social operational control tool.

Finally, and to complement these meetings, the director, and the MA as a whole, are utilising a plethora of data reports and report communication network that are produced withing the organisation and from the EC, to communicate all relevant information for the programme. For example, the EC representatives send a report, and usually on a 6-month basis, sends a report to the director of the MA, to show how the programme that the MA monitors is progressing, and how its budgets are being absorbed, compared to other programmes running simultaneously. With this report, the director goes to the CRO or the relevant unit that monitors projects and discusses this information, in conjunction with the action plan, to see current absorption, potential absorption of funds in the near future, and before the closure of the programme, and effectively, discusses the level of risk of the projects being completed. That way, they can take decision about re-arranging funds to different projects or integrate new ones, so as not to lose EC funds. The units and the operators specifically, discuss these issues with beneficiaries and report back to their supervisor with solutions, which are then reported back to the director. Another element of this is a report produced by the QAO internally and has to do with an internal audit that is done at regular intervals, to see that the MA is operating with the rules and procedures required, and to avoid issues in the case of an external audit. This report is communicated with the director, and includes performance of the MA, and also rectifying mechanisms if an issue is found (very similar to the operational level). As such, all these reports, serve interactively to manage risk at the strategic level, and make sense of uncertainty. For instance, the internal audit reports have a chance to uncover emergent operational risks that need to be mitigated and were not sensed before, for example a new HR regulation, or a new case of fraud within the unit.

6.5.2.4 Strategic uncertainty monitoring: processes and procedures

The meetings mentioned in the previous section, are triggered by sense-making procedures, that the case MA has designed. Specifically for uncertainty monitoring, all operators and the

CRO monitor the external environment of the MA and the beneficiaries and sub-contractors. They monitor the market, politics, financial health of sub-contractors, elections, new regulation on contracts and material, changes in supply chains due to covid or the recent war in Ukraine, and all elements of the external environment that might affect project and specifically project delays and fund absorption. However, that is not always possible:

> *"Look, we have a lot of limitations. In other words, we cannot, from the legislation on public contract, even if we detect that the price of a material essential to our works will increase, PVC plastic material, for example. We may have spotted this, but public contract legislation does not allow us to increase the cost of the project when we know that this will create a problem for the project. What is being done in these cases is a move by the Ministry as a whole. And because of this, which had appeared as a need, a ministry decision was issued that gives some capabilities on this increase. And it tells you, for example, that with the specific plastic we had an issue with, you can include in the cost of your project, as an additional expense. We could not do anything individually for a project. We have limited capabilities, even if we have identified the risk, sometimes we cannot act".*

Irrespective of that, when the MA can act, they actually do. Once a new information is acquired, it is inserted into the risk management system via talks with the risk management team and representatives from all Units. Then, this feedback transcends to the director and senior management level to ensure communication, understanding and updating on operations and main risks. Once that is done, the risk management team, in collaboration with senior management and the overlooking bodies, devises mechanisms, if needed, to mitigate this and pass it to all units for evaluation and mitigation, via meetings and internal auditing.

As a final procedure to monitor uncertainty, Unit Gamma, as an overlooking body for MA support and organisational compliance, scans the regulatory external environment of the organisation, to check for laws, regulation and procedures and how they develop. Then, they take these and see how they need to be applied to the MA for compliance, at the internal level of operations. Once they do so, they utilise existing avenues of communication, to communicate the new laws and regulation with all relevant MA units (regulation can change on programme, on HR, on project materialisation, on internal affairs and so on) and they

discuss compliance options. Moreover, when a new regulation arises, either as a new law or as an update to an existing law, unit Gamma inputs this to an online database they utilise for regulation, that everyone in the MA can see, and, a unit Gamma representative when an updated to regulation occurs, liaises with specific units that this new regulation applies, to raise attention on that they need to focus on and do to comply. The process is followed in a communicative and collaborative manner, rather than a coercive manner asking just to follow the new regulation. This whole process was of particular importance and focus during the Covid19 pandemic preparations. One of the unit Gamma representatives that worked on this as part of the procedures above, commented:

> *"So, we made a business plan for Covid19, telling them what is happening and what should be observed in the workplace and working remotely, we made some forms so that everyone could report the incident to us from start to finish, we gave instructions to each person and contacts and everything about what to follow. We also monitored the whole course of Covid19 regulation application, as we gave the opportunity for our organisation to do. In addition to the continuous disinfection of the building, we also practiced, at our own expense many times, at the expense of the service, to do Covid tests, because we knew that many could not afford it, even before the certificates of illness were needed as part of regulation (early stages of pandemic). We watched all this along the way. We were directly involved. For example, through a form that is online, that everyone can send for certification of Covid19 contact or infection, we kept personal data, files were locked that are managed only by the Covid19 group, no one else has access. So, all this was done and as much as we could we kept all the personal data of everyone. We followed and communicated procedures to the last detail".*

At the heart of all these processes, and to ensure compliance and organisational learning about new laws and procedures, operators within all units are trained yearly to be up to date with process and IT needs, MCS updates, risk management tool updates and law updates. For instance, when the ISS was first implemented in the MA as a system to monitor the programme and projects, operators were trained for IIS to obtain knowledge and experience about all IIS elements, reports and procedures and how to communicate information with beneficiaries. There were official and unofficial training avenues inside and outside of the organisation that

served as training tools such as training sessions, workshops, as well as collegial casual training. Moreover, if there is a risk that needs to be communicated and it applies to many units, then various operators have a meeting or training event with the unit that faced this risk, to learn about it and how it can be mitigated. Training serves as a means of sharing expertise and knowledge about risks, to save time, avoid this risk being manifested again, and increase administration capacity of MA, especially given the fact that they are under-staffed (at least during the period of interviews). This is something informal the MA utilises, with support from Unit Gamma.

6.5.2.5 Strategic Uncertainty management: SRSA and other MA networks

Embedded in the general performance framework of the MA, risk performance management is central to managing risks. Initially, the SRSA has produced the risk management tool according to EC needs and requirements and has included this in the MCS as a rule to be followed by all MAs. In that respect, MAs need to adhere to the MCS by maintaining a clear risk management tool. At the strategic level, the MA is in constant discussion with the SRSA to discuss new emergent risks and revision of current risks, and therefore, revision of this tool. As the main SRSA representative indicated, the way this works is that the SRSA imposes and monitors the application of the risk management tool of the MA, but the MA is left flexible and responsible to engage with this tool and follow their own path of identifying risks, risks that are relevant to their characteristics and the programmes they manage. That flexibility, according to the SRSA, is given to encapsulate the particular needs of each MA. Subsequently, each MA can keep the risks that are relevant to them, from the tool, but also revise them, if needed, ignore risks that are not relevant to them, and develop new risks to attend to, according to their needs. As such, when a new risk emerges, the case MA includes that to the risk management tool, and communicates that as per usual, with the SRSA and other MAs at regular (usually yearly) meetings. The case MA is utilising these meetings interactively to identify emergent risks and learn lessons of risk and risk management from other MA, at the strategic level. Risk management representatives attend these meetings and discuss emergent risks and see stories from other MAs and what risks they have, what risks they have emerged recently, and so on, and make sense of their external environment uncertainties that might have an impact on the main strategic objectives (mainly for fund absorption and closing the programme properly and within deadlines). Finally, these meetings are used interactively by the SRSA for the purpose

of identifying emergent risks, and if needed, as described in a previous section, revise the MCS, in any operational area they need to, to mitigate this emergent risk. The SRSA representative indicated that:

> *"While the risk management tool is running through the year, if there is a need, we update the tool through brainstorming with all relevant MAs that this tool applies to. That happened in the initial creation of the tool as well".*

This process is the final process that begins with each MA, case MA included, brainstorming their own issues and framing them within the risk management tool, before they brainstorm with the SRSA. In describing the risk feedback and inclusion process by the side of the MA, the CRO commented:

> *"If something falls into any of these categories (risk tool categories), we will put it in those categories. And if something that crossed our minds is not a new risk, but is another dimension of an existing risk, we will put it in there, right? So, whenever we find things, and in correspondence with SRSA, we discuss with them. We see this, we see that... How to manage it? So, there is such an understanding with them... In other words, we are quite strict in adding things to the tool indiscriminately. This process is done. From the moment we have our first conversation, we do the following: we divide responsibilities allocated to units, we put the next steps and who will do what, we give a deadline, and have 2-3 meetings... Of course, this takes months. It is a job that everyone does in parallel with their duties. But it is a task that is completed. We will also feed this into our review of our quality assurance system every year".*

6.6 Employee Perception

The last level, external level, of the Tessier and Otley (2012) framework, is the way employees perceive the controls and control systems of the organisation, when they are presented to them, and also when they are part of them and utilize them. As seen in the framework, this perception, this attitude, influenced by several elements, can be positive negative or neutral. In this section,

when asked about the controls, employees of the case organisation, offered mixed thoughts about some controls, and mostly negative. The most positive perception was already presented in the previous section, reflected in the notion of social control towards risk, which makes many operators in the case MA feel part of the job, feel like their work is contributing somewhere and perceive it as a way to understand their work and where it goes to direct effort. However, many employees expressed concerns about many of the controls that were discussed in the previous sections.

6.6.1 Greek public sector perception on risk management

However, before employee attitudes and perceptions are discussed, it is worth presenting the perception of one of the beneficiary participants, a chief risk and operations officer, who sets the scene for the picture of Greek public sector risk management. This participant has worked at different beneficiaries and at various senior levels positions at two out of the 3 participated beneficiaries at his career. This participant has worked with various public sector organisations for the materialisation of transportation projects for over 20 years. This picture will serve as a basis for a lot of later attitudes as it describes the basis for risk management thinking in the Greek public sector context, as it applies in the case MA. This particular participant, previously a director of programme and monitoring and assistant economic supervisor at a beneficiary building road network, and now a director of technical risk at the main beneficiary that constructs subways in Greece, offered valuable insights on the application of risk management in the public procurement projects, effectively the ones that the case MA monitors, in Greece, based on years of experience. In that respect, this participant offered two insights. The first is that in the case of public projects, EC funded projects materialised by the Greek public sector and other private sector beneficiaries, the main consideration is following the law. In the case of materialising projects, gaining green lights for more funds and project delays, materialising elements of the project and any other project business, according to public project law in Greece, all involve the need to follow the law to the strictest point. As the participant indicated, in the example of a new project they were currently integrating, if a risk arises, then the law should be followed to the point, communicate with the MA and get the green light for continuation with a clear justification of why the risk emerged, how it affected the timeline of the project and what mechanisms are in place to mitigate said risk. And the process stops there, it does not go deeper to analyse the general impact of a risk or an emergent risk and how it can

be mitigated, either in this situation, or in other similar projects. As the specific participant indicated, and according to their years of experience:

> *"There will indeed be some common-sense attempts in the next project to eliminate something (a risk), but then again, if you want to change everything, you must incorporate more risk management processes into the law. That is, risk registers and so on. What already exists as procedure is at a very embryonic stage. That is, in a framework of public works that goes on and is applied for years, it is the case that when there is a delay in a project, it will be submitted to the MA with the justifying report, and MA agreement will be sought. And it stops there, there is no risk breakdown structure for example, to further implement due to this issue. It is clear that there is a lot of room to improve both the legislation and the procedures. But, despite this, nobody wants to tamper with the law and everyone who has given an extension needs to have a clear justification".*

Another issue that was identified by this participant is that the Greek public sector, including the case MA, focuses a lot on the big picture of risk, that is they focus on the main risks that are in a project or may arise during a project materialisation. They dignify this with a category, i.e., archaeology, and they focus on mitigating that and whatever comes with it, without paying attention to smaller level risks, that may have an impact to the project. As such, by overfocusing on the main risk category, they overlook mitigating other risks, which become apparent once the main risk is mitigated and then they are picked up for managing. That causes a delay to the project materialisation. There is a compartmentalised approach to managing key risks, one at a time, and then moving to another risk. As the participant indicated:

> *"The other thing that is very interesting about risks is when you have a big risk, which hides the smaller ones. There was a case in the subway where you have this huge archaeology risk, which manifested for years, but at the same time there were other Issues running underneath, less important. But the big one hid the smaller ones. Now, little by little, when the archaeological problem is eliminated, the others are emerging. And this can apply to any project, i.e., running parallel things, one is delayed by 10 months, and the other is delayed by 6 months".*

According to this participant, delays arise from the fact that it takes a lot more time to manage and mitigate one key risk, rather than managing a set of project risks at the same time. The delay happens because each risk needs its own time to be mitigated, and if all these risks were mitigated at the same time, less delays will be caused. That is the main issue of the Greek perception on risk management, which later on manifests into Greek public sector entities, one of which is the case MA.

6.6.2 Employee perception on MCS, Action Plan, IIS and rules

Turning to the way employees perceive the main controls and control systems the case MA utilises to manage their operations, and risk, many employees, especially during the individual interviews, indicated some issues with the main tools they utilise on a daily basis. For instance, many interviewees indicated that the MA response times that operators need to adhere to, for example for a project modification which is 20 days, is a very short amount of time, given the fact that MA units are understaffed, and they have increased workload to attend to. That way, the MCS imposes a very strict timeline that most project operators cannot adhere to. To solve this issue, they form a formal negative report to the relevant MCS body, that is the SRSA, to inform of the issue and push for a change. However, they cannot influence the outcome. As such, it is up to the SRSA to make changes to the MCS operational areas if needed, and, as most participant indicated, this has not been done yet. All participants indicated that this issue creates additional stress and workload. However, some participants work around this to overcome the issue. For example, a participant indicated:

> *"Most of the time we bypassed it, so as not to be seen, and sent mail what needed to be corrected (a project), returned and submitted again what needed to be done. That is, we proceeded to faster procedures, via mail and telephones, of course, so that there was an immediate response. In other words, we all worked faster, but we did it with our own effort".*

Another participant, from the environment and sustainability AM are, and when speaking about the MCS timeframes they need to meet, especially for the response times of the IIS project modifications, commented:

"The times set by the MCS are unachievable. They are not possible to be met. Especially us with the huge number of projects we have in the environment, in relation to transport. We have too many projects, too many projects, with difficult and immature beneficiaries. We cannot apply the times set by the MCS".

The same participant and referring to their perceptions of their whole team in the environmental and sustainability projects, also conveyed their scepticism on the action plan. In essence, and since their projects are very demanding and have much more effort and require more time with beneficiaries (due to their nature), compared to transportation operators, end up needing a lot more time to manage a project. As such, they find the action plan extremely time consuming, adding to their workload, with unnecessary information. In echoing the majority of the MA interviewees on the matter, this particular participant indicated:

"They are tables, which are made every 2-3 months and indicate, for example, the forecasts that we have about expenditures, legal commitments and when the contracts will be made and approximately with what amount, for the various projects and their sub-contracts. It's a goal to be able to keep track of what costs and legal commitments you expect, but you can't be precise because there are too many risks. That is, you do not know when a competition for a project assignment will end. You might have an indication of 6-7 months, with a discount made on the contract. But it may not be the case. And that you will have more expenses than projected. Moreover, with the energy crisis, with Covid19, and with various problems that the MA may have internally, every projection may not be on time. In addition, there is a lack of funding, from the European Union itself, that is, that requests for allocation for the payment of project stages may be delayed. As a result, when this happens within 1-2 months, we have a contract Dissolution, the contractor may stop working because his bill was not paid in the prerequisite. And he has every right to do that. This is a risk reason".

These concerns were heard throughout the MA, and they were discussed with the CRO and the QAO and they gave their own explanation on the matter, including steps in place to mitigate this. Specifically, the CRO, during the final interview, commented:

"And on the issue of the workload that you said, on the action plan, maybe we haven't communicated properly, across all levels, and because it's a part that we've introduced in recent years, I would say that the importance of the action plan hasn't been communicated yet. So, people see the way things worked before the action plan, and based on that, when the action was added, they don't directly see the usefulness that it offers. I would say that the same applies to the beneficiaries. They have learned to do projects in a certain way in the last 20-30 years, and when obligations are enriched and new instructions and messages are conveyed, there is an inertia. I hear it, and it troubles me. But on the other hand, I would say that perhaps the importance of all these things as guidance tools has not yet been communicated, even at the operator level".

Adding to the above, the QAO also commented:

"...for the action plan, because I am not involved, there are some other people who are involved, I can say that perhaps they should get some instructions. Because they get the information from both us and the beneficiary. Let's say I might give some information to the person designated. It is just that the framework needs to be defined a little better. That is, what information does this person want from the action plan, numbers and dates that enter the action plan, what should it capture, are the milestones set central or is it reality? There's a little issue there. And also, the action plan has a lot of information in it and if you see it scares you it's the truth. But it has a very essential role. It needs to be communicated properly. Make proper preparation and updates. That is what we are missing a little, at the moment".

As such, it is evident that the MA, mainly through the help of the CRO and QAO, are working towards training their employees and their mindset towards the necessity of the action plan, to reduce the negativity against it.

Another participant, when asked about disseminating organisational learning about risks withing their organisation and with different project operators, indicated that this is something very difficult. Reflecting back to the use of the risk management as an operational social control to disseminate lessons learned for current and emergent risks and mitigating mechanisms, it is

clear that this process is not well understood and embedded in the mindset of some project operators. That is mainly due to lack of time, increased attention to projects due to understaffing issues, and lack of senior level support (despite the implementation) of such procedures. As the participant indicated:

> *"...but if you were in my position and in the position of many others here, you would find that perhaps we are missing proper organising and directives on this. In other words, idea is fine, but during implementation some other things arise, or priority is not given to this effort of lessons learned, that is, that we will be committed to it. Say that every two months, we will have this meeting, set goals and move on, towards this procedure. It is a way in which the European Union works a lot, but here we get to dance with everyday problems, and we do not pay so much attention to what you said".*

One problem that some participants observed, has to do with the application of the risk management tool as per the MCS. One of the participants, and the CRO, commented that the risk management tool does not have a feedback mechanism that directly feeds emergent risks from the project materialisation or from external environment developments. It is assumed that the tool does not have an adequate feedback mechanism from the bottom-up to convey information sharing at project level. The operators have to rely solely on the communication with beneficiary representatives. As one of the participants indicated:

> *"A proper risk analysis and management tool, at least in our sector, must have at least two levels. One is the level of the operation, i.e., how it is carried out, and indeed by unit Alpha. Unit Alpha, as soon as a project is integrated, must also anticipate the risks. They can see them, and possibly at that moment of integration. These risks are transferred to each unit Beta (respectively), and the implementation of the project begins. All this information and processing at this first level should somehow, with a mechanism, feed into the program's risk management tool. For each project or sub-contract is part of the great set of operations, called the program. So, you can't ignore what happens to each sub-contract. Because although there may be issues that are constantly being addressed, for example the risk of a timetable due to expropriations, OK, this is present in all projects. Or that we will find archaeology. But I might get a*

contract that was a bankrupt contractor who was succeeded by another, as it happened a few years ago. The program's risk management tool couldn't see it, even though I had informed management about it. And it couldn't manage that risk".

As a result, risk tool users see the risk management tool as incomplete towards feeding the tool with new emergent risks that derive from the project and its sub-contracts. Even though the risk management team operates at both operational and strategic levels to make sense of these risks, report to SRSA and integrate new risks, as described in previous sections, some participants still see this as incomplete and require more formal feedback mechanisms. They need to have a tool that manages risks at programme level, and at project/sub-contract level, at the same time. Despite law 4412, article 45, for public projects asking for this, there is not clear project and sub-contract level tool, adequate, at the operational level, and for all project, big or small. The current risk management tool focuses, for example, into project risks only, and not the risks associated with the external environment of the project, e.g., market conditions for materials and sub-contractor conditions. Referring to the risk management tool in helping with taking corrective action to manage risks, through IIS reports, another participant commented:

"I wouldn't say so. I have not detected such a thing myself. We use this report as a means to monitor risks that we have highlighted through the tool, but I wouldn't say that they interact with each other in any other way."

Indeed, it was evident in many individual interviews that, to apply proper risk management procedures and sense the eternal environment of projects and the sub-contractor capabilities, MA staff needs to be trained accordingly. For that matter, their risk management radar needs to be enhanced to include sub-contract and project level risk identification. One participant that raised this, indicated that the risk management tool and the risk management team meetings does not help in taking corrective action, and is just used to enhance legitimacy. The risk management tool itself does not have procedures in place to be followed when risks emerge or need to be managed, and it is up to the project operators to implement procedures for sensing and mitigating risks in their area. Another participant also saw the IIS as a mere data collection and representation tool, irrelevant of risk management.

Finally, referring to the IIS, another participant indicated that it does not have up-to-date data most of the times, and if an issue arises with a project, the project operator needs to go and look for relevant data, thus wasting valuable time. As this participant indicated: “

> *“... the IIS software is not updated to the extent that it needs to be updated. That is, a beneficiary can tell you that it has a contract of 3 million for example, and you don't see it in the IIS. So, you have to speculate and see if this contract exists or not. That is, the IIS is not an up-to-date tool that you can rely on it and do your work. It wants you to investigate as well. That is why we make the action plans, because we also look at what is the real picture in relation to the IIS, which often has discrepancies. Many times, the IIS has, for example, mistakes. Many times, someone who joins a project, from another unit, may not have correctly entered an intervention code. That is, for example, in a hazardous waste management project, the new operator has put an intervention code for an urban development project. We as unit A, at project level, also check this, so that all projects and the program, as it is passed in the IIS, are in line with the approved program, which exists in the database of the European Commission".*

Many participants have indeed pointed out that the IIS is not always updated to current project results, and thus, they use the action plan to monitor projects.

7 Discussion

7.1 Introduction

The purpose of this section is to discuss the findings of this study in a structured manner in two ways. First, to discuss the findings and how these add to existing literature and recent calls, and second, to compare these results with previous studies in the area. In there, the concepts of the Levers of Control (Tessier & Otley, 2012) will be discussed, to show the application of the framework in an empirical setting (section 7.3). Then, section 7.4 discusses the way PMS is central in managing risk, as proposed in previous literature (Cuganesan et al., 2014). Section 7.5 discusses how other controls complement PMS in both organisational levels, to form appropriate systems, and how risk is integrated in these. After that, section 7.6 discusses the control used in managing emergent risks, and how these tools fit in the wider control system of the case study. Finally, section 7.7, discusses how all these control systems synergise and create tension in the case study. This section shows how this study adds to the current management control and risk management literature.

7.2 Brief discussion of main findings

The purpose of this study is to offer an understanding of the processes of how management controls systems are integrated in the risk management process of public sector organisations. The relationship, and integration of these two elements, is clear in the literature (Bhimani, 2009; Soin et al., 2013) but the processes behind it in the public sector are still unclear in practice (Bracci et al., 2022). This is also particularly evidenced in the public sector where their integration is evidenced (Rana et al., 2019). In there, control systems aid risk management (Collier & Woods, 2011; Rocher, 2011), and they also co-exist within the wider control system of organisations (Bracci et al., 2022) but their integration, and process behind this integration, requires more evidence. As such, literature has called for more studies, especially case studies in international contexts, to provide more evidence of this integration in practice (Bracci et al., 2022; Rana et al., 2022).

It is established from the evidence, that the MA has designed their whole control system in direct relation to managing risk and uncertainty, and there is a clear connection and integration

of risk management and management control. In this effort, the study also offers some observations of the success factors behind the risk management implementation. These will be discussed in the next few sections, adding to the relevant literature (Bracci et al., 2022). For that matter, as it was evidenced in the case study, the key success factor for the effective management of risks, was the design and implementation of key MCS, such as the risk mindset and the constant information exchange, that aid in the diffusion of risk management mentalities in the organisation. Hence, one of the key factors affecting the success of PSO risk management, is in fact the design of effective control systems. Furthermore, the wider control framework of the case organisation is informed mainly by risk management considerations. That suggests that the MCS in the case study are structured and designed in direct influence of the risk management agenda (Rana et al., 2019). As a result, and in contrast to the findings of Rana, Hoque and Jacobs (2019), the case in the Greek context had a high level of integration of MCS and risk management. At the same time, evidence suggests that risk management was affected by organisational needs, mainly reflected in the risk management tool. These findings are in line with Rocher (2011). Data from the case study also suggested that the concepts of MCS and risk management influence each other. Within this influence, the notion of PMS is central, as it is one of the key elements of the processes utilised to manage risk, through target setting. However, PMS is only part of the wider control system of the case MA. Finally, especially for the case of managing emergent risks, the study provides evidence of the existence of informal risk management tools, in the form of integrated controls, that facilitate the execution of risk management in the organisation, a view that supports the findings of Carlsson-Wall et al. (2019). In this section, all the co-existing control tools will be discussed, to show complementarity with PMS. These management controls for risk management are also part of the wider control system of the MA case and they co-exist with other systems that are there to manage organisational strategy (Rana et al., 2019), forming a holistic, organisation wide approach to managing contemporary risk. As a result, evidence supports the synergy and co-existence of controls as per Tessier & Otley (2012). The uses of controls are also supported (enabling/constraining, diagnostic/interactive). Evidence from the case study also confirms the conclusions of Mahama et al. (2020), that risk management is an organisation-wide exercise. Furthermore, in discussing the integration of control systems in public sector strategy, with particular attention to the integration of risk management, this study confirms the typology of Bedford (2020), in conceptualising the part of the effect of co-existing MCS as a system.

Indeed, control tools in the case study were seen as complementing or substituting each other, and that is something that will be discussed in the next three sections via Bedford's (2020) typology. More details of this typology can be found in Table 9.6.

7.3 Application of the Revised LoC framework: a brief summary

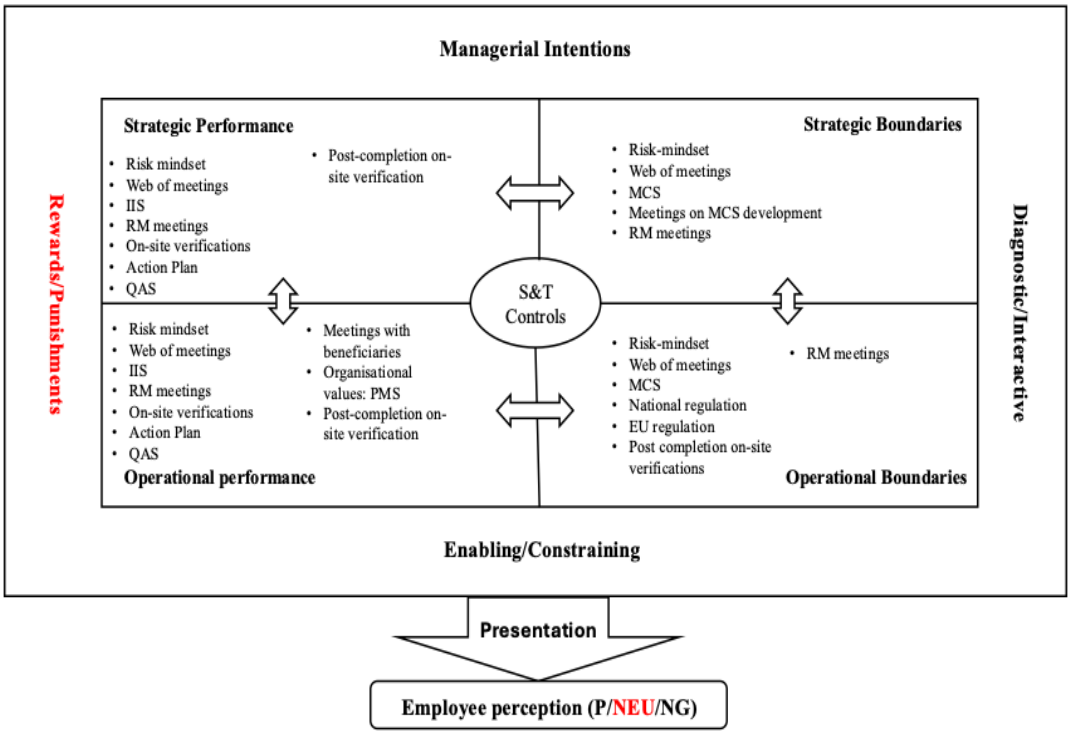


Figure 4.6: Adapted Tessier & Otley LoC framework: case study view.

The Tessier & Otley (2012) Levers of Control framework, as it applies to the case study, can be depicted in Figure 4.6 above. This figure depicts the existence, co-existence and place of controls that form control systems, at both organisational levels, and in direct relation to managing risk. To represent the first level of the revised LoC framework, social and technical controls that form part of the main control systems and are available for managerial use, are depicted in Figure 4.6, by the middle oval-shaped circle. These controls are later used at both operational and the strategic levels to form the main control systems (Tessier & Otley, 2012). These are depicted by the internal rectangle shape that is divided into four areas: strategic performance, strategic boundaries, operational performance, and operational boundaries. Within these 4 areas, the main control that are utilised by the case MA are described briefly.

At this level, synergy of control systems is reflected by the 4 arrows that connect the 4 control system areas, something that will be the focus of discussion on the last sub-section of the discussion chapter. Then, and depicted by another rectangle, encompassing the first one, lies the next level of the revised LoC framework, the level that represent managerial intentions. At this level lie the notion of controls used in an enabling or constraining way, what control used diagnostically and interactively, and the rewards or punishments decided for the consequences of meeting performance or compliance by employees. Finally, to depict the final levels of the framework, managerial intentions, as reflected in the presentation of control, is provided to employees which then, based on the various influences, form an attitude towards them, that can be positive, neutral or negative.

Evidence from this study confirms the application of the revised LOC framework as conceptualised by Tessier & Otley (2012), and in direct relation to managing risk and uncertainty, in the public sector. It also provides a framework for understand risk management integration and MCS, and specifically PMS which is central to PSO risk management (Bracci et al., 2021). However, not all elements of the framework apply. For example, the notion of reward systems to aid in performance management, was absent in the case of managing risk. At the same time, no neutral perception of employees was identified. Employees, when using the designed control tools, were either positive or negative against them. It was also observed that this negative perception was mainly at the operational level, while senior level managers were more positive towards the controls used. To manage risk, of central importance was the design a set of Strategic and Operational Performance technical control tools, that were directly influenced by risk. In there, various technical control tools responsible for monitoring and managing performance were set, majorly used diagnostically and in an enabling way. Moreover, social controls were also important to exude performance decision-making behaviours. That was reflected in the interactively utilised meetings with beneficiaries that were used to make sure performance targets were met before project materialisation stages continue. However, despite its usefulness, the PMS framework of the MA was found to have inherent risks, such as misinterpretation of information and negative effects on employee performance and morale. Employees reported that PMS tools like the IIS and Action Plan were either outdated or overly complicated, leading to additional workload and demotivation. Moreover, in contrast to what Tessier & Otley (2012) indicated, there was a lack of proper

reward or punishment systems for the PMS system utilised by the MA, that further exacerbates these issues, as there is no direct incentive for employees to meet project or performance targets.

Now, to ensure compliance and to avoid associated risks, the study pointed out the importance of Operational and Strategic Boundary systems, that complemented the systems that form the PMS. In there, various technical control tools, utilised in a constraining manner, delineated the acceptable domain action for project selection and materialisation, software operation and programme funding rules. That was complemented by technical control tools, used in a constraining manner, to make sure rules and regulations of the EC and the Greek government are followed, to avoid project delays and loss of funds. All of these control tools complemented performance.

Finally, there were a set of tools that applied to all control systems above. To manage emergent risks, and feed them to the organisation for management, a set of interactive technical control tools were of high importance, as they served as information-exchange channels. These not only communicated risk-related mitigating mechanisms, but also emergent risks from the internal and external environment of the organisation. These interactive tools were also existent in all control systems in Figure 4.6, and they enabled the framing of uncertainty. As a result, uncertainty framing and management control tools, were applicable equally to all operational and strategic control systems. This further supports the strength of the LOC framework in unravelling the controls utilised to manage emergent risks in the PSO (Georgiou & Favotto, 2022). Another tool with the same characteristic, was the risk mindset. The glue that kept together performance and boundary control systems, was the utilisation of a risk mindset that infused a risk-oriented mindset to all organisational decisions. This is a social control that was utilised to make sure that organisational behaviour was directed towards a clear risk decision-making agenda. As a result, the application of the framework shows distinct and shared control tools that are used for PSO risk management. The detailed application of these tools that formed the control system, will be the focus of discussion in the next three sections.

However, the application of the revised lever of control framework, does not come without limitations in the case study. These limitations were indicated above, but they will be now expanded upon, to further demonstrate the application of the LOC framework when

management control is integrated with risk management in PSO. To begin with the heart of the framework, the management control tools and systems, and focusing on their relationships, it was evidenced from the case study, that these tools do not just synergise and co-exist (Tessier & Otley, 2012). In the integration of these management control tools and systems are also designed to complement, substitute each other (Bedford, 2020), to make the management of risk more effective. These tools can also interact with each other in a supplementary or conflicting fashion, but little evidence was found on that in the case study (Bedford, 2020). Turning to the middle part of the framework now, that of the intentions/uses of control systems, the revised LOC framework recognises that, when control tools and systems are designed by managers, they have specific managerial intentions behind them (Tessier & Otley, 2012). However, in the case study, this was partly observed, mainly because many controls were designed to reflect employee intentions. As it was evidenced from the case study, and particularly for the utilisation of informal, interactively utilised information sharing tools, employees had the major influence in their design. As a result, when management control is integrated with risk management frameworks, employees might have a direct effect on the design on some tools, especially the ones that are directly connected with solving the challenges that PSO organisations face, by being exposed to excessive uncertainty. That was, majorly, due to the case study's organisational structure, that directly affected the design of control tools associated with managing risk. To make matters clearer, employees of the organisation, especially the ones directly associated with projects, i.e. the project operators, had the flexibility to not only use the control tools as they seemed fit, but also devise their own forms of communication, in line with the design of central control tools. That reflected the philosophy that different projects are unique, and they might have their own risk and emergent risks that required attention. That also adds to the management control literature, by providing evidence on the influence of employees on the design of control tools (Tessier & Otley, 2012). Furthermore, employees perceived these control tools either positively, or negatively. As the evidence suggests, many employees, mainly at the operational level, found these tools other not helpful or increasing their workloads. Therefore, the notion of neutrality against controls was not present in the application of LoC in the case study. This perception was also affected by the fact that many employees just needed to get the job done and finalise the projects and the funding programme successfully, disregarding the tools, and using them anyways, as part of their job. That goes back to the influence of the Greek culture on getting the job done, despite

the challenges. And that can also be attributed to the fact that, managers within the case study, did present controls tools as Tessier & Otley (2012) suggest, but as tools that need to be followed to get the job done. As a result, these perceptions were not found to affect performance (Tessier & Otley, 2012).The MCS, the regulatory environment and the formal interactions with the beneficiaries are the most key examples that demonstrate this direction. As a result, and in many occasions, control tools were not presented to employees as an implementation mechanism, but more as a requirement. Finally, there was no reward or punishment system directly designed by managers in the case organisation, directly related to risk performance or regulatory and risk management compliance. Evidence from the case study suggested that there were not rewards associated with projects being completed on time, and withing the agreed funds. However, this is something that employees would require in the future, as a recognition that they complete the supervision of the funds efficiently and effectively. This was something that was particularly supported by the CRO. As such, when management controls are designed to integrate the notion or risk in PSO, they might not be associated with clear avenues of reward or punishment. That can be directly applied to organisations that have similar characteristics with the case study. Therefore, in relation to the applicability of the framework, the Tessier & Otley (2012) Levers of Control framework is applicable to managing PSO risk management. In managing risk at both organisational levels, technical control utilised diagnostically are working well in delineating the acceptable performance to reduce risk and eliminate it where possible. Various performance indicators associated with accepted risk and mitigating mechanisms are very important and central in addressing key risk exposures in PSO. Moreover, the importance of boundary controls at both organisational levels also works well in delineating the acceptable domain of action and, most of the times, influence the acceptable performance indicators. At the same time, various technical controls are used interactively are very helpful in making sense of emergent risks and devise organisational responses in different situations where flexibility is required (depending on the nature of projects), with an aim at addressing strategic decision-making. The distinction between controls used interactively and diagnostically is what makes the management of risks more efficient and strategic-oriented. Finally, the antecedents of culture play a key role, as they are reflected in social control tools, in directing the organisation in an effective application of risk management frameworks, and a clear direction towards risk-oriented decision-making.

On the other hand, however, originally, the revised framework assumes managerial intention in designing control tools. In PSO, and given the high exposure to uncertainty, employee needs and intentions also shape informal, interactively utilised information-sharing tools. That shows that employees also have a clear design influence in PSO risk management control tool, reflecting the exposure to high levels of uncertainty in their respective areas. These tools are complemented by diagnostically used risk monitoring and management tools in an acknowledgment that different projects present unique risks requiring tailored approaches. This is something that the revised framework does not include. Finally, despite the fact that employee perception is important in making control tools work efficiently and effectively, in the case of PSO risk management, this was either positive or negative. There was no neutral perception as indicated by the revised framework. In PSO risk management, employees can either be positive or negative towards control tools, and this was majorly affected by the negative effect of these tools on their workloads and the wider cultural environment of the Greek PSO. As a result, some control tools were used simply as a a way to fulfil job expectations rather than risk mitigating tools. Finally, the case of rewards and punishments as designed by managers to direct employee performance, was not applicable in the case of PSO risk management. Rewards and punishments might be there but indirectly connected to the organisational members and control design, and only applicable to the wider environment of the PSO in, for example, not meeting the necessary fund absorption, or resource mismanagement. No rewards or punishments are associated with the design of control tools when it come to managing risk.

Conclusively, in PSO risk management, the Tessier & Otley (2012) revised framework works well, but not all of its elements. Moreover, its applicability adds to the framework in a few ways. First, contrary to the assumption that control tools co-exist and synergise as per the authors, PSO control tools for risk management can also complement or substitute each other to enhance risk management. Therefore, the original assumption of a balanced control system is challenged in PSO risk management control systems. Furthermore, and adding to the revised framework, employees play a crucial role in influencing the design of control tools in PSO risk management, as this reflected the sector exposure to an uncertain environment, compared to the private sector. As a result, and adding to the revised framework, employees also have a design role within the PSO when it comes to designing control tools to manage risk. That is

influenced, to a significant extent, by their perception and cultural elements. As a result, the revised framework does not clearly account for the role of cultural factors in shaping control adoption and effectiveness in managing risk. In fact, employees are very well associated with designing PSO risk management control tools, and the top-down perspective that governs the design of control tools, is not applicable in the case of risk management control tools. Conclusively, the framework works well in defining control mechanisms utilised in PSO risk management and in enforcing compliance but fall short in addressing the design of all available control tools for managing risk, and to take into consideration various employee and cultural perspectives. Employees play a significant role in shaping control tools and their perception influence their effectiveness. The framework serves as a very helpful starting point in addressing the elements of PSO control tools utilised for risk management. However, future adaptations should consider the PSO sector-specific challenges to enhance the framework's applicability to PSO risk management.

7.4 Performance management: centrality and risk integration

To manage risk and uncertainty in the case organisation, PMS were central and represented a key composition of components. That contradicts the view that PMS is disintegrated with risk management in PSO (Bracci et al., 2024). That also confirms previous research that suggested that PMS is central to managing PSO risk (Cuganesan et al., 2014). Evidence also extends literature on how PMS ad risk management are diffused in this context (Rana, Hoque and Jacobs, 2019). The case organisation used a lot of controls in both an enabling and a restraining way (coercive). That evidence supports the view that approaches, if connected together by the different uses of interplaying control tools for PMS, they create a performance-oriented risk management culture (Gong & Subramanian, 2018). That was evident in the case MA, as performance management was directly associated with managing risks. At the same time, evidence supports that this performance risk culture was associated with the long-term success of the organisation (Flemig et al., 2016; Rana et al., 2019). It was also evident that PMS played a central role in the success of the risk management of the case organisation (Bracci et al., 2022).

To begin with, and at the operational level, a key control system that is used to manage project performance is on site verifications. This process serves as a technical control tool, used in a constraining and diagnostic way, to check how projects are performing towards their agreed completion criteria, timelines and agreed completion rates. Indeed, on-site verifications serve to check progress of main project KPIs and informally communicate areas of project attention. Especially in the environmental and sustainability projects, where project contractors are less experienced and have lower capabilities than the mega-projects of transportation, operators go an extra mile to support contractors and municipalities with regulatory, compliance and other information, to aid them in the appropriate project completion within the agreed timelines. In this process, risk is integrated as the main focus of internal verification, which is to check progress and see if there were anything that would instil a delay or affect the funding of projects. Moreover, operators can check the full details of a project, that were not communicated via formal avenues, effectively making sense of any emergent risks that might exist at the time of the verification, especially at the beginning of a project. Here, on-site verifications and interactive meetings work in a compensating fashion (Bedford, 2020). As such, these verifications are also used interactively to make sense of emergent risks, especially for environmental and sustainability projects, where projects are smaller and more complex. In a similar vein, the case MA is utilising post-completion on-stie verifications, within 5 years of project completion, to check project compliance with the criteria that were indicated and utilised when the project was at its completion stage (diagnostically) and to make sense of strategic uncertainties that might affect the long-term strategy of the programme (interactively). These on-site verifications reinforce the on-site verifications at the operational level. However, on-site verifications are not working always as intended. In February 2023, a very tragic accident occurred in Greece, when two opposite trains collided at high speed, effectively killing 57 people, in one of the main train routes between Athens and Thessaloniki (EPPO, 2023). The preliminary investigations revealed that these was an issue with the cruise management and control of the particular train line, along some managerial inefficiencies on behalf of the main train conductor on duty, on the day of the accident. Indeed, the automatic rescue (collision indicating) system was not working as intended, and it was in fact inactive although money was spent to build it from the European Union as part of the EC fund programme managed by the case MA. Moreover, the route manager at that time, gave a green light for the trains to continue their course, despite the imminent collision approaching, by falsely reading the

schedule data. That resulted in the prosecution of 4 public officials from the case MA in 2023 for misappropriation of funds (EPPO, 2023), among others relevant to the incident. This is a clear indication of a set of failures. First, there is the failure to implement the project elements properly, from the side of the project management organisation, after the project was completed. For that matter, although the case MA overlooked the proper completion of the project, with the automatic course and collision management system properly working and implemented upon project completion, they did not adequately create an environment to collect enough information on their post-completion verification. As the CRO commented, the post-completion verification only rests on verifying the operations of a sample of projects. However, in the case of the project where accident described above occurred, not enough information was collected from any post-completion verification avenue. Therefore, post-completion on site verifications, seems to suffer from lack of input to make correct decisions at the operational and the strategic levels. Although the way projects operate after they are completed is not the responsibility of the MA, proper information inputs that may uncover dangerous issues in projects, are and should be welcomed, to make sure a more efficient corrective action is taken in consecutive projects of future rounds of EC funds, to reduce the risk of putting human lives in danger. The case MA cannot manage the operation of transportation projects after they are completed. It is not their responsibility. However, they can make sure that projects are fully completed with specific criteria, and that, through the monitoring of projects, the latter are completed with mechanisms that avoid dangerous events in the future. Conclusively, although not perfect, on-site verifications are a technical control tool that is used to diagnose risks as part of the wider performance management agenda of the case MA. As such, risk management influences this tool because their main focus is to see how known risks are unravelling and are mitigated in a project, but also to identify and make sense of emergent risks. Of particular importance for this interaction, is the function of the IIS that communicates all the above and triggers corrective action.

Speaking of the IIS, on-site verifications are but a part of this system, which serves as a way of monitoring progress project performance as a whole. At the operational level, IIS, by including all information on completions stages, funding, progress reports and operator responses, for a given project, at any point in time, shows all data that are required to see project performance at said point in time. In this oracle system, which serves as a technical control tool

used diagnostically at the operational level, risks are integrated as they are reflected and transformed into project targets, and progress reports, with clear indications of problematic projects, within the IIS. In other words, these targets show the level of risk that a project may entail, in terms of completion progress ad funding absorption. Moreover, these targets are monitored to check project completion at all stages, and they are used to point out issues. As a result, risk is embedded in this tool, as it influences the project completion targets directly. The same applies to monitoring targets that are reflected to project targets. At the operational level, the IIS enhances the effectiveness of on-site verifications (Bedford, 2020). At the strategic level, Unit A utilises the IIS, complemented by information in the action plan, in a diagnostic way to check if projects, though their integration criteria, fulfil the EC funding targets that these funds have been given for. Therefore, by checking the IIS, unit Alpha ensures the strategy of the MA is in place when it comes to project integration. However, because the IIS information can be out of date or not complete, the action plan is utilised to offer additional performance information. Here, the Action Plan compensates for the limitations of the IIS (Bedford, 2020). Through this complementarity, unit Alpha also engages in budget monitoring to see if the EC programme fund budgets are absorbed as intended, by all projects monitored by the MA. As such, the IIS and the action plan are also used in the same fashion, to monitor the performance of the programme as a whole, for transportation and environmental/sustainability projects. Finally, the IIS in also used in managing MA internal performance. The main targets that the MA checks to monitor performance are MA response times to new laws and regulations, MA updates with new regulations for projects and internal operations and MA targets for HR procedures. In essence, risk is integrated in IIS for that matter, as it shows the current laws, regulation, internal capacities and any other internal information on these main targets, that might put the MA at risk of not operation properly, effectively increasing the risk of project delays and decreased fund absorption. As such, risk is integrated in these regulations, and it influences the way the IIS operates, as an operational technical control, used to manage internal performance, diagnostically. However, many MA employees, especially operators, do not perceive the IIS and all associated targets as helpful. For instance, operator attainment of the pre-determined response days targets, for on-site verification reports, or for requested project changes by the beneficiaries, as it was set from the MCS, was almost impossible in the case MA. Response targets were found to be very strict and hard to attain, especially given that the MA operators are understaffed and have increased workloads as a result. Moreover, changing

this target is outside of the influence of the MA, as it is the responsibility of the MCS setter, in that case, the SRSA. As a result, at the operational level, operators influenced the attainment of these pre-determined response targets, by utilising informal interactively used control tools, to collect information from beneficiaries, regarding issues or project changes, to agree on project changes faster. These interactive controls, usually in the forms of meetings, are also used to compensate for the weaknesses of the IIS (Bedford, 2020). And this practice aims at making sure strict response targets are attained. This shows a direct influence of employees to the PMS tool utilised by the MA (Tessier & Otley, 2012). Following that, and in extending Tessier & Otley's framework, this perception had impact on performance. Finally, in complementing the IIS for monitoring and managing internal performance, a QAS is utilised to manage KPIs associated with the operations of the MA and the quality of service, and, at the same time, to monitor MCS compliance. The QAS is utilised as a control tool that reinforces the IIS (Bedford, 2020). Moreover, in this diagnostically utilised control tool, risk is integrated in core procedures that need to be adhered to and this QAS has been devised to mitigate any risk of failure of the MA to provide its services in monitoring EC funded programmes.

As indicated above, and to complement the deficiencies of the IIS, the Action plan is another performance management tool that includes all available information of each project element, to provide project progress in areas where the IIS does not have information or is out of date. Once again, the Action Plan is utilised as technical control tool, at both the operational and the strategic level, to show project and programme performance. By providing all details of all MA projects, this tool shows the progress and fund absorption of all projects at any point in time. As a result, at the strategic level, it shows how the programme is going, and what projects are at risk of not being completed. At the strategic level, the Action plan is of particular importance at the end of the programme period, as it shows which projects are at high risk of not being completed. To avoid the loss of funds, senior level managers, with the support of project operators, identify ways to re-allocated funds of these projects, to other projects, to ensure maximum fund absorption. As such, the Action Plan also serves as a tool that triggers corrective action. Here, the MA is utilising the Action Plan, in conjunction with information from the IIS, as a way to engage in performance budgeting (Bleyen et al., 2017), and as a way to manage the EC allocated budget for their programme. As a result, performance budgets are used for risk management for that matter, aiming for efficient and effective resource allocation of projects,

especially at the end of the programme period. For the case study, this performance budgeting is utilising past project information to check how the programme is performing, while comparing this information with how performance should be at the end of the programme (future information). This result is not in line with the conclusions that Bleyen et al. (2017) that indicated that only past information is fed into PSO performance management systems. In fact, the case MA does not just input past performance in the PMS to see how they are performing, but they also engage in how this performance affects their future, effectively comparing it with future PMS targets. The main influence towards this is the culture of the organisation, especially towards risk management, the expertise of the organisational members, and the risk mindset that was instilled in the case study, influenced and promoted in particular by the CRO, QAO and the director. These control tools are used to enable the use of the Action Plan as a PMS tool (Bedford, 2020).

At the operational level, the Action Plan serves as a tool that diagnoses unknown issues with projects. For that matter, when the Action Plan is fed with all available information about all projects, and with the way it is visually constructed, it points out deficiencies in projects, that operators have not seen before. In such a way, and at the same time, this tool serves as way to make sense of emergent risks. More discussion on this will be held in section 5.4. when control tools for emergent risks will be given more attention. For now, going back to the Action plan function, risk is integrated into key project areas that need attention and by which, if not completed, there is a risk of project delay or loss of funds. As such, to manage risks, the MA has devised this technical control tool, used diagnostically, that indirectly connected to risk, by showing key projects that are in risk of not being completed. Main project risk influences the targets of this Action Plan. However, not all employees perceive this activity as beneficial. Especially when it comes to managing complex environmental and sustainability projects, feeding information into the action plan, from project operators, was deemed an unnecessary exercise (Goh et al., 2015). These projects require a lot of time and personal operator conduct to be invested in, to be completed. That is because they possess specific characteristics and procedures that cannot be quantified. In echoing most environmental and sustainability project operators, the amount of risk and uncertainty in completing said projects is not reflected in the targets set by the Action Plan. That also applies to the environment of the MA, as it might be fully incorporated in this tool. As a result, the Action Plan does not depict reality and cannot

fully depict project performance, eventually decreasing the accuracy of the PMS tool, something that Goh et al. (2015) also concluded in their study.

At the operational level, and to manage operational performance, the case MA has designed and utilised one of their core control mechanisms, that is, risk management meetings. This tool, which serves all organisational levels in a different manner, is used at the operational level to ensure operators are performing as intended and within the agreed timelines and procedures delineated by the MCS. One of the main focuses of this meeting, among others, is the discussion of results on operator response time to beneficiary issues, when they input a project change in the IIS, or when operators produce various reports for project attention, to the beneficiaries, for example, after an on-site verification. In this meeting, operators discuss, mainly with the CRO and the QAO, if these MCS targets are met and project operators indicate reasons for delays. After that, mitigating mechanisms are devised. Effectively, risk management meetings are there to enable the rules of the MCS (Bedford, 2020). When a corrective action is agreed for that matter, project operators that represent their units in this meeting, go and communicate this corrective action with their respective teams, in more meetings. The same applies to any other target that operators need to meet, when it comes to project monitoring. Moreover, in managing project and programme performance, more meetings are utilised interactively to communicate corrective action. At the strategic level, when a re-allocation of funds happens, or when a programme target is at risk of not being met, senior management discusses mitigating mechanisms. These mechanisms are later communicated with project operators, mainly through the risk management team meetings, and they flow to the operational level for project attention. The same applies if a target is not met at the operational level. Operators discuss this with their respective teams, communicate issues with performance at the risk management meeting, which instils corrective action that is later fed back to the operational level. Moreover, these meetings are complemented by organisational values at the operational level, a social control tool used diagnostically to manage project risks, even before they are inputted into any formal communication system, i.e. the IIS. Effectively, this social control is designed to instil a culture to mitigate risks before they emerge and to make sense of emergent issues before any project initiation, at all stages. As such, informal, personal engagement with beneficiaries occurs, to agree on steps and mitigating mechanisms on emergent risks, before they formally initiate each project via the IIS,

or before a beneficiary communicates a project issue via IIS at any point in the completion stage of a project. As such, this social control reinforces the meetings as a control tool (Bedford, 2020). Effectively, this social control is devised to ensure proactivity towards mitigating risk, that also aims at making sure that the project stages are well prepared, to avoid delays, and hence, meet projects targets, effectively reducing the risk of project delays. This social control was devised with a clear reflection on risk management, and it is influenced by it.

As it was shown above, the effort to manage MA performance, in direct connection with risk management, was complemented by a variety of informal control tools, the majority of which, if not all, were used interactively. To represent the continuous and flexible interaction between the organisation and its members, a variety of informal control tools were utilised. However, PMS focused mostly on the interaction between operators and beneficiaries. To complement these interactions and foster organisational-wide communication, informal meetings and interactions were used as well. However, this will be further discussed in section 7.6. For the PMS, a variety of informal information exchange control tools were utilised, mainly to increase the effectiveness of the formal controls (Bedford, 2020). For example, at the beginning of projects, and even at the stage of integration and allocation of beneficiaries, operators and members of the Alpha units, were utilising informal avenues of communication. On many occasions, the operators were familiar with the beneficiaries. Hence, once a project was assigned, operators were informally communicating with representatives from the beneficiaries, to raise issues, for example documentation of completion of regulatory pre-construction reports. These informal communications were done via informal meetings, or phone calls and exchanges of emails. This was done to avoid delays in project integration, and as a result, project completion. At the same time, and during project integration, on-site verification visits were usually utilised to also informally exchange information with contractors and beneficiaries as to any emergent issues or problems within a project. At the same time, and in exuding proactivity, when a new issue was arising, project operators were proactively utilising informal meetings with beneficiaries to attend to engaging issues, and agree to a course of action, before this was formally input into the IIS system to be monitored formally. That was particularly important when beneficiaries were identifying considerable delays and went ahead to informally communicate the nature of the delay to the MA to check and agree on viable options. At the same time, and to ensure internal attention was directed

towards managing internal and project performance, the MA members were utilising informal knowledge exchange avenues. Informal meetings and chats, especially on the everyday job, were key in exchanging knowledge and expertise about risks and managing these and similar situations, with other members. This served as a way to save time, share a co-ordinated approach to managing risks and emergent risks in key areas, and increase the administrative capacity of the organisation, given the constraints imposed by the lack of staff.

To showcase the above, it has been suggested in the literature that performance information is mostly used to monitor top manager and subordinate performance, and for internal accountability, rather than for learning and improvement to identify problems or for communicating with stakeholder or users of public services. That reflects the most common issues in PMS (Van Doore and Hoffmann, 2018). However, this was not found in the case of the PMS systems, integrating risks, in this study. In fact, all PMS were utilised to instil communication on performance and target-setting on all organisational levels, mainly with the support and moderation of the risk management meetings, and the associated subsequent meetings at all organisational levels. All PMS targets were directly or indirectly associated with mitigating the effect of risk, as this would affect the main MA targets. It is worth mentioning here that PMS did not manage reputational risks for the case MA at all. This finding does not support the conclusion of Power et al. (2009), that has identified reputational risks are central to contemporary public sector risk management. That is mainly due to the fact that the case MA does not directly provide services to the public, but rather overlooks the appropriate implementation of projects, with an indirect aim at these being utilised to serve the public, by their organizations that manage them after completion. Conclusively, as a whole, and despite its issues, the performance management system in the case organisation is designed to monitor performance of projects, programme and internal operations, in a holistic manner. That is because, when it comes to target setting, target attainment and corrective action, all organisational members from all parts of the case MA, are included. This process is enhanced by the various technical and social controls complementing, reinforcing or enabling each other (Bedford, 2020). The case MA has designed these PMS tools in an effort to show that it is not only the project beneficiaries and the operators that need to perform well, but also the organisation and its internal operations as a whole, in a collaborative fashion, to make sure projects are completed on time and with the desired fund absorption, and this is the main aim

of the PMS system in the case MA. For the case MA, however, and despite their positive efforts, no reward of punishment is instilled for this effort. Evidence from the case study revealed no performance-related rewards or punishments for reaching the intended levels of organisational performance, something that is no in line with the Tessier & Otley's (2012) framework typology. The only indication of punishment was only in the case where the case MA integrated projects related to EC programme targets, or when projects where not completed on time, resulting in the loss of EC funds. If the organisation did not meet the targets of project completion and fund absorption, and the other related risk-related operational targets under this umbrella, punishment would be imposed on the funding itself and the Greek government. The case MA does not have any rewards/punishment system related to this. As such, this study finds no evidence of the design of rewards or punishment of the identified control systems by the case MA (Tessier & Otley, 2012). However, it is worth mentioning that the CRO, together with some other employees of different units, and the risk management team, have suggested the implementation of a rewards system for meeting yearly targets to the relevant overlooking authorities, but without any progress throughout the period of the data collection.

In a brief summary, the findings discussed above, as they apply to the integration of risk in PSO PMS tools and systems, show that PMS systems are not only central to managing organisational risks, but they also contribute to managing PSO risk in a holistic manner. However, just discussing their contribution without their inherent risks, would be an incomplete contribution to the literature. In addition to the evidence above, evidence from this study adds to the extant literature on the issues of PSO performance management (Arnaboldi et al., 2014), especially as these are reflected in the inherent risks of performance management systems (Cuganesan et al., 2014). In the integration of PMS and risk management two PMS risks were identified as per the typology of Cuganesan et al. (2014): PMS systems misinterpreting information and the risk of PMS systems negatively affecting employee performance. The former was manifested in the fact that PMS tools associated with managing performance, did not include accurate information. Indeed, both these MA PMS tools were either out of date or incomplete (see the IIS), or they did not incorporate all risk dimensions in the pre-determined targets (see the Action Plan). That points to the fact that the ISS, as a PM system, was under-utilised (Cuganesan et al., 2014). This negatively affected employee morale, which is in line with the conclusions of Verbeeten (2008). This evidence is also in line with

Goh et al. (2015), suggesting PMS an unnecessary exercise due to the data overload and accuracy. In the case study, that was mainly because, as many participants indicated, the system was disregarding some performance dimensions (Cuganesan et al., 2014), especially the ones related to the external environment of the MA and its projects, and the inherent risks manifested in this environment. To mitigate that risk, the case MA engaged into training for all their systems, for all their employees. In the case of the ISS, information was also not caught up with current affairs, hence its complementarity with the Action Plan. Moreover, the PMS system was complemented, or co-existing, with other control tools, especially informal ones, to make sure that the pre-determined targets are attained. No adjustments to the system were made as Cuganesan et al. (2014) suggested.

Furthermore, another PSO PMS risk that has been identified in the literature is that it negatively affects employee welfare (Cuganesan et al., 2014; Arnaboldi et al., 2015), especially motivation, morale and behaviours. This was evident in the case study for the risk-integrated PMS as well, as they were demotivating and also created additional workload (Cuganesan et al., 2014). This is also consistent with the findings of Oh (2023). However, this was the case not because of poor design, or due to top-down authoritative implementation of the PMS as suggested by Cuganesan et al. (2014). In case MA, and in the risk-integrated PMS system, employee welfare was negatively affected due to inaccuracy of PMS information, and because of the inherent characteristics of the organisation itself, which us understaffed and under-trained, mainly due to lack of resources in the wider sector. Again, to mitigate this, employee training was offered. Moreover, and with specific relation to mitigating the risk of employee welfare, the case MA utilised the notion of Greek honour, embedded in their social controls, and engaged in personal sacrifice. There were also some formal procedures followed by the MA, especially by Unit Gamma, to request for more staff, but since these were not fruitful, they did not mitigate any risk. These findings add to the literature in showing how PMS risk on employee welfare can be mitigated, something that Cuganesan et al. (2014) concluded that it has no mitigating mechanisms. Conclusively, To mitigate most inherent PMS risks, the case MA, instilled, from the top and especially with the support of the CRO and the QAO, training regimes. These trainings were communicated reflecting the vision communicated from the top, and a focus on how the PMS will help the MA. However, as the CRO and the QAO commented in their last interviews, these regimes are still at their initial infant stages. These findings are in

line with what Goh et al. (2015) that indicated as positive influences of PSO PMS application. In general, as it was found in this case study, mitigating mechanisms for both identified PMS risks, were in the form of other control tools themselves, complementing the core PMS process.

7.5 Additional management control systems: PMS complementarity and risk integration

The main control tool that not only complements and influences PMS but is also embedded and influencing all other controls and control systems that complement PMS, is the risk mindset that serves as a strategic social control tool. This social control dictates that all daily activities of the MA and its employees, should have a clear reflection on risk. This mindset, instilled at the strategic level and directed to the bottom of the organisation, majorly championed by the CRO and the QAO, has one clear mentality. This mentality, this significantly desired attitude, is that all decisions at all organisational levels are made in that way that they integrate the element of risk handling. Effectively, everything the organisation does, has risk at the back of its decision. This was crucial in managing risk in the case MA. As a consequence, the MA, and the QAO in particular, value the meaningful application of the risk management tool, as directed by the MCS, and value the flexibility that it offers in enhancing their risk appetite. That is why many operators and the CRO or the MA director, constantly scan the eternal environment of the MA and its projects, to identify emergent risks. As such, the risk mindset serves as a central control tool that reinforces the effectiveness of all control tools in the case study (Bedford, 2020). At the same time, this extends the view of Palermo (2014) that risk officers are important in the adoption, implementation and facilitation of not only risk management practices, but also integrated controls. And that was particularly evident in the successful maintenance of a proper working environment, without affecting their service, and without project delays, during the Covid19 pandemic. It also provides evidence that risk culture is associated with a successful integration between risk management and control (Bracci et al., 2024). As such, risk influences this social control of the case MA, by instilling a mindset and a set of risk management values. However, many operators at the operational level, indicated that it is not easy to embed this mentality due to understaffing issues and the lack of senior level management support.

Another control tool that complements the role of PMS at all organisational levels, is overarching rules of engagement, the MCS. This tool, that serves as a technical control tool, delineates the acceptable domain of action for project operators and how they can monitor projects. It also guides senior level management to the most appropriate actions when deciding for changes in the programme. At the operational level, the MCS sets the rules of managing projects and internal operations. It is also advised when emergent risks arise, to guide the appropriate mitigating action. Moreover, the MCS sets the rules for maintaining a clear risk management tool. Risk is so important for the EC funds that they have integrated it in a clear and sophisticated risk management tool, within the MCS, to be followed by all MAs, in a flexible manner. For the risk management tool, that is a technical control tool used to delineate the acceptable risk and the acceptable domain of mitigation action, it follows the same processes as the MCS. Moreover, the MCS serves in supplementing the PMS, as I many cases, it sets the desired performance of the organisation, its projects and its beneficiaries (Bedford, 2020). Risk is later infused into all MCS rules, procedures and areas of concern, as it is represented by these rules, in an effort to mitigate it. However, the sophistication of this tool has been questioned during data collection. Indeed, and to reflect the sector-wide approach, the application of this tool has been deemed a mere box-ticking exercise. Despite the fact that the MA applies the risk management tool with passion and a lot of support from championing senior level managers, it lacks depth. For instance, when risks are identified by beneficiaries and they are communicated with the MA, the operators mitigate them by referring to the law and the MCS to see appropriate action. The do not further brainstorm on ow these risks may or may not manifest in later projects or in the same project as a whole. If the mitigating mechanism adheres to law, then they stop there. They do not break down the risk and its constituencies, as they apply to all project elements, to further project stages or parts. To make matters clearer, by utilising the MCS, the managing authority is trying to mitigate risks that are associated with project delays and loss of funds. Most of these risks are known from previous projects and are usually common in most projects the MA monitors. The MCS itself has been built at its core to mitigate those risks, and when new risks arise, it changes accordingly. Moreover, the management of emergent risks is also embedded in this MCS. Stemming from a new regulation, a new project development, or any event that can negatively affect the project deadlines and fund absorption rate, the MCS is consulted to show how an emergent risk applies as a "risk to be avoided" (Tessier & Otley, 2012, p. 180). Evidently, all participants consult the

MCS in that case, to see not only if this new emergent risk needs to be included in the whole risk management and mitigated, but also how they can mitigate this, and how it can be transformed to known risks. The second integration of risk in MCS, is the integration or risk in the whole MCS boundary system, in a separate set of rules that delineate the risk procedures all MA, and the case MA, needs to follow to manage risks.

In referring to the strategic level now, it is also worth mentioning that the MCS procedures and rules are not static, and change based on MA needs, and emergent risks that are made sense via various avenues, including the web of meetings within the organisation, and the inter-organisational meetings with the SRSA and other MAs. At the strategic level, the MCS is utilised as an opportunity-seeking tool, with risk management (and the risk management tool) being at the heart of this process. For that matter, the main strategic goal of the case MA is to adhere to the MCS and make sure that their risk management tool, as translated by all MCS operational areas, is utilised appropriately. If the risk appetite changes, due to new emergent risks, then, senior level management consult with the SRSA to modify the MCS to ensure strategic coherence, and alignment with rules and regulations. That happens with the utilisation of interactive meetings between the MA, the SRSA and the Ministry or the European Commission itself, when and where required. All this process is triggered by changes in the risk appetite for the MA and effectively, the whole process is dictated by the logic to engage in proper risk management. At the strategic level, these interactively utilised communications are used in an effort to reinforce the MCS and its application (Bedford, 2020).

A key process of how the MCS works is through the fraud risk management as part of the MCS. At this area, the MCS shows the way the fraud risk management took works, which as integral in the MCS. In this technical control tool, which delineated the rules for responding to, managing and mitigating fraud risk at the operational level, risk was integrated as it delineated the procedures required to manage it. The tool itself delineated all fraud risks in all elements and stages of each project, from its integration to completion. In there, the risk was reflected in the fraud risk categories that the team devised, that covered the key fraud areas that needed attention. Fraud risk categories affect the rules for fraud risk, delineating the appropriate and detailed descriptions, project elements and procedures required to be followed, to allow for the minimum lack of evidence when a fraud claim is investigated. This risk integration also influences the feedback process that was devised and used interactively. For that matter, the

case MA has designed and utilised a complain form that anyone can go and report fraud, online, available to all stakeholders. In essence, the publicly available complain forms are used interactively to generate feedback on fraud risk handling by the MA and is used to affect changes in the fraud risk management system to decrease fraud in the future and manage it more efficiently. As a result, the case MA can re-evaluate fraud risk and effectively make sense of new emergent fraud elements, and also receive feedback to re-evaluate and update their fraud risk management processes and procedures. Finally, the area of fraud risk management in the MCS, delineates the rules of engagement for all the MA employees, effectively designed to reflect risk. As such, these rules are clearly influenced by fraud risk, as they are devised to mitigate fraud from internal MA employees, and beneficiaries. However, this system is not perfect, as there is room for misappropriation. In February 2023, following a tragic railway accident killing 57 people in one of the central railway arteries in Greece, 4 officials of the case MA were prosecuted with allegations for misappropriation of funds for this specific railway construction (EPPO, 2023). The accident mainly occurred due to the improper implementation and use of the railway signalling system. As such, it was not built or used as intended. However, the court has not reached a conclusion yet. The point here is that, given these charges, there fraud risk management tool is still incomplete, as there is room for misappropriating funds, and it is something that might need to be set by the case MA, via stricter rules covered by the fraud risk management tool.

Finally, and to complement the rules of the MCS, the MA and its projects, need to comply with the relevant law and regulation. In general, and in line with the findings of Burke & Demirag (2019), the case MA, as dictated by the MCS and the relevant law and regulation, utilised a set of criteria and rules for contractors, that aim at reducing the risk of no completion and the risk of incompetent contractors. Effectively, this is an additional technical boundary control tool, utilise at both organisational levels, to make sure that projects, internal operations and strategic decisions are adhering to EU and national regulation. This additional boundary technical control also supplements the PMS (Bedford, 2020). For this tool, risk is reflected to the compliance or non-compliance with law and regulation and is embedded into tools that are used in monitoring beneficiary and internal organization compliance, to ensure adherence to all relevant laws and regulations. Here, to diagnose the levels of risks and if the regulation is followed accordingly, a set of technical controls are used diagnostically. For example, the IIS

plays a pivotal role here, as it is used to ensure project stages are completed in a law-abiding manner, when communicated by the beneficiaries through formal IIS inputs. Moreover, interactive controls complement this process when it comes to making sense of emergent risks in ensuring beneficiary and internal organisation compliance. Since the IIS is not always complete, and given the fact that many decisions are final, to avoid delays and faulty IIS input, interactive informal meetings are devised to discuss issues with beneficiaries, identify and mitigate emergent risks, and have the most efficient input in the IIS for project continuation. This allows for law compliance when the IIS is populated by the beneficiaries, and it ensures that project stages are completed or continuing in a lawful manner, thus avoiding project delays. As such, interactive meetings are used here to compensate for the IIS limitations (Bedford, 2020). However, delays are not always inevitable. For example, when a new law is in effect, it might take months to be applied, or procedures that follow the law, for example court appeals from project sub-contractors, might take more than expected to be completed. As a result, this control tool cannot completely address all possible project delays. Subsequently, evidence from this study support the co-existence of informal, vernacular, risk management systems, with other formal systems in PSO risk management processes, in the form of controlling for risk management (Carlsson-Wall et al., 2019). Moreover, evidence suggests that, in the case of risk management integrated in control systems, tacit systems are used to enhance PSO risk management.

At the heart of all procedures above, and the PMS, lies the function of the risk management team of the MA. This technical control tool, chaired by the CRO, is used both interactively and diagnostically within the case MA, as part of their operational and strategic operations, and performance, as discussed in section 5.2. As shown from the evidence, the risk management team has a central role in the MA, designed by the organisational itself, with representatives from all operational units, and a clear communication with senior management. In there, and with the help of formal interactively utilised meetings, not only risks and emergent risks are brainstormed, and uncertainty is framed, but the team also triggers corrective actions, which are later communicated throughout the organisation, with the aid of unit representatives as carriers of information to their irrespective units. This team also engages with inter-organisational interactive meetings to communicate risks and make sense of the wider uncertainty of the wider MA environment. Mainly by the representation of the CRO and the

CQP, that is done through communicating and sharing experiences with other MAs, in annual SRSA moderated meetings. Sometimes, talks and brainstorming with the SRSA and other MAs in that fashion, may trigger new approaches to managing projects, and as such, updates to the MCS elements. These meetings, as it will be further discussed in the next section, are the heart of the control system for the organisation, and they are influencing all other control procedures, as they are used in a compensating, enabling and reinforcing manner (Bedford, 2020). Therefore, this study extends Bedford's (2020) typology by providing evidence of the multi-effect of control tool interconnectedness, especially in controls that are central to a specific procedure, that of managing risk and uncertainty.

The discussion above, triggers a discussion on how findings are compared with previous literature. For instance, in extending literature on the antecedents of the implementation of RM (Bracci et al., 2022), evidence supports the findings of Subramanian et al. (2011) that the higher-level of uncertainty perceived for the organization, the more sophisticated the RM. That was evident in the case study from the establishment of the sophisticated procedures of risk management, further translated into different control systems. That is also because the case MA has high probability of losing funds, as the materialisation is often complex, or done by inexperienced contactors. The level of uncertainty the case MA is exposed to, is relatively high. However, this level of sophistication, still needs to go deeper. For example, the case MA needs to find a way around picking up certain risks at a sequence, effectively focusing on a single event/risk at a given point in time and start focusing on the bigger picture of managing all risks at the same time and for all project elements. That would reduce project delays. Moreover, evidence suggests that factors such as the centrality of IT systems (Woods, 2009; Nedaei et al., 2015), the size of the projects and the decentralised approach to operations, decision-making and risk management, were positively affecting the sophistication of risk management procedures. While this study supports this view, it also argues that an additional aspect that directly affects the sophisticated implementation of risk management tools and procedures, was the risk mindset of the organisation. The case MA significantly and passionately to have a sophisticated risk management system, and the CRO, the QAO and the director played a pivotal, championing role in instilling this mindset throughout the whole organisation (Kaplan & Mikes, 2016). Everything they do has risk directly or indirectly connected, whether it is decision-making, allocation or resources on projects, project completion and changes, or other

internal organisational decisions and processes. Subsequently, this study supports the findings that utilising a clear risk management thinking, can enhance the achievement of organisational objectives in PSO, with clear connections to project success, effective use of funds and reduced fraudulent activities (Hood & Smith, 2013). This mindset later extends to framing risk and uncertainty for the case MA. Indeed, evidence from this study also suggests that inter-organisational collaboration was key in creating a culture of integrating risk management and control systems. This was evident mainly in the use of risk management mindsets at all organisational levels. Thus, the conclusions of Hinna et al. (2018) are supported by the evidence of this study.

On the other hand, mixed results emerge for some elements of the study. For example, findings differ from Woods (2010) that found that risks are identified in middle-level management and are communicated at senior level management. Evidence from the case MA suggest a bottom-up approach, especially from the project beneficiaries to the operators, then the risk management team and then at senior levels, through constant communications between the CRO and the director. Also, compared to Woods (2010), risks were not directly fed into a PMS system, but they were rather indirectly connected to meeting specific project and programme targets. This is only in line with Woods (2009) findings, when the imposition of CPA targets was utilised as risk target indicators. Moreover, this study contradicts the findings of Rana, Hoque & Jacobs (2019). In the case study utilised, evidence suggests a full integration between risk management and management control, with an inclusion of all areas of risk that might affect the organisational strategy and strategic objectives and did none of the risks were overlooked.

7.6 Management control for emergent risks: processes and technologies.

In general, the case MA utilises a variety of technical control tools, in an interactive manner, to make sense and manage emergent risks, at both the operational and the strategic levels. Many of these tools are also informal and tacit. They are also influenced by a Greek culture characteristic that maintains a sense of honour in completing work. That translates back to the use of additional control tools, majorly informal, to manage issues with their system disregarding formal emergent risk management procedures. Indeed, there is an issue with the formalised approaches of the risk management tool, as this is constructed by the MCS

authorities. In there, the risk management tool, despite its sophisticated application in the particular MA, does not convey adequate information on how to manage and mitigate emergent risks. The notion of emergent risk is very vague in the MCS risk management tool and does not have clear formalised procedures. The risk management tool also ignores certain risk categories. But, on the other hand, MAs are given the flexibility to adjust this tool to their needs for that matter. That is why the MA themselves had to add their own category that reflects emergent risks in the tool, with mechanisms that match their circumstances. The process and control tools the MA have utilised works bottom-up from the beneficiaries, and goes back to the organisation, from the operators, to the CRO and to the director. Moreover, these procedures influence and dictate part of the process, in other control systems, discussed in the previous sections.

One technology that the case MA utilises to make sense of emergent risks, is the IIS. The MA, as dictated by the MCS, utilises the ISS to communicate emergent risks with beneficiaries. When a beneficiary, which is in close relationship with its sub-contractors, realises an emerging issue that might affect any of the elements of the completion of a project, communicates this information, formally, by IIS input. This IIS input often wise shows how stages of a project are affected, e.g. funding. However, the IIS system does not sow the full picture of the issue, and the MA cannot clearly agree on a pathway to solve it. That is because the IIS and its applications, as dictated by the MCS, is disconnected from emergent risks, as it is mainly used to mitigate known risks. As such, one more time, interactively used meetings are utilised here as a control to compensate for the weakness of the IIS (Bedford, 2020). As such, project operators use this information to make sense of emergent risks and to trigger interactively used meetings with the beneficiaries to better understand these, in an informal fashion. Operators pick all relevant IIS information up and complements this process with informal meetings, to make better sense of the information and discuss mitigating mechanisms, and to help the beneficiary take corrective action, to avoid delays. As such, the IIS and the informal meetings are two complemented control tools that are used to make sense of emergent risks at the operational level, both used interactively and in an enabling way.

To complement the process above, and when the IIS returns with a project issues, operators monitor the situation and report to the risk management team meetings. If a new issue arises, in the form of new regulation or new project issues, the operator discusses this within the

relevant meeting, and mitigating mechanisms are devised and communicated to the team, their units, and relevant operators. As such, corrective action is taken. Therefore, these meetings are utilised as a technical control tool, used interactively, to make sense of emergent risks at the operational level. Therefore, evidence suggests that formal or tacit systems of information exchange appeared in making sense of emergent risks, as suggested by Scheytt et al. (2006) and Fischbacher-Smith and Fischbacher-Smith (2014). Evidence also supports the view of Fischbacher-Smith and Fischbacher-Smith (2014) that these formal and informal information sharing systems enhance the understanding of emergent risks, as they played a pivotal role in the case study. Moreover, many of them were informal bottom-up directed channels (Fischbacher-Smith & Fischbacher-Smith, 2014), to convey information from the projects themselves and the contractors, to the operators, the risk management team, and the director of the MA, where necessary, to trigger mitigating actions. These systems were also devised to be part of the risk management agenda of the case MA, supplementing other control systems, as discussed above. Therefore, in contrast to the conclusions reached by Fischbacher-Smith and Fischbacher-Smith (2014), and as evidenced from the case study, tacit informal systems are presented and fully utilised in the public sector. The only issue with these systems was that picking up of emergent risks happens one at a time and ranked based on impact. That nullifies the mitigating mechanisms put in place, as all these risks might be connected with each other. All emergent risks are not fully addressed at the time they arise, thus instilling unavailable delays.

Another tool that is used in conjunction with the tacit informal information systems and the IIS, in an effort to make sense of a wider range of emergent risks, is the Action Plan. For that matter, when the action plan is updated, has the ability to trigger procedures to identify emergent risks in projects, that operators have not yet picked up. As a result, the action plans compensate the IIS and basically all other avenues of making sense of emergent risks (Bedford, 2020). The tool, because it represents and shows a snapshot of completion stages and EC fund absorptions, for a specific point in time, it might show project progress that was not picked up by any operators. As a result, the operators see this depiction and go over to discuss with beneficiaries and uncover issues not earlier picked up, with other avenues. In that case, the Action Plan shows a pathway to direct operators to uncover emergent risks, in problematic projects, and in that case, a technical control tool, at the operational level, used diagnostically

to make sense of emergent risks. Effectively, the action plan triggers a process of meetings, as described above, to make sense of this uncertainty, from beneficiaries to the CRO and the MA director. This evidence from the case study shows how a different mode of presenting data other than graphical representations (Themsen & Skærbæk, 2018) are also useful in framing emergent risks. The use of the IIS, and the vast, detailed excel map of the Action Plan, enhance emergent risk management through the addition of extra detail. That is later re-enforced with the filter tools that can give a snapshot of a project, or an area of funding issues, a set of high-risk projects in the form of colours, or any attention-drawing software elements, that serve as a graphical representation of uncertainty.

Moreover, at the strategic level, the risk management tool serves as the very essence of the maintenance of the risk management procedures withing the case MA. The strategic purpose of the MA is to update this tool with relevant risks, according to their needs. That process works two ways. If they MA identifies a risk that is relevant to their operations or programme, they discuss it internally, frame it with the mechanisms discussed above, and bring it to the attention of the SRSS in formal and informal meetings. That is done to seek legitimate agreement that this risk needs to be managed, from the overlooking authority. The same applies to all relevant MAs that this risk management tool applies to. Then, if the SRSA deems that this risk is relevant, they feed it to other MAs. That triggers the second process of how emergent risk is communicated and framed. Effectively, the SRSA engages into meetings with risk representatives from all MAs. At these meetings, all MAs are brought together to the table to discuss new emergent risks and new inclusions to the risk management tool, in a collaborative and sharing fashion. This process applies if the SRSA has identified that an emergent risk applies to all MAs. When the meetings are done, the case MA takes back this information to their organisation, and applies the mitigating mechanism discussed with the SRSA. Both processes described above, serve as an uncertainty sense tool, and as a trigger for corrective action. As a result, the case MA utilises all of these meetings above, interactively, as a technical control tool, to make sense of emergent risks in their projects and operations, that they could not make sense trough other avenues, and this tool complements the other control tools, forming a system that is specifically designated to make identify, and later manager, emergent risks, in a holistic manner. Here, as it has already shown before, interactive meetings are used to enable the use of the MCS, and, in this case, the specificities and procedures of the risk

management tool. Indeed, as it will be shown below, all these tools are part of the same systems, that is hold together with a single mechanism withing the case MA.

Speaking of which, the most important sensor of emergent risks, that complements the above, are the web of meetings utilized in a connected fashion, throughout the whole organisation. For that matter, in the plethora of meetings that the case MA is utilising as a technical control tool in an interactive manner, emergent risks are integrated clearly and play a central element of discussion to make sense of uncertainty, at all organisational levels. These webs of meetings go from the bottom of the organisation to the top, and affect project management, internal operations and organisational strategy. In a nutshell, these meetings work in multiple ways. For example, there is an abundance of constant inter-organisational meetings of the director and the senior level management with the EC, regulators and the ministry, as well as the SRSA and other legal overlooking bodies. Other MAs are also included in these meetings when it comes to identify emergent risks, as discussed in section 5.4 That is done to see programme updates and progress, funding issues and any other elements that might affect the programme strategy. These meetings are complemented by reports from all relevant bodies. All this information triggers new meetings within the organisation. Effectively, the director discusses with the CRO, QAO and other senior level managers, new advancements and new information on the programme progress, for example. The CRO then takes this information and presents it to the risk management meeting, that frames how all emergent issues affect the organisation and its projects. Then, corrective action is implemented at the operational level, triggered by emergent risk management. Furthermore, the web of meetings also works in a bottom-up fashion. At the internal, intra-organisational, operational level, operators exchange information via interactively utilised meetings with beneficiaries, and exchange information both through the IIS and informally, to make sense of emerging projects risks. Those later feed back to the MA and other projects, through the IIS and the risk management meeting, that frames uncertainty and mitigating action, through its discussions on new regulation, new external environment advancements, and new project changes. The risk management meetings then disseminate this information to the senior level and to all units and operators. Another example is how these meetings serve as a tool to enhance or update the risk management tool, as part of the MCS. In essence, they are utilised to bring emergent risks to the risk management team, via the risk management meeting, and then disseminate this information to the strategic level, and the

regulatory body, to induce an update to the risk management tool. Essentially, it is like a web of very well-designed optical fibre system of constantly exchanging information, both formally and informally, with the risk management meetings at the heart of the system. These web of meetings, are reinforcing the effect of all other control practices and, at the same time, compensate and enable them, via the use of the risk management meetings (Bedford, 2020). Here, risk is not only integrated in all information exchanges, but this whole system is completely influenced by the notion of emergent risks, and with an aim at making sense, and later on, mitigating these. Finally, it was evidenced from the case study that all these webs of meetings, together with the risk mindset social control, are the main contributors to holistically manage risk in the case MA. The meetings serve the purpose of integrating the notion of risk and risk mindset in the organisation as a whole, as they are the ones that communicate all available information on risks, emergent risks, mitigating mechanisms and corrective action, as well as re-enforce the engagement of all MA employees, at both the strategic and the operational levels, with the notion of risk management that the case MA has implemented from the top managerial level. Webs of meetings are the glue that keeps all MA members together towards managing their risks. In fact, these webs of informal meetings, complemented by the formality of the meetings of the risk management team, supported the identification and management of emergent risks in the case study very effectively. As it can be concluded from the findings of the study, the key activity of these informal tools was the exchange of knowledge and ideas of emergent risk management throughout the organisation (Laguir et al., 2019). Starting from the operational level, operators identify and discuss, with their colleagues, situations that emerge in their projects, and ways to manage these situations, in their respective teams. After all, different project might require different approaches to managing risk and emergent risk. The same applies at the internal operational level. Then, this identification triggers an exchange of information between these employees and their risk representatives in every unit. These representatives later collate and communicate this information in the risk management team meetings, and they also discuss how their teams managed these issues. Then, in the risk management meeting, an organisation-wide approach to manage risks that have been identified as important to the organisation, emerges. This is then communicated to the strategic level to ensure that the strategic direction of the organisation is not invalidated or changed if the main strategic goals are threatened. At the strategic level, the management of these events is agreed and further communicated to the operational levels, according to the resource

capabilities of the organisation. The process described above also works the other way. If a change in organisational strategy is required at the strategic level, for example a re-allocation of funds or operator attention of projects that are of high risk to not be finished on time, then a directive is provided. As a result, operators are advised to either speed up processes or focus their attention into different projects. Conclusively, informal avenues of information exchange was very much present in various technical control tools utilised interactively by the case organisation to convey information for emergent risks and course of action, as well as re-direction of organisational efforts when a project was at high risk on not achieving the required targets of fund absorption and deadlines.

However, despite their importance, no connection of these information systems was found, to make sense of reputational risks (Power et al., 2013). This was something that emerged only after the study and the QAO was keen to explore as an inclusion to the risk management tool. That happened mainly because the case MA is not responsible for utilising funds, but for ensuring their appropriate and effective/efficient utilisation. As such, loss of funds was majorly outside of the control of the MA, as these may be affected by external influences, like politics, new laws and regulations, or even contractor competencies. In a similar vein, this study extends the literature on how public sector organisations utilise technologies, in a holistic manner, to understand and shape uncertainty. Evidence from this study suggest that IT-based systems are integral in realising emergent risks (Themsen & Skærbæk, 2018), especially when used interactively in an enabling way. It was evidenced in the case MA that, for any project, the ISS and the on-site verifications, as discussed in section 5.3, serve as a way to make sense of emergent risks, as these are shaped in the field, and communicated directly from project contractors to the project operators. However, due to workload issues, sometimes operators went the extra mile to engage with further discussions, as these controls were not enough. Moreover, there were issues with information relevance withing the IIS and the on-site verifications. IIS was not updated and did not include all information required, and on-site verifications sometimes did not uncover the whole truth. As such, operators had to use their own time and effort to engage in informal communications with the project contractors and the beneficiaries, to better understand the issue. Later, if a new issue rose withing a project, it was communicated interactively within the Beta unit and with the risk management team at the team meetings, to be brainstormed and an approach agreed. The latter was later on

communicated to the organisation, or relevant members, to ensure the issue is managed. At the same time, the controls used to identify emergent risks, also influence the use of other control systems, as presented in the previous sub-sections of this chapter. For example, when an emergent risk arises in a project, operators consult the MCS to show the acceptable domain of action for mitigating those risks. All meetings discussed in this section, have the power, and are utilised, to make changes to the MCS in accordance with new relevant mitigating mechanisms that those emergent event dictate. The same applies to the feedback channel of the fraud risk management tool. Finally, operators engage in informal meetings to make sure all emergent risks are addressed before finalising the IIS input for the completion stages of a project.

7.7 Synergy and tension

The purpose of this brief, final, discussion is to reconcile the discussions in sub-sections 5.3 to 5.5 on how the levers of control are utilised by the case MA, with particular reference to risks and emergent risks. This reconciliation will be offered to discuss how the various controls form a system and are connected with each other, effectively extending management control literature on the matter (Tessier & Otley, 2012). As it is evident from Figure 4.6, in sub-section 6.3, some controls are utilised at both organisational levels, to manage risks to be avoided (boundaries) and performance. For example, the social control that exudes a risk-oriented mindset, is present and utilised in all control systems. The same applies for the technical control that exudes the web of meetings for organisational learning throughout the organisations. The risk mindset social control creates synergy between all control systems as it delineates the acceptable domain of opportunity seeking at the strategic level, in terms of devising strategies and activities that not only exude a risk-oriented attitude, but at the same time frame the boundaries of strategy that needs to be formulated to manage all organisational risks. At the same time, this mindset serves as a setter of required performance towards managing risk at all levels and complying with activities that aim at putting managing risk and uncertainty at the heart of the organisational activities at the operational level. In fact, synergy occurs when the risk mindset, as a control tool, travels down to the operational level, to delineate the acceptable way of making project decisions, with mitigating risk at the heart of this process. Moreover, in reflecting managerial choices, this control tool is intended to be used in a constraining way to ensure compliance, but at the same time, in an enabling way, as, when it is used in conjunction

with the technical control of the web of meetings, it informs the choice of this control being used interactive, hence creating tension. Similarly, the web of meetings is used interactively and in an enabling way to enhance organisational learning on best practice on mitigating known risks and increase knowledge and understanding of emergent risks. Here, the utilisation of risk management meetings at the middle-level management, plays a central role, and also serves as they key component of the web of meetings that sticks all control systems together within the case MA. Starting from the operational level, operators, which are close to projects, make sense of known risks and emergent ones, as different projects progress. These operators mase sense of all these through formal and informal meetings with beneficiaries and their contractors, complemented by official communications, for example through the ISS. The same applies to operators in Unit Gamma, that are responsible for internal operations efficiency and mitigating internal risks. Then, this information flows back to risk representatives from each unit, and mainly thought the risk management team meetings, this information is diffused to the CRO which discusses it with Unit Alpha responsible for the programme, and the MA director. That triggers the update of current strategy of the whole MA, if needed, informed by those emergent risks. Then, the senior level management, for example the CRO and the director, reflect this information and devise new actions that need to be taken, and they are communicated to the other units, and the unit operators. Then, once new strategy for projects is formulated, it is communicated to operators which take the necessary actions to manage their individual projects. Here, meetings are used to ensure compliance with the new strategy. Therefore, these meetings are used to inform the necessary elements of action that the MA needs to take to manage all risks associated with their programme, at the strategic level (performance), and set the operational rules of managing projects, with a clear focus managing risk (compliance) creating synergy. Moreover, managers in the case MA, have chosen this web of meetings both interactively and diagnostically, and in an enabling and constraining way, thus creating tension.

Another synergy between operational and strategic boundaries, is created by the utilisation of the MCS as a technical control tool. At the strategic level, the MCS delineates the rules, procedures and structures the MA needs to follow in operating and seeking strategic opportunities when it comes to operating, managing, and terminating the cycle of EC funds. At this level, risk management is central as it is not only a standalone requirement of the MA that needs to transform into a proper risk management tool, but also, all other elements of the MCS

are formulated, in constant communication with the SRSA through meetings. Therefore, at the strategic level, the MCS is utilised as an element of strategic opportunity seeking. At the same time, the MCS is diffused at the operational level and sets the acceptable domain of activities that the operators need to follow in order to complete projects. Or, in the case of Units Alpha and Gamma, the integration criteria of projects, and the rules and regulations that the M operations need to follow, respectively. As such, the MCS is utilised as a tool to manage compliance with rules and regulations, at the operational level. This technical control tool has been chosen by managers to serve in an enabling way at the strategic level, interactively, and in a constraining manner at the operational level, hence creating tension.

Furthermore, in the case of the operational boundaries and strategic control systems, post-completion on-site verifications of fully operational projects, as a technical control tool, are used to ensure that the MA complies with the regulation that requires these types of verifications to ensure the operation and the physical presence of the project, is there after its completion (usually within 5 years after completion). As a result, this technical control is utilised diagnostically to ensure compliance. At the same time, these post-completion verifications are used interactively to inform best practice when materialising different projects in the future, at the operational level. This information, is later communicated with senior level managers, usually mediated by formal risk management meetings, to check current strategy and form a response if a post-completion on-site verification has identified an issue. For example, the physical presence of a road network, might have been deformed due to its natural surroundings. If that is the case, a conversation is triggered that discusses the issue with the beneficiary and the MA, as well as the SRSA, and triggers discussions to include new activities in the MCS that require more detailed research from contractors in similar projects in the future. Hence, post-completion on-site verifications materialise the synergy of the operational boundary system, with the strategic and operational performance systems, for the case MA. At the same time, this technical control tool has been chosen to exude organisational learning in an enabling way, and, at the same time, ensure compliance with MCS rules on post-completion verification procedures, hence creating tension.

In a similar manner, on-site verifications work to establish a synergy between the operational performance and the strategic performance systems utilised by the MA. Operators, in their daily monitoring of their various projects, utilise on-site verification because this is required as

a process to be completed by the MCS, and also as a way to diagnose how beneficiaries manage known issues of the project, how they comply with regulation, and how the physical object progresses as agreed by the information shared formally through ISS. At the same time, operators utilise on-site verification to unravel emergent issues of their projects that might put their completion and fund absorption at risk. Later on, information gathered from these on-site verifications, is diffused at the strategic level, and usually flows from project operators to unit supervisors, to risk representatives in each unit, to the regular risk management meetings, to the senior level management. The latter, and usually by collaboration of the director, the manager of Unit Alpha and the CRO and QAO, serves as information to formulate strategy on project development and materialisation, inform MCS changes and serve as a tool to inform strategic formulation towards project development, later diffused to operators serving as the rule of the project materialisation game. Thus, managerial choice here creates tension as the on-site verification technical control tool is used diagnostically and in a containing manner to ensure project compliance, and at the same time, interactively and in an enabling manner to inform organisational strategy and attitude towards the whole programme and its projects as a whole.

Another technical control tool that is materialising the synergy of control systems, is the IIS, that connects the strategic and the operational control systems. Information on the system, which is required to be there and communicated with beneficiaries as per the MCS, serves as tool to ensure compliance with the MCS, as all operators needs to use it to formally exchange information with beneficiaries on the different stages of the development of their projects. At the same time, the ISS informs the acceptable performance of operators, and beneficiaries, in terms of meeting deadlines, communicating information and complying with regulation, at the operational levels. This information is collated at the strategic level to show compliance of project performance targets in terms of completion, meeting of regulation and so on, as well as operator performance in terms of replying to beneficiaries, collating reports and managing project deadlines. The ISS and producing information for all the projects in a holistic manner, informs organisational performance as well as delineates the acceptable domain of activities, especially at the operational level. As a result, the ISS, is an oracle system that serves diagnostically and in a containing way, and, at the same time, it is used to ensure compliance with the rules of the MCS in terms of operator-beneficiary communication. Thus, the way this

control tool is used, creates tension. The ISS is complemented by meetings, web of meetings and the risk management team meetings, as mediators to convey this information for the purposes of performance and compliance.

Speaking of information for the programme, and due to the fact that the ISS does not include all relevant information on project completion as, at times, it can lag behind and can be incomplete, it is used in conjunction with the Action Plan, that further strengthens the synergy between strategic and operational performance control systems for the case MA. As discussed in the findings above, the Action Plan serves as a diagnostic technical control tool that provides information on the completion of projects, on a yearly basis, and its importance increases as the EC funding period approaches its end, to show fund absorption. In the action plan, all projects of the programme are seen as a whole, to see progress and fund absorption. Thus, at the strategic level, and through the collaboration of the director, all unit supervisors and the supervisor of Unit Alpha, decision are made to re-allocate funds, if needed, to ensure full EC fund absorption. Moreover, at the operational level, the Action plan sees the completion progress and fund absorption for every individual project, and operators can check the performance of these projects in term of key funding and deadline variables. Operators, by feeding the Action Plan with this information from their projects, not only inform their project monitoring and actions to bring their projects to required completion and funding targets (according to agreed yearly progress targets), but they also populate the excel that reflects the Action Plan, to serves as a tool for programme decision-making at the strategic level. Hence, the Action Plan is a performance management control tool, that is used both interactively and diagnostically and serves as both a containing and an enabling control tool at the same time. That shows that these managerial choices create tension between organisational learning and performance management.

At the internal level, the QAS is a technical control tool that is used to audit that all operations and internal procedures are working as expected from the MCS and the regulations, at the operational level. Moreover, at the same time, senior level management utilises this tool with an aim at managing and monitoring internal operations performance and how the MA operations adhere to rules of the MCS, regulations about staff and project monitoring. The QAS, through audits, is used to set the rules of MA operations at the strategic level, and, at the same time, it is used to delineate the required levels of MA internal operation at the operational

level, as an additional technical control tool that intensifies the synergy of performance controls at both organisational levels. Moreover, managers in the case MA utilise this tool diagnostically in both an enabling and a constraining fashion, hence creating tension due to this managerial choice of control operation.

8 Concluding remarks

8.1 Conclusions

8.1.1 Summary of the study

The primary aim of this study was to explore the integration of risk management and Management Control Systems (MCS) in a public sector setting, focusing on how they coexist, influence one another, with PMS being central towards that effort. This research was grounded in addressing gaps identified in the literature, which primarily overlooked the processes of how MCS are be integrated with risk management frameworks, particularly in public sector institutions. For that matter, the study aimed at answering the following research question:

"How are management control systems integrated with risk management in public sector organisations?

The following data collection questions will be asked:

1. What management control systems are utilised to manage risk in the Greek public sector?
2. What are the processes by which PMS in is integrated in PSO risk management?
3. How do different control systems facilitate the risk management process in the public sector and complement PMS to form a wider control framework?
4. What are the processes by which a PSO controls for emergent risks as part of their risk management framework?

To answer these research questions, and provide evidence, a qualitative case study design was adopted, which allowed for an in-depth exploration of how a public sector organization integrates MCS with risk management to address both known and emergent risks. To provide evidence for this study, a public sector institution in Greece selected that is responsible for managing the materialisation of transportation and environmental/sustainability projects funded by the EC through the 2014-2020 Partnership Agreement for the Development Framework (PADF). Evidently, this organisation is responsible for the proper allocation of EC funds, while at the same time supervised by the Greek Government and the European Commission. For meeting their main strategic and operational objectives, the case MA's dual focus was on ensuring proper project completion within specified timeframes and absorbing allocated funds. This complex environment required the integration of sophisticated risk management systems complemented by MCS to ensure both financial and strategic objectives were met. Indeed, this case provided an exemplary context for exploring the interaction between PMS and other control mechanisms within a risk management framework. Not only the case study had a clear and sophisticated risk management tool the delineated their operations, but they are also proponents of a clear and sophisticated application of all associated risk management procedures. With a strong focus on EC compliance and project-based risk management, the MA was an ideal environment to study how MCS can be utilized to manage public sector risks holistically. For that matter, data were collected through semi-structured interviews, focus groups, documentation analysis, and observations, in line with this study's elected methodology (Broadbent & Laughlin, 1997).

In brief, the Tessier & Otley (2012) framework plays a critical role in the research, providing a robust lens through which the interaction of control systems with risk management can be examined. In general, the framework offers a conceptual understanding of how managers utilise various controls to manage intended strategies, and it proved to be a helpful lens to explore risk management in the public sector, since contemporary risk management has become strategic (Andersen, 2016). Subsequently, and for this study, the revised LOC framework emphasized the dynamic relationships between control systems and risk management tools, particularly in environments characterized by uncertainty and emergent risks. Through its concepts, the important control tools were explored, that were associated with the managing of risk and uncertainty. As a result, this study provided evidence of the

revised LOC framework, as this applies to contemporary risk management of public sector organisations.

8.1.2 Summary of Findings

Before discussing the findings, it is worth giving a summary of the main operations and strategic profile of the case organisation that was utilised in this study, that will later be reflected in the main findings. To begin with, the MA oversees the implementation of the PADF programme, focusing on transportation and environment/sustainability projects that absorb these funds. To make this happen, the MA is divided into three key units. The first one is unit Alpha that is responsible for assessing and integrating projects by advertising them to potential Greek beneficiaries, for example subway developers and local municipalities. Then, this unit weeds out the most capable beneficiaries for materialising projects. Once projects are integrated, they are assigned to beta units, who are responsible for their materialisation and flow of funds. These units are called Beta units. Each Beta unit also has an Alpha sub-unit to work on their projects. Finally, there is unit Gamma, an internally oriented, that manages the organisation's internal needs, such as HR, finance, and regulatory compliance. The case MA is supervised by a director, with oversight from the SRSA and the Ministry of Development and Investments to ensure compliance with European and Greek laws for project materialisation and fund utilisation.

The primary goal of the Managing Authority (MA) is to fully absorb the European Commission funds allocated for the PADF programme, ensuring no funds are lost and that projects are completed within the agreed timelines by the end of the programme period. For the 2014-2020 programme, the target was to absorb and spend 4.7 billion euros. The MA's objectives can be divided into two levels. At the operational level the target is to ensure projects are completed on time and within budget. If this target is met, it will then influence the strategic level target that is to successfully close the programme with all allocated funds absorbed, meaning funds are spent on actual project expenditures, not just projected or planned. Additionally, the programme must meet European Commission targets related to the social impact of projects, such as serving a specific number of citizens, reducing travel times, improving water supply, and enhancing recycling efficiency. These targets are closely linked to risks, as managing all

associated risks and emergent risks is central to all the processes utilised to meet these targets and informs the design of all management control tools utilised for that effort.

The MA faces various risks and uncertainties that could impact its primary targets of fully absorbing European Commission funds and successfully completing projects. The MA's risk profile is centred around a risk management tool, mandated by the European Commission's MCS, but tailored to the MA's specific needs. The MA has the flexibility to influence this tool and tailor it to its needs. This tool classifies risks into categories such as programme risks, operational risks, non-compliance risks, and political/economic risks, and outlines mitigation strategies. Risks are assessed based on their probability and impact on fund loss, with the risk management team regularly updating the tool to reflect new risks or changing circumstances. Examples of risks include understaffed municipalities struggling to manage environmental projects, legal challenges from project beneficiaries, and delays due to inadequate monitoring or reporting by the MA. The tool also addresses emergent risks, such as those posed by the Covid-19 pandemic, which introduced new uncertainties like supply chain disruptions and material price increases. The MA's risk management process involves continuous monitoring, re-evaluation, and adaptation to ensure that all potential risks are effectively managed to meet the programme's targets. As a result, the first and key management control tool utilised by the MA is the risk management tool that they have built, which is used both interactively and diagnostically to manage all risks they are exposed to (Tuomela, 2005). In that effort, specific risk management meetings, an interactively used technical control tool, that are utilised to enhance the process, and discuss emergent risks, and updates in current risks, and mitigating mechanisms. Central to the MA’s risk management processes, these two tools have a specific place in the wider management control framework of the case MA, that is directly influenced by the concept of managing all risks the MA is exposed to.

To manage risk and uncertainty, PMS was central in the case MA. Starting with the operational level, the MA utilised PMS extensively, to oversee critical targets associated with mitigating various risks. This PMS is central to overseeing the progress and success of the projects it manages. This system is designed to ensure projects are completed on time, within budget, and in compliance with EC and Greek regulations. The performance of projects is monitored using pre-set KPIs which focus on timelines, budget adherence, and regulatory compliance. These KPIs serve a dual purpose, also acting as indicators of potential risks, where failures in meeting

these KPIs could signal project delays or financial losses. A key process in monitoring all these targets was found to be the on-site verifications, a technical control tool utilised at the operational level and dictated by the MCS. This tool schedules regular on-site visits, used interactively and in an enabling way, to allow the MA to assess the physical progress of projects, engage directly with beneficiaries, and identify issues that may not be evident through formal communication channels. Moreover, the completion, budget and regulatory KPIs are also confirmed with these visits, which makes this technical tool used in a diagnostic way as well, to ensure compliance. This hands-on approach also helps the MA to diagnose project performance, detect emergent risks and take corrective actions to avoid delays or other project complications. Another tool that monitors project KPIs is the IIS which is crucial technical control tool that supports the MA's operations by providing real-time data on project progress. This system facilitates formal communication between the MA and project beneficiaries, tracking everything from project timelines to compliance with laws and regulations. Therefore, the IIS is a technical control tool utilised in a diagnostic way, to monitor project performance. IIS data are also used to monitor the internal performance of the MA, ensuring that all operations align with the required standards and procedures. In the absence, and in fact the incompleteness of, up-to-date IIS data, the MA utilises the Action Plan, that is an extensive technical control tool used diagnostically, to monitor the status of all projects managed by the MA. It tracks project progress, fund absorption, and identifies projects that require additional attention. Moreover, since the Action Plan is devised by data from all operators, and strategic data, the former have a chance to identify issues with their projects that were not able to identify through other avenues, effectively directing operator attention to crucial project areas. Now, if the IIS, the on-site verifications or the Action Plan identify an issue, or point out to issues with meeting said KPIs, then the MA utilises another technical control tool that aims at directing towards acceptable performance of projects, the risk management meetings. Effectively, the risk management team holds regular meetings to assess and address risks that could impact project completion and fund absorption. These meetings involve representatives from different units within the MA, each responsible for managing risks in their respective areas. The meetings serve both diagnostic and interactive purposes, helping the team to learn from emergent risks and adjust strategies for known risks accordingly, effectively triggering mitigation action. In other words, the risk management meetings are used interactively to assess emergent risks, and diagnostically to check project and internal operation activity and

compliance towards the main KPIs. As such, this technical control is utilised both in an enabling and a constraining way. Finally, to ensure compliance with all rules, regulations, codes of conduct and operational rules, the MA utilises a technical control tool that complements the Action Plan by ensuring compliance with the MCS and other regulations, serving as a safeguard against potential issues that could arise during any external audits. In fact, this tool serves a diagnostic purpose, to ensure operational compliance.

At the operational level, PMS is complemented by a set of other control tools, that form the wider control framework utilised by the MA. These tools, together with the PMS, form the operational boundary and performance systems. Starting with the main rules of the game, the MA needs to adhere to the MCS that outlines the rules framework within which the MA operates, including the procedures for selecting, monitoring, and completing projects. It mandates the use of a risk management system, which the MA implements and customizes to its needs. The MCS serves as a technical control tool at the operational level, utilised in a constraining way, defining the acceptable range of actions and ensuring that all project activities align with legal and regulatory requirements delineated by the EC and the Greek government. Risk management is woven into the fabric of the MCS as all procedures were set in an effort to mitigate project risks and ensure proper project completion. In fact, the MCS is so strong in delineating the rules of project monitoring and materialisation, that all operators refer to it when they need to manage an emergent risk that might arise in a new project. The MCS also gives a strong emphasis on preventing the loss of EC funds and ensuring project completion within the prescribed timelines. Part of the MCS is the risk management tool that, as dictated before, serves in assessing, and mitigating risks at every stage of a project's lifecycle. The risk management tool, mandated by the MCS, is used to classify and monitor risks, while also providing mechanisms for addressing emergent risks as they arise.

At the strategic level of the MA, and to manage risks reflected in its main strategic target, it was also found that PMS is still central to this effort, complemented by other control tools. Similar to the operational level, and to manage programme performance, the MA utilises the Action Plan and on-site verifications, but post-project completion. The Action Plan serves as the central tool for tracking the performance and risk management of the entire programme at a strategic level. The Action Plan at the strategic level is crucial for overseeing the progress of projects by tracking financial data and fund absorption rates, as well as project completion

progress. This vast excel map shows every detail for all the MAs project for the programme period, effectively focusing on every little detail that might affect project completion and fund absorption. As it was indicated by the findings, this tool provides a clear picture of which programme areas are performing well and which might need corrective action, such as reallocating funds between different types of projects (e.g., from transportation to environmental projects) to mitigate risks and ensure full fund absorption. The MA regularly revisits and updates the Action Plan, particularly as the programme period is close to ending, to avoid losing any EC funds. The Action Plan also helps in monitoring uncertainty by identifying potential issues that might not have been previously detected. For example, changes in regulations that could impact ongoing projects are assessed through meetings with relevant units to gauge their effects and decide on necessary actions.

A horizontal team within the MA, which works closely with unit Alpha and the programme director, uses the Action Plan and data from the IIS to monitor the overall programme's financial health and to propose strategic decisions about fund allocation. This team checks for deviations in budget usage across the programme and reallocates funds to projects that are more likely to absorb them efficiently, thereby minimizing the risk of losing EC funds. Moreover, to ensure that projects continue to meet their intended goals even after completion, the MA conducts post-completion on-site verifications within the first five years of a project's completion. This technical control tool, which resembles the operational on-site verifications but with a wider focus, checks that projects have not undergone unauthorized changes that could affect their functionality or long-term value. These verifications, at the strategic level, serve as a diagnostic tool to ensure compliance and an interactive tool to inform future programme strategies. As it was found during data collection, and as the MA prepared to close the 2014-2020 programme and transition to the 2020-2027 PADF programme, these verifications and the subsequent assessments were crucial. The MA submitted a report to the EC evaluating the readiness and capabilities of beneficiaries based on their performance in previous years, which helped inform the planning of the new programme. In summary, strategic performance management in the MA involves using the Action Plan as a dynamic tool for monitoring project performance, managing risks, and ensuring full fund absorption. Post-completion verifications further ensure that projects continue to deliver value and meet long-term objectives, providing essential feedback for future programme planning.

Similar to the operational level, PMS at the strategic level is complemented by other control tools to form a system of tools utilised as strategic performance and boundary tools. For instance, at the strategic level, the MCS serves as a technical tool, that delineates acceptable room for strategic opportunity seeking. However, here, despite the compliance that the tool delineates, the MA, at the strategic level, utilises the contents of this tool, as a way to inform new strategies and strategic developments. For example, and through a constant interaction with the SRSA, the EC and the Greek government, the MA aims at triggering changes in this MCS, in the form of updated rules and procedures, that reflect its strategic needs. Here, this process is utilised interactively to incorporate the notion of emergent risks, as these unravelled throughout a programme period or part of it. In essence, if a new emergent risk arises and requires a new approach to be dealt with, the MA discusses this with the SRSA, the Greek Government and the EC, in conjunction with other MAs, to identify the appropriate response to this new issue, that will trigger a new strategic approach, that will later be reflected to the MCS. As such, the MCS is a tool that is also utilised to ensure strategic compliance, and strategic opportunity seeking for the MA, and the sector of MAs that manage EC funds as whole. As a result, at the strategic level, the MCS is utilised in an enabling way to direct and inform strategic considerations. At the same time, at the strategic level, the MA has designed a risk-oriented mindset, a social control tool that exudes the belief and core values of the case MA, that aims at enhancing risk-informed decision-making at all levels. This mindset, driven by senior management, permeates the entire organization, ensuring that risk management is integrated into daily operations and that any decision that is taken at any organisational level, is taken with considering the effect of risk behind it, and the action to mitigate or at least consider it in this decision. This was particularly evident in the findings when the MA promoted this tool in an effort to promote a culture of risk awareness in response to challenges imposed by the Covid-19 pandemic. Another technical control tool that the MA has designed at the strategic level, equally instilled at all organisational levels similar to the risk mindset, is a complex network of meetings, utilised interactively and in an enabling way, to discuss and manage emergent risks at both the strategic and operational levels. These meetings involve various key stakeholders, including the SRSA, EC representatives, and internal MA units, to address issues, make decisions, and ensure that the programme remains on track. This process is complemented by the use of reports and data communication networks to monitor progress and adjust strategies as needed. In fact, and to monitor external factors that might be unknown

and may affect the programme and could impact project completion, such as market conditions, political changes, and regulatory updates, the MA utilises employee expertise and environment monitoring in an interactive fashion. In that effort, unit Gamma plays a crucial role in scanning the external environment for new laws and regulations, ensuring that the MA remains compliant and responsive to changes. Conclusively, a summary of these findings can be explicitly illustrated in Figure 4.5 depicting the interaction between social and technical controls at both operational and strategic levels. As this figure illustrates, findings of this study support the conceptual understanding of Tessier & Otley's (2012) LOC framework, that conveys that various technical and social control tools are designed and utilised in organisations that form systems. These systems aim at managing operational and strategic performance as well as delineating the operational and strategic boundaries of the organisation. The way controls were utilised for risk management in the case MA followed exactly the classification of Tessier & Otley (2012). However, as it will be shown in the next section, not all elements of the framework were found to be relevant in the findings of this study.

In further reflecting the outer LOC framework in figure 4.5, this study also found evidence on how employees perceive the control systems utilised in the MA. But, before that, and in direct relation to the general perception of the Greek PSO risk management, a few findings need to be summarised. These perceptions have a direct effect on the design of risk management tools, and associated controls, and they influence the controls of the case MA as well. Indeed, risk management in the Greek PSO, so far, primarily involves strict adherence to legal requirements. When risks arise in project materialisation, the process typically involves the beneficiaries following legal procedures and obtaining approvals from the MA, without in-depth analysis or broader risk mitigation strategies. Moreover, there is a tendency to focus on major risks (e.g., archaeological issues) while smaller, potentially impactful risks are often overlooked. This compartmentalized approach can lead to project delays as minor risks become apparent only after major risks are addressed. Finally, the existing risk management procedures in the Greek context are considered embryonic and in need of development to incorporate more comprehensive risk management practices.

Now, turning to the internal employee perceptions, and in reflection of the above, findings of the case study suggest issues, first of all, with the MCS. More specifically, employees expressed concerns about the MCS, particularly regarding unrealistic response times mandated

by the MCS, as are often seen as unachievable, creating stress and prompting workarounds. The Action Plan is also perceived as time-consuming and filled with unnecessary details. Employees find it difficult to adhere to the timelines due to understaffing and project complexities. Many participants also identified problems with outdated or inaccurate data in the IIS, leading employees to rely other tools, such as the Action Plan, to track projects. Finally, the risk management tool was found to lack an effective feedback mechanism, and it does not adequately address risks at both the project and subcontract levels. Some participants believe the tool is incomplete and not reflecting project realities. As a result, many interviewees found it helpful to have a better communication and training regarding the importance of risk management tools and the Action Plan. Employees often see these tools as burdensome rather than beneficial, and there is a lack of clarity on their utility.

8.1.3 A brief discussion of findings

As a key take from the finding for this study, PMS are critical for managing risks in PSO projects, confirming prior research that suggests their centrality to managing organizational risks. For the case MA, and as part of the wider PMS framework of managing project risks, on-site verifications were a key control tool used to check project progress and detect potential risks early on, especially in complex environmental and sustainability projects. These were complemented by post-completion verifications, a strategic control tool, intended to assess long-term project success. But these proved to be often incomplete, leading to operational and strategic failures, as exemplified by a tragic train accident in Greece. To support the wider PMS framework of the MA the IIS was used to track project performance, through real time project data. These data were directly associated with risk as they were clearly indicating projects that were at risk of not being completed on time and the associated reasons. However, the IIS was often outdated or had incomplete data. As such, the Action Plan complements IIS by providing more detailed and up-to-date project information in support of better understanding project performance. Finally, risk management meetings are another essential tool used to address project performance issues and initiate corrective actions. These meetings, that involved key project operators from all units of the MA, served as an information disseminating tool about project and internal performance, clearly indicating risks and emergent risks that might hinder the planned performance, in an effort to discuss these and trigger corrective action. To mitigate the negative impacts of PMS, the case organization has introduced training programs aimed at

improving employee understanding of these systems. However, these initiatives are still in their early stages. There were also social control mechanisms, including informal meetings and personal engagement with project beneficiaries, are used to manage risks more proactively, especially in the early stages of projects, and in reflecting the deficiencies of some PMS tools.

To complement PMS, a set of other technical and social control tools were utilised by the MA with a clear reflection of managing risks. A key social control tool that was utilised in the MA, with direct association to managing risk, was the risk mindset instilled to all organisational members. This mindset, promoted by senior managers such as the CRO and the QAO, ensures that all decisions at every organizational level incorporate risk handling. This risk-oriented approach influences all other control systems and enhances the overall operation of the PMS. This risk mindset is central to all MA operations, ensuring that risk management is considered in daily activities by integrating risk across all decisions. For the case MA this is particularly evident when they are executing the risk management tool, which allows them flexibility the organization adapt to external risks according to their risk appetite. As a result, this risk-based approach helped maintain operations and avoid project delays during the Covid19 pandemic. However, operational staff find it difficult to fully embed this mindset due to understaffing and a lack of senior management support. Another control tool that complements PMS for the case MA was the MCS at all organizational levels. This technical control tool defines the boundaries for project operators and guides senior management in decision-making, especially in risk mitigation. For that matter, it sets rules for managing projects, internal operations, and responding to emergent risks. The MCS also includes the risk management tool to guide flexible and appropriate mitigating actions. Risk is embedded into MCS procedures, and the system is directly designed to prevent risk associated with project delays and fund losses, while using lessons from previous projects to adapt to new risks. However, while the MCS is applied with strong support from management, its application has been criticized for lacking depth. Risk management often becomes a box-ticking exercise, with little analysis on how risks may evolve across project stages. On the other hand, project operators, and the MA as a whole, still utilise the MCS as a way to frame a response to emergent risks, showing how they can be managed and transformed into known risks, ensuring risks are avoided in future projects. At the strategic level, the MCS is dynamic and adapts to the needs of the MA and its emerging issues. For that matter, the MCS procedures and rules are updated based on MA needs and new

risks identified through internal and inter-organizational meetings with bodies like the SRSA. Moreover, the MCS, along with the risk management tool, is used strategically to align with changes in the MA's risk appetite. For instance, senior management consults with the SRSA, the Ministry, and the EC, using interactive meetings to adjust the MCS to ensure strategic coherence and adherence to regulations. Changes in risk appetite trigger this process, with a clear focus on maintaining effective risk management across the organization. Conclusively, the MCS serves as a very important control tool that enhances performance, with a clear direction towards managing risk and uncertainty. To complement the rules set by the MCS, the MA and its projects must also comply with relevant laws and regulations. As an additional technical control tool, the MA follows specific criteria to reduce the risk of project non-completion and the involvement of incompetent contractors, ensuring adherence to EU and national regulations. In turn, this process serves as an additional control tool to complement the PMS, ensuring compliance with legal frameworks. For that matter, the IIS is used to monitor compliance, though it has limitations, leading to delays in project stages due to incomplete inputs or the slow application of new laws. That is complemented by informal meetings with beneficiaries help address issues and emergent risks, compensating for the IIS's limitations and ensuring law-abiding project progression. The main challenge here lies within delays that can still occur due to slow legal processes or new laws, which can't always be mitigated by the control tools.

At the heart of all the above and serving as the main control tool that keeps all control systems in line for the MA, with a clear reflection on managing risks, is the utilisation the risk management team. This team plays a central role in the Ma’s operations and strategic performance. Chaired by the CRO, it serves as both a technical and social control tool, operating interactively and diagnostically to manage risk and uncertainty. For that matter, the team brings together representatives from all operational units, facilitating communication with senior management. It identifies and addresses risks, triggering corrective actions that are communicated across the organization. Moreover, and in exuding inter-organizational collaboration, the team engages in meetings with other MAs and the SRSA, allowing for shared learning and adjustments to control systems like the MCS. This collaboration helps refine risk management practices.

Now, and in specific reference to emergent risks, and in extending previous literature, the study found an amalgamation of control tools utilised by the MA to manage unknown issues. To make sense, and manage, emergent risks, the MA uses a combination of formal and informal control tools to manage emergent risks. Informal tools often compensate for weaknesses in formal systems, such as the IIS, which lacks detailed data. For instance, informal, bottom-up communications of operators with beneficiaries, often through meetings, is key to identifying and mitigating risks that are not captured through formal channels when it comes to project materialisation. The IIS is also used to communicate emergent risks, but it is often incomplete, so it is supplemented by informal meetings and the Action Plan. The Action Plan highlights risks and issues that may not be visible in the IIS, prompting further action. Both tools work together to provide a clearer picture of project progress and emerging risks. Speaking of meetings, they proved to be central to the MA's risk management, both within the organization and with external entities like the SRSA and other MAs. These meetings help frame risks, facilitate information sharing, and prompt corrective actions. This network of meetings acts as a control tool, ensuring that risks are identified and managed at all levels. For example, The MA collaborates with other organizations to manage shared risks and update the risk management tool based on new information. However, despite the MA's sophisticated risk management system, it lacks mechanisms to fully address reputational risks, and workload issues sometimes hinder effective risk identification. Moreover, it was found emergent risks are often handled sequentially, which can delay overall risk mitigation. There is a need for more comprehensive approaches to manage multiple risks simultaneously across projects.

Finally, and to comprehend these findings better, it is worth noting that the case organisation had some particular feats, at the point of data collection. The most important feat was that the case MA had an abundant exposure to devising tools and managing risks for at least 5-6 years. The notion of risk management in the Greek PSO, especially for organisations managing EC funds, only started in the mid-2010s, around 2015. Before that, as discussed in the findings, the notion of risk management was overlooked. As a result, these tools that the case MA has devised, have been practiced, updated and utilised for many years for the current EC funding round of 2014-2020. That gives a more robust picture of management control tools for risk management, that has been practiced in the context of service provision. At the same time, the case MA is also flexible to devise their own tools and have the freedom to discuss and apply

their risk management tool as they see fit, for their purposes. This is something that needs to be considered, especially when devising informal control tools. The interaction with these tools, and their testing through time and different situations, make them more sophisticated. Moreover, not only the MA was flexible, but they were influenced by their willingness to develop and utilise these tools appropriately, as a way of promoting and regulating the effective and efficient provision of services. If funds were lost in the process, the Greek government and its reputation would be degraded, leading to reduced funds in future programmes. Following that, and despite increased workloads and understaffed operations, the organisational support to risk management and associated control tools, was very high. That was majorly affected by the Greek sense of honour that was abundantly present in the case MA. As pointed out by the CRO, they want to be a model MA and manage their projects in the most efficient and effective way possible. However, it is also worth noting that this effort is hindered by the fact that risk management in the Greek public sector is still at a low level of sophistication at the sector. As a result, and despite the MA efforts, they might sometime work with organisations that materialise their projects, that do not have a clear direction of what risk management is. Thus, this might contribute to unexpected or unintended results when managing risk and emergent risks. That was particularly evident in the case of the small project materialisers working for environmental and sustainability projects. Mega-project operators faced a different approach, as they are usually working with experienced, large beneficiaries that have systems and rules in place, to materialise projects.

8.1.4 Summary of contributions

This study contributes to current management control and risk management literature in several ways. First, this study contributes to the continuous calls to better understand the relationship between risk management and management control (Bhimani, 2009; Soin et al., 2013). As it was found in the case study, and for the PSO, risk management and management control are integrated. The study also showed how this integration applies to a public sector context, through the use of various control tools that were directly associated and designed with a clear focus on managing risks and uncertainty. As a matter of fact, the whole management control framework of the case study was directly designed to manage risk and emergent risks for all its operations and projects, at both the operational and the strategic level. As such, this study adds to the ongoing calls for an understanding of the integration of risk management and

management control, especially how the formed affects the structure, design and behaviour of MCS systems in PSO (Rana et al., 2019). Through that effort, this study adds to how the processes of integration work in practice (Bracci et al., 2022; Rana et al., 2022). Indeed, and through the Tessier & Otley (2012) LOC framework, it was found that many control systems within the case study were important in managing risk and identifying emergent risks. These systems were directly associated with the strategic considerations of the organisation under study. Moreover, the context of the study proved fruitful, as the background, expertise and persistence of the organisational members, instilled a sophisticated application of a risk management framework directly associated with managing all risks the case MA was exposed to. As such, it was evident that a variety of control tools and systems were clearly responsible for managing public service risks (Rana, Wickramasinghe & Bracci, 2019). Subsequently, this study, through the case study design, provided evidence of the integration and co-existence of management control systems for public sector risk management, in a holistic manner, that was also put in a theoretical basis, that of Tessier & Otley (2012), something extends previous literature on conceptualising these controls (Bracci et al., 2021). Through the use of this framework this study also added to the current management control literature by providing evidence of the application of the revised Levers of Control framework, as requested by the authors, and especially through the use of case studies (Tessier & Otley, 2012). As it was evident in the case study, not only the framework applies to explaining the wider management control framework in PSO, directly influenced by risk management, but also, the concepts held very well when it came to co-existence of the aforementioned control systems.

Moreover, this literature added to the need to better understand a specific element of control, that of performance management for risk in the public sector, a tool that is key in managing public risks (Power, 2004b), but partly explored (Cuganesan et al., 2014). It is clear in the literature, that performance management systems do aid public sector risk management (Woods, 2009, 2010; Rana, Hoque & Jacobs, 2019), and that was evident in the case study, despite their inherent issues in quantifying public sector performance, due to its complexity and multi-dimensional character (Bouckaert & Balk, 1995; Smith, 1995). Indeed, PMS was the central framework that guided risk management in the case organisation, as it was used to diagnostically monitor strategic and operational performance, clearly influenced by risk. Through the PMS, the case MA monitored project and internal performance, to ensure not only

compliance with the MCS rules and the pre-determined deadlines and elements of projects, but to also ensure compliance with laws and regulation, both internally and to their beneficiaries. These targets, if met, they would directly mitigate risks associated with project completion and absorption of funds. However, as proposed in the literature (Cuganesan et al., 2014), this risk-oriented PMS, is indeed only part of the wider framework for managing risks, as the case study PMS was complemented by other control tools, to form the wider control framework of the organisation. This study's empirical evidence showed that PMS for risk management was complemented by a set of tools that aimed at reinforcing the risk management process. All these tools were combined and operated together to build a wide control framework clearly directed by risk management concepts and directions. The way they were combined was mainly by helping each other solve control issues (Bedford, 2020). For instance, at the operational level, and with clear PMS-oriented focus, the IIS was used to enhance the effect of on-site verifications via sharing vital information for operator attention. At the same time, and because the IIS did not show a big picture of performance (operational or strategic), the Action Plan was used to compensate for that. For the MCS, the rules of the game for the case MA, it supplemented PMS in a way that it was dictating the intended performance targets. The same applied to the external regulation that the MA and its beneficiaries needed to adhere to. Moreover, the Action Plan also compensated the IIS when it came for emergent risks. The IIS itself did not show the full picture of projects to fully understand emergent issues, and the Action Plan did. Finally, to ensure MCS compliance and to reinforce its application, extending to the IIS as a result, QAS was utilised to compensate for its application within the MA. All of these control tools were also held together and reinforced, enabled and compensated by the web of meetings within the MA. This vital tool, reinforced by the risk mindset instilled in the organisation, helped all other control tools. For example, when on-site verifications were not enough to show the full picture of an emergent issue or project risk, interactive meetings were utilised with beneficiaries for more details. The same applied to IIS to check law adherence, avoid delays by discussing issues inputted in the IIS before they are final. At the same time, these meetings were utilised at the strategic level to reinforce the application of MCS via its updates to reflect emergent MA strategies. One way or another, interactive meetings reinforced other control tools. They also enabled and compensated them with the use of risk management meetings, as all information for new risks, performance results and so on, were passed through that meeting to be later on applied to other tools to work as intended. Finally, the risk mindset

served as the wide umbrella to further reinforce and enable all of these control tools. For instance, this set of values enabled the use and operation of the Action Plan, and the MCS as a whole, when it came to its application. As such, this study not only confirmed Bedford's (2020) typology, but extended it by providing evidence of its multidimensional existence for key control tools in a control framework. Risk management controls was also found to enhance and complement each other in many ways. For the same risk exercise, however, control tools are mainly connected through a complementing and substituting way. Not all Bedford's classifications of relationships were observed for control in PSO risk management. Furthermore, for the case MA, there were rules to be adhered to (MCS, external law and regulation), compliance procedures such as the QAS, organisational values and mindsets (risk mindset) and a network of meetings. All these, aided the application of the PMS as they informed targets, influenced its application and instilled corrective action. As a result, the role of performance management is central to managing PSO risk, but they do not work alone as they need the support of a wide array of other tools that reinforce their operation (Cuganesan et al., 2014). Moreover, the study unravelled that, in line with previous propositions, that PMS systems have inherent risks by themselves (Cuganesan et al., 2014). This was evident in the case study as the PMS utilised for risk management carried its own risks in the case MA, in the form of PMS systems misinterpreting information and the risk of PMS systems negatively affecting employee performance. It was also found that for the case MA, and in reflecting the Greek context, no reputational risks were directly associated with the PMS system in the case organisation.

Furthermore, the current study, and in an effort to further understand the use, role and influence of management control tool for managing public sector risk (Bhimani, 2009; Soin et al., 2014; Bracci et al., 2022), offers evidence on the use of management control tools in a very important neglected area of risk management: managing emergent risks. As an integral part of the risk management process, emergent risk identification is extremely important, and this study provides evidence of their existence, as key in contemporary risk management, and as a part of the wider control framework of the case study (Scheytt et al., 2006). As it was found in the case study, there is an amalgamation of control tools, usually informal, that can be used to identify emergent risks, which are pivotal to enhancing the risk appetite and risk mitigation of an organisation. Specifically for the case study, these tools were also directly connected and

influenced by emergent risks, as their sole purpose was to exactly extract useful information for the nature of these risks, in an effort to frame them and manage them. For instance, to make sense, and manage, emergent risks, the MA uses a combination of formal and informal control tools, something which is in line with previous literature that argues for the tacit, informal use of information systems to make sense of these risks (Fischbacher-Smith & Fischbacher-Smith, 2014). Examples from the case study include informal, bottom-up communications of operators with beneficiaries, often through meetings, is key to identifying and mitigating risks that are not captured through formal channels when it comes to project materialisation. The IIS is also used to communicate emergent risks, but it is often incomplete, so it is supplemented by informal meetings and the Action Plan. In turn, the Action Plan highlights risks and issues that may not be visible in the IIS, prompting further action, especially by operators. The Action Plan, since it gives the bigger picture for projects, brings information to the attention of operators, that they could have not seen via other routes. Both tools work together to provide a clearer picture of project progress and emerging risks. Speaking of meetings, they proved to be central to the MA's risk management, both within the organization and with external entities like the SRSA and other MAs. These meetings help frame emergent risks, facilitate information sharing, and prompt corrective actions in the forms of updating the MCS or various risk mitigating mechanisms and approaches. This network of meetings is integral and central to managing emergent risks, as information exchange through it, is vital for making sense of uncertainty in projects and internal operations. That was particularly evident when the MA collaborates with other similar organizations to manage shared risks and update the risk management tool based on new information. Since this process of identifying emergent risks is vital in public sector risk management (Power, 2007), this study, further extends current literature on the interplay, integration and practice of control systems for risk management (Bracci et al., 2022), through evidence for the use of control tools to manage emergent risks.

Conclusively, this study contributed to management control and public sector risk management literature in several ways. Initially, it explored the integration of risk management and management control in the Greek public sector, adding to the relevant literature on evidence of how these two practices are integrated, specifically in the Greek PSO context (Bracci et al., 2022). Through evidence on various management control systems that were utilised in the case study, it was evident risk management directly influence management control tools. These tools

are integrated in the risk management process by clearly identified processes, procedures and influences, that have implications for practice. That created space to answer calls in the literature to enhance practice and policy in PSO risk management (Rana et al., 2019; Rana et al., 2022). Hence, this study extended previous literature on the the implementation of risk management frameworks in PSO and what control tools were utilised in that effort, (e.g., Woods, 2009, 2010; Collier & Woods, 2011; Rocher, 2011; Paape & Speklé, 2012; Rana, Hoque & Jacobs, 2019) by showing not only the controls tools that are associated with risk management in PSO, but also how they worked and influenced each other. In this effort, this study focused on specific management control tools, for example PMS tools which we found to be central to managing PSO risk, further extending current literature (Power, 2004b), and showed how these systems are not only central to PSO risk management, but that they also co-exist with other control tools, forming a wider risk management and management control framework (Cuganesan et al., 2014). Additionally, the study addressed the limited evidence on managing emergent risks through management control systems, particularly information-sharing systems (Scheytt et al., 2006; Fischbacher-Smith & Fischbacher Smith, 2014) and control tools for identifying emergent risks (Themsen & Skærbæk, 2018; Jordan et al., 2013). Finally, by applying the revised Levers of Control theory (Tessier & Otley, 2012), this study extended current literature in understanding how management control tools are integrated with PSI risk management (Rana et al., 2020). That in turn, extended the management control literature shoing how these two notions are connected (Bhimani, 2009; Soin et al., 2014) and how a specific management control theory applied to management control systems integrated in PSO risk management frameworks.

8.2 Implications for practice.

The findings of this study, have implications for practice. Even though not perfect, a set of control tools can be devised by PSO to manage risk and uncertainty. In fact, it is the appropriate design and implementation of control tools that makes the diffusion of risk management practices more effective. Starting with risk, it would be beneficial if risk in service provision is reflected to the overall targets of the organisation. For mega projects in particular, that absorb and utilise a large amount of funds, this would be beneficial to make sure funds are not lost, and projects are completed appropriately to serve societal needs. As the same time, physical checks of projects and services could enhance performance attainment, as it would make sure

that agreed project elements are present as they are supposed to, to avoid risks of non-completion. Moreover, these physical verifications can make sense of emergent issues, adding to a better understanding of project uncertainty. Given the lack of resources, PSO can also utilise meetings to identify performance issues, and be proactive towards mitigating these. To further enhance performance, regular meetings within the organisation need to be set, to ensure corrective action is taken, and that everyone works with a performance-oriented mindset.

Moreover, a clear set of rules and procedures needs to be established, in order to delineate the support of public service provision, and the notion of performance management that entails risk. These rules, which come from external supervision, or from the regulatory environment of the organisation, can serve as the boundaries within which operations and service provisions are executed, to avoid risks that can lead to failure. They also need to be communicated within the organisation and applied to the public service providers, to ensure compliance. Especially for mega projects, it is particularly important that these rules not only apply but monitored constantly for the provision of public services.

To manage uncertainty, information exchange avenues should be implemented in PSO as they are key to make sense of emergent risks. As it was pointed out from the case study, a web of meetings that starts from public service providers to supervisors of this provision within the organisation, to the senior level management and the external regulators and supervisors, can frame uncertainty. This uncertainty framing can be complemented by visual representations of information and can be framed on how it applies for the organisation. Of particular importance was the informal interactions, as part of these interactive web of meetings, especially with service providers, to informally communicate emergent issues. As a result, the over-reliance on formal knowledge exchange procedures, might not be helpful in adequately framing emergent risks. This needs to be complemented by informal avenues especially at the operational level. Once its application is discussed, mechanisms can be devised to manage it as a known risk, and changes in rules and regulations can be triggered, through discussions with rule enforcers and supervisory organisations. The latter can update rules and procedures accordingly, to incorporate new risks in their risk appetite, and management agenda of the organisation. That might also be applicable to the wider segment of the sector.

Finally, the most important element that helps in managing risk and uncertainty, and that influences all the control practices above, is the mindset of the organisation, that is directly associated with risk management and risk decision-making. That represented the key success factor in the case organisation, when it came to managing risks and emergent risks. This risk mindset can be set at senior level management, and instilled to lower levels on how it applies to each segment of the organisation. However, it is imperative that this mindset is constantly communicated and championed by senior level management. In fact, the design and effect of this risk mindset, was pivotal in the successful implementation of the risk management framework in the case study. Hence, before anything else, PSO needs to influence their organisational members with clear risk management-oriented ideas in their context, before starting to reap the benefits of sophisticated risk management practices.

The findings from the study emphasize the critical role of designing appropriate and effective management control systems in managing risks within the public sector, particularly in the context of large-scale, publicly funded projects. The integration of management control and risk management strategies, particularly through the lens of the Tessier & Otley (2012) LoC framework, emphasizes the need for robust systems that align operational and strategic objectives with risk management protocols. To ensure effectiveness in managing risks, public sector entities should design robust and standardised management control tools that align with the rules and regulations of supervisory entities, governing bodies and other regulators, while allowing flexibility to adapt to specific operational needs. At the same time, policymakers should mandate regular updates and reviews of risk management tools to ensure emerging risks are adequately captured and mitigated, as seen in the case of the MA adapting to the Covid19 events, and in reflecting their own circumstances. Moreover, these risk management tools should reflect frameworks that are integrated with management control tools and systems specifically designed for managing risks. For example, at the operational level, the use of diagnostic and interactive control systems, including on-site verifications and complemented by oracle software support, is critical for real-time monitoring of project risks and performance management. These tools not only monitor compliance with regulatory requirements but also enable real-time identification and management of emergent risks, contributing to improved project performance and fund absorption. At the same time, regular risk management team meetings, as practiced by the MA, should be designed and institutionalized to facilitate

knowledge sharing, performance evaluation, and emergent risk identification. The use of these complementary control systems and regular risk management meetings should be institutionalized. These tools not only monitor compliance with regulatory requirements but also enable real-time identification and management of emergent risks, contributing to improved project performance and fund absorption. In fact, policies should promote the use of integrated information systems, like the IIS, to facilitate transparent and timely data sharing between managing authorities, beneficiaries, and regulatory bodies. This ensures that project performance is continuously monitored, and risk management practices are data driven. Furthermore, establishing regular risk management meetings and fostering a culture of knowledge exchange and information sharing, through the design of informal interactive control tools within management practices, can enhance organizational learning. This practice is crucial for adapting to changing external environments, such as legal and regulatory shifts or political and economic uncertainties and shocks.

The findings of this study also highlight the need to design clear control tools that delineate the adherence to both national and international regulations the PSO is exposed to. Practical implementation of policies should include compliance KPIs, systematic audits, and performance assessments against established benchmarks to mitigate risks associated with non-compliance. Finally, given the identified risks related to staff shortages and operational inefficiencies, policy recommendations should include streamlined processes for public sector recruitment, staff training, and resource allocation. This is critical to maintain operational performance and manage risks related to project delays and fund absorption.

As far as policymakers are concerned, they need to ensure a standardization of risk management tools is followed. Policymakers should establish standardized risk management frameworks, such as the European Commission Management and Control System (MCS), allowing flexibility for organizations to adapt these tools to specific operational contexts. Policies should also mandate regular updates to risk management tools to accommodate emergent risks, such as those introduced by the COVID-19 pandemic, ensuring that public sector entities remain resilient to external shocks.

8.3 Limitations and avenues for future research

Despite the richness of this study's findings, they must be treated with caution. One limitation of the study is that it explores the use of control systems for risk management in a PSO that has a specified supervision model. However, it has been suggested in the literature that there are different modes of public service supervision (Wise & O'Leary, 2003; Hämberg, 2013; De Groot, 2015). For example, there are strict supervision on public services (Wise & O'Leary, 2003), and the supervision of services might differ based on context, regulation and the services themselves (Hämberg, 2013). Moreover, there is evidence of different modes of supervision even at the (PPP) level of a contract executed with public funds (Gao & Liu, 2019). All the above suggest that there are different public sector contexts, with a variety of autonomy and characteristics. This case study has a specific mode of regulatory and government supervision, with a lot of autonomy. That applies especially when building, moderating and managing their risk management tool, which, despite being dictated at its base, it allows for flexibility to meet the case MAs needs, environment and risk exposure. Taking this into account, other modes of supervision, or lack of flexibility in applying risk management tools, might yield different practical or even behavioural results, in the design and influence of controls for risk management, and vice versa. Therefore, future research should explore case studies with different supervision modes.

Adding to the limitations of the context, this study utilised a single case study design. The results were very rich and fruitful, but the context itself still provides limited results for the sector as a whole. For that matter, Bracci et all (2022) call for research on the integration of RM in international contexts. This study is a good starting point for the Greek context. As a result, more case studies, especially comparative case studies or multiple case studies, can show the way integration of RM and MACS is applied into different contexts and enhance literature findings. By utilising the same theoretical framework, these case studies can also provide evidence on the application of this framework in different contexts. For example, the case organisation considered in this study had specific limitations, cultural influences, regulatory environments and modes of risk management implementation, intervention and application. Other contexts might offer different practical considerations due to different culture, different supervision and different stakeholder engagement. In this study, for example, stakeholder engagement was not dominant in managing risks. That had implication for the integrated

controls. However, many key stakeholders are important in framing and influencing risk management and associated controls. For example, when it came to PMS, no external stakeholder engagement was found to be relevant. That was because, mainly, this was not the study focus. However, especially when it comes to PMS (Siccilia & Stecollini, 2017; Melo & Mota, 2020), stakeholder participation and communication of targets, is important, as it influences value creation. Therefore, future research may explore this direction and provide more empirical evidence to add to this study, especially in the case of performance management for risks. As a result, stakeholder might be extremely central to the process, thus influencing control tools. Therefore, exploring the same integration of risk management and management control, especially through the LOC perspective, in different contexts with different characteristics, would be fruitful to add more complete results in future research.

Finally, previous literature has pointed out the importance of the influence of society on controls. Some societal aspects were found, like Greek sense of honour, but since this was not the focus of the study, no more societal aspects were uncovered. However, recent research has suggested that the design and appropriateness of controls is influenced by society and institutions (Chenhall, 2003; Greve et al., 2017; Ramasinghe & Wickramasinghe, 2021), or from social aspects such as social capital (Chenhall et al., 2010). As such, future research can expand on the influence of society on the design of controls in managing risk, especially since PSO risk management it targeted for society itself (Andreeva at al., 2014). Different cultural contexts will have different characteristics and will influence the design of controls for RM differently, affected by politics, culture and other contingent external and internal environmental characteristics.

9 References

Adler, P. S., & Chen, C. X. (2011). Combining creativity and control: Understanding individual motivation in large-scale collaborative creativity. *Accounting, Organizations and Society*, *36*(2), 63-85.

Ahrens, T., & Chapman, C. S. (2004). Accounting for flexibility and efficiency: A field study of management control systems in a restaurant chain. *Contemporary accounting research*. *21*(2), 271-301.

Alawattage, C., & Wickramasinghe, D. (2014). Systems Logic, Unpublished Manuscript.

Alvesson, M., & Kärreman, D. (2004). Interfaces of control. Technocratic and socio-ideological control in a global management consultancy firm. *Accounting, Organizations and Society*, *29*(3-4), 423-444.

Andersen, T. J. (2016). *Introduction: Strategic Risk Management* in Andersen, T. J. (2016). *The Routledge Companion to Strategic Risk Management*. New York: Routledge.

Andersen, T. J. & Young, P. C. (2023). Reshaping Public Sector (Enterprise) Risk Management. *International Journal of Public Admnistration,* 1-6.

Anderson, S., & Guilding, C. (2006). Competitor-focused accounting applied to a hotel context. *International Journal of Contemporary Hospitality Management. 18*(3), 206-218.

Anderson, R. (2011). *Risk Appetite and Tolerance*. London: Institute of Risk Management.

Andreeva, G., Ansell, J., & Harrison, T. (2014). Governance and accountability of public risk. *Financial Accountability & Management*, *30*(3), 342-361.

Anthony, R. N. (1965). *Planning and Control Systems: Framework for Analysis*. Boston: Harvard University Press.

Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of Enterprise Risk Management. *Accounting, Organizations and Society*, *35*(7), 659–675.

Arena, M., Arnaboldi, M., & Palermo, T. (2017). The dynamics of (dis)integrated risk management: A comparative field study. *Accounting, Organizations and Society*, pp. 65–81.

Arjaliès, D. L., & Mundy, J. (2013). The use of management control systems to manage CSR strategy: A levers of control perspective. *Management Accounting Research*, *24*(4), 284–300.

Arnaboldi, M., Lapsley, I., & Steccolini, I. (2015). Performance Management in the Public Sector: The Ultimate Challenge. *Financial Accountability & Management, 31*(1), 0267-4424.

Barros. R.S., & Ferrerira, A.M.D.S.D.C. (2022). Management Control Systems and Innovation: a levers of control analysis in an innovative company. *Journal of Accounting & Organizational Change. 18*(4), 571-591.

Basel Committee. (2001). *Sound practices for the management and supervision of operational risk.* Bank for International Settlements: Basel Committee Publications.

Baxter, P., & Jack, S. (2008). Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. *The Qualitative Report. 13*(4), 544-559.

Beasley, M., & Frigo, M. L. (2007). Strategic risk management: creating and protecting value. *Strategic Finance,* 25-32.

Bebbington, J., Larrinaga, C., & Moneva, J. M. (2008). Corporate social reporting and reputation risk management. *Accounting, Auditing & Accountability Journal, 21,* 337.

Bedford, D. S. (2015). Management control systems across different modes of innovation: Implications for firm performance. *Management Accounting Research, 28*, 12-30.

Bedford, D. S. (2020). Conceptual and empirical issues in understanding management control combinations. *Accounting, Organizations and Society, 86*, 101187.

Beck, U. (1992). *Risk Society: Towards a new modernity*. London: Sage.

Binder, A. (2007). For love and money: Organizations' creative responses to multiple environmental logics. *Theory and society*. *36*(6), 547-571.

Bisbe, J., Batista-Foguet, J. M., & Chenhall, R. (2007). Defining management accounting constructs: A methodological note on the risks of conceptual misspecification. *Accounting, organizations and Society*. *32*(7-8), 789-820.

Bhimani, A. (2009). Risk management, corporate governance and management accounting: Emerging interdependencies. *Management Accounting Research*, *20*(1), 2–5.

Bleyen, P., Klimovský, D., Bouchaert, G., & Reichard, C. (2017). Linking budgets to results? Evidence about performance budgets in European Municipalities based on a comparative analytical model. *Public Management Review, 19*(7), 932-953.

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

Bracci, E., Tallaki, M., Gobbo, G., & Papi, L. (2021). Risk management in the public sector: a structured literature review. *International Journal of Public Sector Management*.

Bracci, E., Mouhcine, T., Rana, T. & Wickramasinghe, D. (2022). Risk management and management accounting control systems in public sector organisations: a systematic literature review. *Public Money and Management. 42*(5), 395-402.

Bracci, E., Bruno, A., D'Amore, G. & Ievoli R. (2024). The integration of performance management and risk management in the public sector: an empirical case. *Journal of Management Control, 35*, 157-163.

Braun, V. & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in Psychology. 3*(2), 77-101.

Braun, V. & Clarke, V. (2023). Toward good practice in thematic analysis: Avoiding common problems and be(com)ing a knowing researcher. *International Journal of Transgender Health. 24*(1), 1-6.

Broadbent, J., & Laughlin, R. (1997). Developing empirical research: an example informed by a Habermasian approach. *Accounting, Auditing & Accountability Journal. 10*(5), 622-648.

Broadbent, J., & Laughlin, R. (2008). Middle-Range Thinking. In R. Thorpe & R. Holt (Eds) *The Sage Dictionary of Qualitative Management Research.* London: Sage, 130-133.

Broadbent, J., & Laughlin, R. (2009). Performance Management Systems: A Conceptual Model. *Management Accounting Research. 20*(4), 283-295.

Broadbent, J., & Laughlin, R. (2013). *Accounting Control and Controlling Accounting: Interdisciplinary and Critical Perspectives.* Bradford: Emerald.

Broadbent, J., & Laughlin, R. (2014). Middle-Range Thinking and Management Control Systems. In D. Otley & K. Soin (Eds) *Management Control and Uncertainty.* London: Palgrave McMillan, 255-268.

Brivot, M., Himick, D., & Martinez, D. (2017). Constructing, contesting and overloading: a study of risk management framing. *European Accounting Review, 26*(4), 703-728.

Brunsson, N., & Sahlin-Andersson, K. (2000). Constructing organizations: The example of public sector reform. *Organization studies*, *21*(4), 721-746.

Burke, R., & Demirag, I. (2019). Risk management by SPV partners in toli road public private partnerships. *Public Management Review, 21*(5), 711-731.

Cäker, M., & Siverbo, S. (2011). Management control in public sector Joint Ventures. *Management Accounting Research, 22*(4), 330-348.

Caldarelli, A., Fiondella, C., Maffei, M., & Zagaria, C. (2016). Managing risk in credit cooperative banks: Lessons from a case study. *Management Accounting Research*, *32*, 1–15.

Capaldo, G., Constantino, N., Pellegrino, R., & Rippa, R. (2018). The role of risk in improving goal setting in performance management practices within public sector: An explorative research in court offices in Italy. *International Journal of Public Administration, 41*(12), 986-997.

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), 3-19.

Chartered Institute of Management Accountants. (2005). *Terminology.* CIMA Publications.

Chenhall, R. H. (2003). Management Control Systems design within its organizational context: Findings from contigency-based Research and direction fort he future. *Accounting, Organizations and Society, 28*, 127-168.

Chenhall, R. H., Hall, M., & Smith, D. (2010). Social capital and management control systems: A study of a non-government organization. *Accounting, Organizations and Society, 35*, 737-756.

Collier, P. M., & Berry, A. J. (2002). Risk in the process of budgeting. *Management Accounting Research*, *13*(3), 273–297.

Collier, P. M. (2009). Fundamentals of risk management for accountants and managers. Routledge.

Collier, P. M., & Woods, M. (2011). A comparison of the local authority adoption of risk management in England and Australia. *Australian Accounting Review*, *21*(2), 111-123.

Committee of Sponsoring Organizations of the Treadway Commission. (2004). *Enterprise Risk Management - Integrated Framework, Executive Summary*. AICPA.

Cooper, D. J., & Morgan, W. (2008). Case study research in accounting. *Accounting Horizons, 22*(2), 159-178.

Cuganesan, S., Guthrie, J., & Vranic, V. (2014). The riskiness of public sector performance measurement: a review and research agenda. *Financial accountability & management*, *30*(3), 279-302.

Dai, N. T., Free, C., & Gendron, Y. (2019). Interview-based research in accounting 2000-2014: Informal norms, translation and vibrancy. *Management Accounting Research, 42*, 26-38.

Dávila, A., Derchi, G.B., Oyon, D. & Schnegg, M. (2023). External complexity and the design of management control systems: a case study. *Management Accounting Research.* 100875, https://doi.org/10.1016/j.mar.2023.100875

De Groot, M. (2015). Supervision of Public Service Performance by Private Providers: the Relevance of the EU Law. *European Procurement & Public Private Partnership Law Review, 10*(4), 243-253.

Demirag, I., Khadaroo, I., Stapleton, P., & Stevenson, C. (2012). The diffusion of risks in public private partnership contracts. *Accounting, Auditing & Accountability Journal*, 25(8), 1317-1339.

De Villers, C., Dumay, J., & Maroun, W. (2019). Qualitative accounting research: dispelling myths and developing a new research agenda. *Accounting & Finance, 59*(3), 1459-1487.

European Commission (2014). *Summary of the "Partnership Agreement" with Greece, 2014-2020.* European Commission: Brussels. Available from: https://commission.europa.eu/document/download/af8f5454-1e8c-45ad-bf91-

e8e3bb4d82a0_en?filename=partnership-agreement-greece-summary-may2014_en.pdf [Accessed 14 March 2024].

European Public Prosecutor's Office (EPPO). (2023). *Greece: EPPO charges 23 suspects with crimes involving railway signalling systems.* EPPO. Available from: Greece: EPPO charges 23 suspects with crimes involving railway signalling systems | European Public Prosecutor's Office (europa.eu) [Accessed 15 March 2024].

Ferreira, A., & Otley, D. (2009). The design and use of performance management systems: An extended framework for analysis. *Management accounting research*. *20*(4), 263-282.

Flemig, S., Osborne, S. & Kinder, T. (2016). Risky business – reconceptualizing risk and innovation in public services. *Public Money & Management, 36*(6), 425-432.

Fombrun, C. J., Gardberg, N. A., & Barnett, M. L. (2000). Opportunity platforms and safety nets: Corporate citizenship and reputational risk. *Business and society review*, *105(1),* 85-196.

Fone, M., & Young, P. C. (2000). *Public sector risk management*. Oxford: Butterworth-Heinemann.

Fossey, E., Harvey, C., McDermott, F. & Davidson, L. (2002). Understanding and evaluating qualitative research. *Australian and New Zealand Journal of Psychiatry. 36*(6), 717-732.

Financial Reporting Council (2005). *The combined code of corporate governance.* London: FRC.

Financial Reporting Council (2014). *Guidance on Risk Management, Internal Control and Related Financial and Business Reporting.* London: FRC.

Fischbacher-Smith, D., & Fischbacher-Smith, M. (2014). What lies beneath? The role of informal and hidden networks in the management of crises. *Financial Accountability & Management*, *30*(3), 259-278.

Gao, R., & Liu, J. (2019). Selection of government supervision mode of PPP projects during the operation stage. *Construction Management and Economics, 37*(10), 584-603.

Georgiou, V., & Favotto, A. (2021). New Development: Management control for emergent risks in the public sector-a levers of control perspective. *Public Money & Management. 42*(6), 417-419.

Gephart, R. P., Van Maanen, J., & Oberlechner, T. (2009). Organizations and risk in late modernity. *Organization Studies*, *30*(2–3), 141–155.

Goh, S., C., Elliot, C. & Richards, G. (2015). Performance management in Canadian public organizations: findings from a multiple-case study. *International Journal of Productivity and Performance Management, 64*(2), 157-174.

Gomm, R., Hammersley, M. & Foster, P. (2000). *Case study and Generalization* in Gomm, R. Hammersley, M. & Foster, P. (Eds), *Case Study Method.* London: Sage, 98-115.

Gond, J.P., Grubnic, S., Herzig, C. & Moon, J. (2012). Configuring management control systems: Theorizing the integration of strategy and sustainability.

Gong, M., Z., & Sabramaniam, N. (2018). Principal leadership style and school performance: mediating roles of risk management culture and management control systems in Australian Schools. *Accounting & Finance, 60*(3), 2427-2466.

Greek Ministry of Development and Competition. (2014). *Corporate Agreement for the PADF 2014-2020 Development Framework.* Athens: Greek Republic, p. 1-191.

Greve, J., Ax, C., Bedford, D. S., Bednareck, P., Brühl, R., Dergård, J., Ditillo, A., Dossi, A., Gosselin, M., Hoozée, S., Israelsen, P., Janscheck, O., Johanson, D., Johansson, T., Madsen, D. O., Malmi, T., Rohde, C., Sandelon, M., Strömsten, T., Toldbod, T., & Willert, Jeanette. (2017). The impact of society on management control systems. *Scandinavian Journal of Management, 33*(4), 253-366.

Hägg, I., & Hedlund, G. (1979). “Case studies” in accounting research. *Accounting, Organizations and Society, 4*, 135-143.

Hämberg, E. (2013). Supervision as control system: the design of supervision as a regulatory instrument in the social services sector in Sweden. *Scandinavian Journal of Public Administration, 17*(3), 45-64.

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

Hayne, C., & Free, C. (2014). Hybridized professional groups and institutional work: COSO and the rise of enterprise risk management. *Accounting, Organisations and Society, 39*(5), 309-330.

HEFCE. (2001). *Risk management: a guide to good practice for higher education institutions.* (2001/29).

Hennink, M., & Kaiser, B. N. (2022). Sample sizes for saturation in qualitative research: A systematic review of empirical tests. *Social Science & Medicine, 292*, 114523.

Henri, J. F. (2006). Organizational culture and performance measurement systems. *Accounting, organizations and Society*, *31*(1), 77-103.

Hiebl, M. R. W. (2024). The integration of risk into management control systems: towards a deeper understanding across multiple levels of analysis. *Journal of Management Control, 35*, 1-16.

Hinna, A., Scarozza, D., & Rotundi, F. (2018). Implementing risk management in the Italian public sector: hybridization between old and new practices. *International Journal of Public Administration, 41*(2), 110-128.

Höglund, L., Mårtensson, M., & Thomson, K. (2020). Strategic management, management control practices and public value creation: the srategic triangle in the Swedish public sector. *Accounting, Auditing & Accountability Journal, 34*(7), 1608-1634.

Hood, C., Rothstein, H., & Baldwin, R. (2001). The government of risk: Understanding risk regulation regimes. Oxford: Oxford University Press.

Hood, C & Miller, P. (2009). 'Public Service Risks: What's Distinctive and New?' *CARR Special Publication – Risk and Public Services,* 2–3.

Hood, J. & Smith, T. (2013). Perceptions of quantifiable benefits of local authority risk management. *International Journal of Public Sector Management, 26*(4), 309–319.

Hoque, Z., Covaleski, M. A., & Gooneratne, T. N. (2013). Theoretical triangulation and pluralism in research methods in organizational and accounting research. *Accounting, Auditing & Accountability Journal, 26*, 1170-1198.

Huber, C., & Scheytt, T. (2013). The dispositif of risk management: Reconstructing risk management after the financial crisis. *Management Accounting Research*, *24*(2), 88–99.

Huber, M. (2011). *The Risk University: Risk identification at higher education institutions in England*. Centre for Analysis of Risk and Regulation at the London School of Economic and Political Science. http://eprints.lse.ac.uk/38891/1/The_risk_university_Risk_identification_at_higher_education_institutions_in_England.pdf

Hutter, B. M. (2006). *Risk, Regulation and Management* in Taylor-Gooby, P., Zinn, J. (Eds.). *Risk in Social Science*. Oxford: Oxford University Press.

ICAEW. (1999). *Internal control – Guidance for directors on the combined code (Turnbull Report)*. London: Institute of Chartered Accountants in Ireland and Wales.

IRGC, International Risk Governance Council (2005). *Risk Governance: Towards and Integrative Approach*. Geneva: IRGC.

Jemaa, F. (2022). Recoupling work beyond COSO: A longitudinal case study of Enterprise-wide Risk Management. *Accounting, Organizations and Society, 103,* 101369.

Jordan, S., Jørgensen, L., & Mitterhofer, H. (2013). Performing risk and the project: Risk maps as mediating instruments. *Management Accounting Research*, *24*(2), 156–174.

Kaplan, R. S., & Mikes, A. (2016). Risk management – The revealing hand. *Journal of Applied Corporate Finance, 28*(1), 8-18.

Kim, K., Andrew, S. A., & Jung, K. (2021). Building resilient organizations: Organizational resilience as a network outcome. *International Journal of Public Administration. 44*(15), 1319-1328.

Kober, R., Ng, J., & Paul, B. J. (2007). The interrelationship between management control mechanisms and strategy. *Management Accounting Research*. *18*(4), 425-452.

Kominis, G. & Dudau, A. (2012). Time for interactive control systems in the public sector? The case of Every Child Matters policy change in England. *Management Accounting Research. 23*(2), 142-155.

Laguir, L., Laguir, I, & Tchemeni, E. (2019). Implementing CSR activities through management control systems: A formal and informal control perspective. *Accounting, Auditing & Accountability Journal, 32*(2), 531-555.

Langfield-Smith, K. (1997). Management control systems and strategy: A critical review. *Accounting, Organizations and Society. 22*(2), 207-232.

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

Laughlin, R. (1995). Empirical research in Accounting: alternative approaches and a case for "middle-range" thinking. *Accounting, Auditing & Accountability Journal. 8*(1), 63-87.

Laughlin, R. (2004). Putting the record straight: a critique of 'methodology choices and the construction of facts: some implications from the sociology of knowledge'. *Critical Perspectives on Accounting. 15*(2), 261-277.

Lee, B., Collier, P. M., & Cullen, J. (2007). Reflection on the use of case studies in accounting, management and organizational disciplines. *Qualitative research in Organizations and Management: An International Journal, 2*(3), 169-178.

Lee, B., & Humphrey, C. (2017). Case studies in accounting research, in Hoque, Z., Parker, L. D., Covaleski, M., & Haynes, K., eds., *The Routledge Companion to Qualitative Accounting Research Methods.* Routledge: Abingdon, 163-183.

Leitch, M. (2008). *Intelligent Internal Control and Risk Management.* London: Routledge.

Lleo, S. (2009). Risk Management: A Review. *The Research Foundation of CFA Institute: Literature Review.*

Lewis, R. L., Sutton, N. & Brown, D. (2024). How senior managers use interactive controls to manage strategic uncertainties: An attention-based view. *Management Accounting Research. 62*, 100864.

Louth, J., & Boden, R. (2014). Winging it? Defence procurement as risk management. *Financial Accountability & Management*, *30*(3), 303-321.

Lukka, K., & Modell, S. (2010). Validation in interpretive management accounting research. *Accounting, Organizations and Society, 35*(4), 462-477.

Mahama, H., Elbashir, M., Sutton, S. & Arnold, V. (2020). Enabling enterprise risk management maturity in public sector organizations. *Public Money & Management, 42*(6), 403-407.Malina, M.A., Nørreklit, H.S.O. & Selto, F.H. (2011). Lessons learned:

advantages and disadvantages of mixed methods research. *Qualitative Research in Accounting and Management. 8*(1), 59-71.

Malmi, T., & Brown, D. A. (2008). Management control systems as a package—Opportunities, challenges and research directions. *Management accounting research*. *19*(4), 287-300.

March, J., G. (1994). *A Primer on Decision Making: How Decision Happens*. New York; Free Press.

Melo, A., & Mota, L. F. (2020). Public sector reform and the state of performance management in Portugal: is there a gap between performance measurement and its use? *International Journal of Public Sector Management, 33*(6/7), 613-627.

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,* 39-55.

Merchant, K. A., & Otley, D. T. (2006). A review of the literature on control and accountability. *Handbooks of management accounting research*, *2*, 785-802.

Merchant, K. A., & van der Stede, W. A. (2006). Field-based research in accounting: accomplishments and prospects. *Behavioral Research in Accounting, 18*(1), 117-134.

Merchant, K. A., & Van der Stede, W. A. (2012). *Management control systems: performance measurement, evaluation and incentives*. Pearson Education: Essex.

Mikes, A. (2009). Risk management and calculative cultures. *Management Accounting Research*, *20*(1), 18–40.

Mikes, A. (2011). From counting risk to making risk count: Boundary-work in risk management. *Accounting, Organizations and Society*, *36*(4–5), 226–245.

Mikes, A. (2016). The triumph of the humble chief risk officer. In Power, M. (Ed.), *Riskworks: Essays on the organizational life of risk management.* Oxford: Oxford University Press.

Modell, S. (2012). Strategy, political regulation and management control in the public sector: institutional and critical perspectives. *Management Accounting Research, 23*(4), 278-295.

Moeller, R. R. (2011). *COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance (GRC) Processes*. Hoboken: John Wiley and Sons.

Morgan, H. (2022). Conducting a Qualitative Document Analysis. *The Qualitative Report. 27*(1), 64-77.

Mundy, J. (2010). Creating dynamic tensions through a balanced use of management control systems. *Accounting, Organizations and Society*, *35*(5), 499-523.

Nedaei, H. N. B., Abdul Rasid, S. Z., Sofian, S., Basiruddin, R., & Amanollah Nejad Kalkhouran, A. (2015). A contingency-based framework for managing enterprise risk. *Global Business and Organizational Excellence, 34*(3), 54–66.

Office for Students. (2018). *Securing student success: Regulatory framework for higher education in England*. (OFS 2018.01). https://www.officeforstudents.org.uk/media/1406/ofs2018_01.pdf

Oh, Y. (2023). Exploring the dysfunctional consequences of performance evaluation systems: how does 'evaluation overload' affect organizational performance? *Public Management Review*.

Otley, D. T. (1980). The contingency theory of management accounting: achievement and prognosis. *Accounting, Organizations and Society*. 5, 413-428.

Otley, D. T., & Berry, A. J. (1980). Control, organization and accounting. In *Readings in accounting for management control*. Boston, MA: Springer.

Otley, D. (2014). *Management Controls under Uncertainty: Thinking about Uncertainty* in Otley, D., Soin, K. (2014). *Management Controls and Uncertainty*. London: Palgrave Macmillan.

Paape, L., & Speklé, R. F. (2012). The Adoption and Design of Enterprise Risk Management Practices: An Empirical Study. *European Accounting Review*, *21*(3), 533–564.

Palermo, T. (2014). Accountability and expertise in public sector risk management: a case study. *Financial Accountability & Management*, *30*(3), 322-341.

Parker, L., Guthrie, J. & Gray, R. (1998). *Accounting and management research: passwords from the gatekeepers. 11*(4), 371-402.

Parker, L. (2012). Qualitative management accounting research: Assessing deliverables and relevance. *Critical Perspectives on Accounting, 23*(1), 54-70.

Parker, L.D., Northcott, D. (2016). Qualitative generalising in accounting research: concepts and strategies. *Accounting, Auditing & Accountability Journal. 29*(6), 1100-1131.

Power, M. (1999). *The Audit Implosion: managing risk from the inside.* London: Institute of Chartered Accountants in England and Wales.

Power, M. (2004). *The risk management of everything: Rethinking the politics of uncertainty*. Demos.

Power, M. (2007). *Organized uncertainty: Designing a world of risk management*. Oxford: Oxford University Press on Demand.

Power, M. (2009). The risk management of nothing. *Accounting, Organizations and Society*, *34*(6–7), 849–855.

Power, M. (2013). The apparatus of fraud risk. *Accounting, Organizations and Society*, *38*(6–7), 525–543.

Power, M., Scheytt, T., Soin, K., & Sahlin, K. (2009). Reputational Risk as a Logic of Organizing in Late Modernity. *Organization Studies*, *30(2–3),* 301–324.

Power, M. (2016). *Riskworks: Essays on the organizational life of risk management.* Oxford: Oxford University Press.

Public Interest Disclosure Act 1998 (c.23). London: HMSO.

PWC. (2015). *Enterprise Risk Management in the Public Sector: 2015 Survey Results*. Pricewatercoopers LLP. https://www.pwc.se/sv/pdf-reports/enterprise-risk-management-in-the-public-sector.pdf

PWC. (2019). Managing Risk in Higher Education: Higher Education Sector Risk Profile 2019. (190402-105724-HK-UK). Pricewatercoopers LLP *https://www.pwc.co.uk/industries/government-public-sector/education/managing-risk-in-higher-education.html*

Rabaiah, H. I. A., Hanefah, M.M., Masruki, R. Jamil, N.N. (2023). Review of the Public Sector Organizations' Environment: Accounting and Internal Control Systems, and Audit Quality. *International Conference of Business and Technology,* 19-40. Cham: Springer International Publishing.

Ramasinghe, S. B., & Wickramasinghe, D. (2021). Unveiling a postcolonial neoliberalism: hybridised controls and emancipatory potentials for tea-plunking women in Sri Lanka. *Accounting, Auditing & Accountability Journal, 34*(3), 651-679.

Rana, T., Hoque, Z., & Jacobs, K. (2019). Public sector reform implications for performance measurement and risk management practice: Insights from Australia. *Public Money & Management*, *39*(1), 37-45.

Rana, T., Wickramasinghe, D., & Bracci, E. (2019). New development: Integrating risk management in management control systems—lessons for public sector managers. *Public Money & Management*, *39*(2), 148-151.

Rana, T., Wickramasinghe, D. & Bracci, E. (2022). Editorial: Management accounting & risk management - research and reflection. *Public Money & Management, 42*(6), 361-364

Renn, O. (2008). *Risk Governance. Coping with Uncertainty in a Complex world*. London: Earthscan.

Renn, O., Klinke, A. (2016). *Complexity, uncertainty and ambiguity in inclusive risk governance* in Andersen, T. J. (2016). *The Routledge Companion to Strategic Risk Management*. New York: Routledge.

Rocher, S. (2011). 'Re-opening the black box': The story of implementing a risk analysis method in a French local government. *Financial Accountability & Management*, *27*(1), 63-82.

Rossing, C.P. (2013). Tax strategy control: The case of transfer pricing tax risk management. *Management Accounting Research. 24*(2), 175-194.

Rothstein, H., Huber, M. & Gaskell, G. (2006) 'A theory of risk colonisation: the spiralling logics of societal and institutional risk'. *Economy and Society 35*(1), 91–112.

Rika, N., & Jacobs, K. (2019). Reputational risk and environmental performance auditing: A study in the Australian commonwealth public sector. *Financial Accountability & Management, 35(2),* 182-198.

RRAC. (2009). *Tackling Public Risk: A Practical Guide for Policy Makers.* Risk and Regulation Advisory Council, London.

Salmona, M., Kaczynski, D., & Smith, T. (2015). Qualitative theory in finance: Theory into practice, *Australian Journal of Management, 40*(3), 403-413.

Sarens, G., & Christopher, J. (2010). The association between corporate governance guidelines and risk management and internal control practices: Evidence from a comparative study. *Managerial Auditing Journal, 25*(4), 288-308.

Scheytt, T., Soin, K., Sahlin-Andersson, K., & Power, M. (2006). Special Research Symposium : Organizations and the Management of Risk Introduction : Organizations , Risk and Regulation. *Journal of Management Studies*, *43*(6), 1331–1337.

Siccilia, M., Stecollini, I. (2017). Public Budgeting in search for an identity: state of the art and future challenges. *Public Management Review, 19*(7), 905-910.

Simons, R. (1995). Levers of control. Boston, Mass.: Harvard Business School Press.

Soin, K., Huber, C., Wheatley, S. (2014). *Management Controls and Uncertainty: Risk Management in Universities* in Otley, D., Soin, K. (2014). *Management Controls and Uncertainty*. London: Palgrave Macmillan.

Soin, K., & Collier, P. (2013). Risk and risk management in management accounting and control. *Management Accounting Research*, *24*(2), 82–87.

Soobaroyen, T., Ntim, C. G., Broad, M. J., Agrizzi, D., & Vithana, K. (2019). Exploring the oversight of risk management in UK higher education institutions: the case of audit committees. *Accounting Forum, 43(4),* 1-12.

Spira, L. F., & Page, M. (2003). Risk management: The reinvention of internal control and the changing role of internal audit. *Accounting, Auditing & Accountability Journal, 16*(4), 640-661.

Stacey, R. D. (2010). *Complexity and organizational reality: Uncertainty and the need to rethink management after the collapse of investment capitalism.* London: Routledge.

Stake, R.E. (1994). Case study: Composition and performance. *Bulletin of the Council for Research in Music Education.* 31-44.

Sutton, R. I., Staw, B. M. (1995). What theory is not. *Administrative Science Quarterly.* 371-384.

Taleb, N., N. (2007). *The Black Swan: The Impact of the Highly Improbable*. New York: Random House.

Tekathen, M., & Dechow, N. (2013). Enterprise risk management and continuous re-alignment in the pursuit of accountability: a German case. *Management Accounting Research, 24*(2), 100-121.

Tessier, S., & Otley, D. (2012). A conceptual development of Simons Levers of Control framework. *Management Accounting Research*, *23(3*), 171-185.

Themsen, T. N. & Skærbæk, P. (2018). The performativity of risk management framework and technologies: The translation of uncertainties into pure and impure risks. *Accounting, Organizations and Society, 67*, 20-33.

Tuomela, T. S. (2005). The interplay of different levels of control: case study of introducing a new performance measurement system. *Management Accounting Research. 16*(3), 293-320.

Van Doore, W., 7 Hoffmann, C. (2018). Performance management in Europe: an idea whose time has come and gone?" in Ongaro, E. and Van Thiel, S. (Eds), *The Palgrave Handbook of Public Administration and Management in Europe.* Palgrave McMillan: Basingstoke, 207-225.

Vaivio, J. (2008). Qualitative management accounting research: rationale, pitfalls and potential. *Qualitative Research in Accounting & Management, 5*(1), 64-86.

Verbeeten, F. H. M. (2008). Performance management practices in public sector organizations. *Accounting, Auditing & Accountability Journal, 21*(3), 427-454.

Vinnari, E., & Skærbæk, P. (2014). The uncertainties of risk management: A field study on risk management internal audit practices, in a Finnish municipality. *Accounting, Auditing & Accountability Journal, 27(3),* 489-526.

Wahlström, G. (2009). Risk management versus operational action: Basel II in a Swedish context. *Management Accounting Research*, *20*(1), 53-68.

Weitzner, D., & Darroch, J. (2010). The limits of strategic rationality: Ethics, enterprise risk management and governance. *Journal of Business Ethics, 92*(3), 361-372.

Widener, S. K. (2007). An empirical analysis of the levers of control framework. *Accounting, organizations and society*, *32*(7-8), 757-788.

Wise, C. R., & O'Leary, R. (2003). Breaking up Is Hard to Do: The Dissolution of Judicial Supervision of Public Services. *Public Administration Review, 63*(2), 177-191.

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

Woods, M. (2010). Reporting and Managing Risk: A Look at the Current Practice at Tesco, RBS, Local and Central Government. *Chartered Institute of Management Accountants*, 6(8).

Yin, R. (2014). *Case Study Research: Design & Methods.* London: Sage.

Appendix

Appendix 1: Ethical Approval Outcome

28 June 2022

Dear Vasileios Georgiou,

College of Social Sciences Research Ethics Committee

Project Title: Management Control for Risk Management in the Public Sector: A Levers of Control Perspective.

Application No: 400210096

The College Research Ethics Committee has reviewed your application and has agreed that there is no objection on ethical grounds to the proposed study. It is happy therefore to approve the project, subject to the following conditions:

- Start date of ethical approval: 28/06/2022
- Project end date: 01/10/2023
- Any outstanding permissions needed from third parties in order to recruit research participants or to access facilities or venues for research purposes must be obtained in writing and submitted to the CoSS Research Ethics Administrator before research commences: socsci-ethics@glasgow.ac.uk
- The research should be carried out only on the sites, and/or with the groups and using the methods defined in the application.
- The data should be held securely for a period of ten years after the completion of the research project, or for longer if specified by the research funder or sponsor, in accordance with the University's Code of Good Practice in Research: (https://www.gla.ac.uk/media/media_490311_en.pdf)

- Any proposed changes in the protocol should be submitted for reassessment as an amendment to the original application. The **Request for Amendments to an Approved Application** form should be used:

  https://www.gla.ac.uk/colleges/socialsciences/students/ethics/forms/staffandpostgraduateresearchstudents/

Yours sincerely,

Dr Susan A. Batchelor

College Ethics Lead

Appendix 2: Interview and Focus Group Questions (semi-structured interviews)

1. What is your position within the organisation, and how are you associated with the risk management team formed?
2. Can you describe risks in your organisations and your area of responsibility? What are these risks and how can they occur?
3. What about uncertainty? Do you know the term and how do you manage this within your projects?
4. Can you describe the risk management process at your organisation? What procedures do you have for managing known and emergent risks?
5. Can you give me any examples of how you recently utilised these procedures? Can you describe any specific situation?
6. What about the risk management meetings and the Action Plan? How does this work and how these are connected? Can you tell me about the MCS? What does it involve? How do you use it in the organisation?
7. How do you use the MCS for managing risk at your organisation? Can you give me an example, recent or not?
8. How about the IIS system? What is it and how do you use it? How does this IIS work for managing risk? Can you give me an example?
9. (Questions 6 till 8 were asked again for all tools identified).
10. What about the organisations that materialise your projects? How do you work with them? How do you work with them to manage risks?
11. Can you describe how you communicate risks with these people? What do you do to communicate risks? Can you give me an example of a recent project?
12. What do you do to communicate risks that have not been identified from the beginning of the process? Can you give me an example from a recent project?
13. Do you want to add something to the above? Anything you feel we did not discuss about risks, uncertainty, or their management, or the way you do things with the people materialising your projects?

Appendix 3: Consent forms

Consent Form (interviews)

Title of Project: "Management Control for Risk Management in the Public Sector: A Levers of Control Perspective"

Name of Researcher: Vasileios Georgiou, University of Glasgow

Name of Supervisors: Georgios Kominis and Alvise Favotto, University of Glasgow

Please tick as appropriate

Yes ☐ No ☐ I confirm that I have read and understood the Participant Information Sheet (or Plain Language Statement) for the above study and have had the opportunity to ask questions.

Yes ☐ No ☐ I understand that my participation is voluntary and that I am free to withdraw, without giving any reason and at any time during the interview, and data that I have provided will be deleted.

Yes ☐ No ☐ I consent to observations being audio-recorded

Yes ☐ No ☐ I acknowledge that copies of transcripts will be returned to participants for verification.

Yes ☐ No ☐ I acknowledge that participants will not be referred to with identifiers (that includes the organisation too), but with a pseudonym to maximise anonymity.

Note: Anonymity and confidentiality cannot be fully guaranteed, for example, due to practical reasons, and legal and/or regulatory considerations and mosaic identification. However, mechanisms have been put in place to ensure anonymity and confidentiality to the best extent practicable and with the best ability of the researcher.

I agree that:

Yes ☐ No ☐ All personal data of participants (and the organisation) likely to identify individuals will be kept and treated as per the Participant Information Sheet.

Yes ☐ No ☐ Transcripts, recordings, and company documents will be treated as confidential as possible and kept in secure storage at all times for the whole duration of the project.

Yes ☐ No ☐ Transcripts, recordings, and company documents will be kept for 10 years as per the University of Glasgow policy.

Yes ☐ No ☐ Transcripts, recordings, and company documents material may be used in future publications, both print and online.

Yes ☐ No ☐ I have understood that I can request my research data, after these have been collected, to be deleted and for myself to be removed from the study, before October 31st, 2023.

Yes ☐ No ☐ I waive my copyright to any data collected as part of this project.

Yes ☐ No ☐ I acknowledge the provision of a Privacy Notice in relation to this research project.

I agree to take part in this research study ☐

I do not agree to take part in this research study ☐

Name of Participant …… Signature
……

Date ……

Name of Researcher ……Signature
……

Date ……

Consent form: focus groups

Title of Project: "Management Control for Risk Management in the Public Sector: A Levers of Control Perspective"

Name of Researcher: Vasileios Georgiou, University of Glasgow

Name of Supervisors: Georgios Kominis and Alvise Favotto, University of Glasgow

Please tick as appropriate

Yes ☐ No ☐ I confirm that I have read and understood the Participant Information Sheet (or Plain Language Statement) for the above study and have had the opportunity to ask questions.

Yes ☐ No ☐ I understand that my participation is voluntary and that I am free to withdraw and at any time during the focus group, without giving any reason, and data that I have provided will be deleted.

Yes ☐ No ☐ I consent to observations being audio-recorded

Yes ☐ No ☐ I acknowledge that copies of transcripts will be returned to participants for verification.

Yes ☐ No ☐ I acknowledge that participants will not be referred to with identifiers (that includes the organisation too), but with a pseudonym to maximise anonymity.

Note: Anonymity and confidentiality cannot be fully guaranteed, for example, due to practical reasons, and legal and/or regulatory considerations and mosaic identification. However, mechanisms have been put in place to ensure anonymity and confidentiality to the best extent practicable and with the best ability of the researcher.

I agree that:

Yes ☐ No ☐ All personal data of participants (and the organisation) likely to identify individuals will be kept and treated as per the Participant Information Sheet.

Yes ☐ No ☐ Transcripts, recordings, and company documents will be treated as confidential as practicable and kept in secure storage at all times for the whole duration of the project.

Yes ☐ No ☐ Transcripts, recordings, and company documents will be kept for 10 years as per the University of Glasgow policy.

Yes ☐ No ☐ Transcripts, recordings, and company documents material may be used in future publications, both print and online.

Yes ☐ No ☐ I have understood that I can request my research data, after these have been collected, to be deleted and for myself to be removed from the study, before October 31st, 2023.

Yes ☐ No ☐ I waive my copyright to any data collected as part of this project.

Yes ☐ No ☐ I acknowledge the provision of a Privacy Notice in relation to this research project.

I agree to take part in this research study ☐

I do not agree to take part in this research study ☐

Name of Participant …… Signature ……

Date ……

Name of Researcher ……Signature ……

Date ……

Consent form: observations

Title of Project: "Management Control for Risk Management in the Public Sector: A Levers of Control Perspective"

Name of Researcher: Vasileios Georgiou, University of Glasgow

Name of Supervisors: Georgios Kominis and Alvise Favotto, University of Glasgow

Please tick as appropriate

Yes ☐ No ☐ I confirm that I have read and understood the Participant Information Sheet (or Plain Language Statement) for the above study and have had the opportunity to ask questions.

Yes ☐ No ☐ I understand that my participation is voluntary and that I am free to withdraw, without giving any reason and at any time during the observation, and data that I have provided will be deleted.

Yes ☐ No ☐ I consent to observations being audio-recorded

Yes ☐ No ☐ I acknowledge that copies of transcripts will be returned to participants for verification.

Yes ☐ No ☐ I acknowledge that participants (that includes the organisation too) will be referred to using pseudonyms to maximise anonymity.

Note: Anonymity and confidentiality cannot be fully guaranteed, for example, due to practical reasons, and legal and/or regulatory considerations and mosaic identification.

However, mechanisms have been put in place to ensure anonymity and confidentiality to the best extent practicable and with the best ability of the researcher.

I agree that:

Yes ☐ No ☐ All personal data of participants (and the organisation) likely to identify individuals will be kept and treated as per the Participant Information Sheet.

Yes ☐ No ☐ Transcripts, recordings, and company documents will be treated as confidential as possible and kept in secure storage at all times for the whole duration of the project.

Yes ☐ No ☐ Transcripts, recordings, and company documents will be kept for 10 years as per the University of Glasgow policy.

Yes ☐ No ☐ Transcripts, recordings, and company documents material may be used in future publications, both print and online.

Yes ☐ No ☐ I have understood that I can request my research data, after these have been collected, to be deleted and for myself to be removed from the study, before October 31st, 2023.

Yes ☐ No ☐ I waive my copyright to any data collected as part of this project.

Yes ☐ No ☐ I acknowledge the provision of a Privacy Notice in relation to this research project.

I agree to take part in this research study ☐

I do not agree to take part in this research study ☐

Name of Participant …… Signature
……

Date ……

Name of Researcher ……Signature
……

Date ……

Appendix 4: Participant Information Sheet

Participant Information Sheet (interviews)

"Management Control for Risk Management in the Public Sector: A Levers of Control perspective"

Researcher: Vasileios Georgiou, University of Glasgow.

Supervisors: Georgios Kominis and Alvise Favotto, University of Glasgow.

You are being invited to take part in a research study. Before you decide to take part, it is important for you to understand why the research is being done and what it will involve. Please read the following information carefully and discuss it with others if you wish. Ask the researcher/s if there is anything that is not clear or if you would like more information. Take some time to decide whether or not you wish to take part.

Thank you for reading this.

Study details:

The purpose of this study is to explore the use of controls in managing risk in the public sector. More importantly, the study is willing to explore risk controls for risk and uncertainty in such a context, how these fit with other systems in your management control framework in your organisation and how all the above apply to your projects.

For that reason, you are invited to participate in a 1-hour interview (approximately), at your convenience and at a time, date or place agreed between yourself and the researcher. It is worth noting that your participation is completely voluntary, and you will only be asked to provide information about the risk management processes in your organisation, and nothing else beyond that. In that interview, the researcher will ask you a set of semi-structured questions relating to the purpose of the study above. You will also be asked for the interview to be recorded, however, you can opt-out of this option should you feel uncomfortable (see next paragraph for additional withdrawal options).

The interview process will produce interview data in the form of recordings and transcripts. These data and related details will be anonymized to the extent possible and to the best of the ability of the researcher. All practicable efforts will be done to protect the anonymity of the participants, although it needs to be understood that 100% anonymity and confidentiality cannot be guaranteed. These data will be securely and confidentially kept by the researcher in a password-protected online drive provided by the University of Glasgow. Personal data and contact details will be required to arrange the interviews, however they will be kept in a separate password-protected spreadsheet and if they are in the transcripts, they will be deleted when analysing the data. Should you be required to be mentioned in this research when disseminating results, you will be referred to by a pseudonym i.e. “Manager 1”, or “Risk Officer”. However, if you have a fairly definite position, you might be indirectly identified and that is something you need to be aware of, despite the mitigants in place. After the interviews, you will be able to view and comment on the transcripts of this research. This will be done to confirm the data and, should you require, request the removal/non-use of any material that you see unfit. You will also be able to withdraw from this process, and effectively request deletion of your transcript and relevant research data, by October 31st, 2023. After that, it will be impossible to withdraw, as data analysis will commence. Following this, once these transcripts

or notes are used to produce results, they will be kept for 10 years as per University policy, in a secure place. Your personal details' spreadsheet, however, will be destroyed (at the end of the study, when my degree is awarded, that is the 1st of October 2024).

Note: More generally, and subject to the foregoing, confidentiality will be respected throughout the process subject to applicable legal constraints and professional guidelines.

Furthermore, the results of this study will be sent to the organisation (publicly available email) through a downloadable link for the organisation to send the results to you should you require. The organisation might also be presented the results of this study, however, this is something that can be arranged later on, before the end of the project in October 2024, and the organisation can contact you to attend if required (that means none of personal data will be required for this process). Please also be aware that the researcher is intending to publish the results of this study in the future. Finally, please note that this project has been considered and approved by the College Research Ethics Committee.

To pursue any complaint about the conduct of the research: contact the College of Social Sciences Ethics Officer, Dr Susan Batchelor, email: Susan.Batchelor@glasgow.ac.uk

Thank you for your time in participating in this study.

End of Participant Information Sheet

Participant Information Sheets (focus groups)

"Management Control for Risk Management in the Public Sector: A Levers of Control perspective"

Researcher: Vasileios Georgiou, University of Glasgow.

Supervisors: Georgios Kominis and Alvise Favotto, University of Glasgow.

You are being invited to take part in a research study. Before you decide to take part, it is important for you to understand why the research is being done and what it will involve. Please read the following information carefully and discuss it with others if you wish. Ask the researcher/s if there is anything that is not clear or if you would like more information. Take some time to decide whether or not you wish to take part.

Thank you for reading this.

Study details:

The purpose of this study is to explore the use of controls in managing risk in the public sector. More importantly, the study is willing to explore risk controls for risk and uncertainty in such a context, how these fit with other systems in your management control framework in your organisation and how all the above apply to your projects.

For that reason, you are invited to participate in a 1-hour focus group session (approximately), at your convenience and at a time, date or place agreed between yourselves and the researcher. It is worth noting that your participation is completely voluntary, and you will only be asked to provide information about the risk management processes in your organisation, and nothing else beyond that. In that focus group, the researcher will ask you a set of semi-structured questions relating to the purpose of the study above and you will be given the chance to discuss them with the rest of the participants present at this meeting. You will also be asked for the focus group session to be recorded, however, you can opt-out of this option should you feel uncomfortable. Moreover, to protect your anonymity, to the most practicable extent, the focus groups will need to have some discussion rules. These will be to not identify your colleagues in the focus group with their names or any other possible personal information, do not provide any personal details about anyone in the company and refrain from identifying yourselves when discussing. Furthermore, if it is necessary for a participant's role to be identified, although their name will not be disclosed, their role might make it possible to identify them. If that is the case

with you, please discuss it with the researcher to ensure you consent to that. Should you feel this is an issue, please refer to the next paragraph to see withdrawal options. Thank you for understanding. Subsequently, you should be aware that despite these measures, complete anonymity and confidentiality cannot be guaranteed. Especially for this focus group, you need to know that all efforts will be made to keep anonymity/confidentiality to the most possible extent, but given the nature of the focus group, there might be a potential breach of confidentiality, hence the measure above. Anything you require on this matter, please feel free to discuss it with the researcher any time prior to the focus group.

The focus group process will produce data in the form of recordings, notes and, eventually transcripts. These data and related details will be anonymized to the extent possible and to the best of the ability of the researcher. All possible efforts will be done to protect the anonymity of the participants, although it needs to be understood that 100% anonymity and confidentiality cannot be guaranteed. These data will be securely confidentially kept by the researcher in a password-protected online drive provided by the University of Glasgow. Personal data and contact details will be required to arrange the interviews, however they will be kept in a separate password-protected spreadsheet and if they are in the transcripts, they will be deleted when analysing the data. Should you be required to be mentioned in this research when disseminating results, you will be referred to by a pseudonym i.e. “Manager 1”, or “Risk Officer”. However, if you have a fairly definite position, you might be indirectly identified and that is something you need to be aware of, despite the mitigants in place After the interviews, you will be able to view and comment on the transcripts of this research. This will be done to confirm the data and, should you require, request the removal/non-use of any material that you see unfit. You will also be able to withdraw from this process, before October 31st, 2023. Due to the nature of this process, it would be impossible to do so once it has been completed. Following this, once these transcripts or notes are used to produce results, they will be kept for 10 years as per University policy, in a secure place. Your personal details’ spreadsheet, however, will be destroyed (at the end of the study, when my degree is awarded, that is the 1st of October 2024).

Note: More generally, and subject to the foregoing, confidentiality will be respected throughout the process subject to applicable legal constraints and professional guidelines.

Furthermore, the results of this study will be sent to the organisation (publicly available email) through a downloadable link for the organisation to send the results to you should you require. The organisation might also be presented the results of this study, however, this is something that can be arranged later on, before the end of the project in October 2024, and the organisation can contact you to attend if required (that means none of personal data will be required for this process). Please also be aware that the researcher is intending to publish the results of this study in the future. Finally, please note that this project has been considered and approved by the College Research Ethics Committee.

To pursue any complaint about the conduct of the research: contact the College of Social Sciences Ethics Officer, Dr Susan Batchelor, email: Susan.Batchelor@glasgow.ac.uk

Thank you for your time in participating in this study.

_____End of Participant Information Sheet_____

Participant Information Sheet (observations)

"Management Control for Risk Management in the Public Sector: A Levers of Control perspective"

Researcher: Vasileios Georgiou, University of Glasgow.

Supervisors: Georgios Kominis and Alvise Favotto, University of Glasgow

You are being invited to take part in a research study. Before you decide to take part, it is important for you to understand why the research is being done and what it will involve. Please read the following information carefully and discuss it with others if you wish. Ask the researcher/s if there is anything that is not clear or if you would like more information. Take some time to decide whether or not you wish to take part.

Thank you for reading this.

Study details:

The purpose of this study is to explore the use of controls in managing risk in the public sector. More importantly, the study is willing to explore risk controls for risk and uncertainty in such a context, how these fit with other systems in your management control framework in your organisation and how all the above apply to your projects.

For that reason, the researcher of this study, would like to be an external observer to this particular risk management meeting/process/project meeting (delete as appropriate), for the duration of it, at your convenience and at a time, date, or place agreed between the participants of these processes and the researcher. It is worth noting that your participation is completely voluntary, and you will only be observed to collect information on the risk management processes in your organisation, and nothing else beyond that. In this observation, the researcher will take notes relating to the purpose of the study above. You will also be asked for the observation to be recorded, however, you can opt-out of this option should you feel uncomfortable.

The observation process will produce data in the form of recordings or notes. These data and related details will be anonymized to the extent possible and to the best of the ability of the researcher. All practicable efforts will be done to protect the anonymity of the participants, although it needs to be understood that 100% anonymity and confidentiality cannot be guaranteed. These data will be confidentially kept by the researcher in a password-protected online drive provided by the University of Glasgow. Personal data and contact details will be required to arrange the observations, however they will be kept in a separate password-protected spreadsheet and if they are in the transcripts or notes, they will be deleted when

analysing the data. Should you be required to be mentioned in this research when disseminating results, you will be referred to by a pseudonym i.e. “Manager 1”, or “Risk Officer”. However, if you have a fairly definite position, you might be indirectly identified and that is something you need to be aware of, despite the mitigants in place After the observation, you will be able to view and comment on the transcripts of this research. This will be done to confirm the data and, should you require, request the removal/non-use of any material that you see unfit. You will also be able to withdraw from this process, and effectively request deletion of research data by October 31st, 2023. After that, it will be impossible to withdraw, as data analysis will commence. Following this, once these transcripts or notes are used to produce results, they will be kept for 10 years as per University policy, in a secure place. Your personal details’ spreadsheet, however, will be destroyed (at the end of the study, when my degree is awarded, that is the 1st of October 2024).

Note: More generally, and subject to the foregoing, confidentiality will be respected throughout the process subject to applicable legal constraints and professional guidelines.

Furthermore, the results of this study will be sent to the organisation (publicly available email) through a downloadable link for the organisation to send the results to you should you require. The organisation might also be presented the results of this study, however, this is something that can be arranged later on, before the end of the project in October 2024, and the organisation can contact you to attend if required (that means none of personal data will be required for this process). Please also be aware that the researcher is intending to publish the results of this study in the future. Finally, please note that this project has been considered and approved by the College Research Ethics Committee.

To pursue any complaint about the conduct of the research: contact the College of Social Sciences Ethics Officer, Dr Susan Batchelor, email: Susan.Batchelor@glasgow.ac.uk

Thank you for your time in participating in this study.

End of Participant Information Sheet

Appendix 5: Participant Information table-interviews

Participant ID	Position	Location	Duration
P1	CRO	Online via Zoom	1 hour
P2	QAO	Online via Zoom	1 hour
P3	Operator- unit Beta (transportation)	Online via Zoom	1 hour 30 minutes
P4	HR rep – Unit Gamma	Online via Zoom	51 minutes
P5	Operator- unit Beta (transportation)	Online via Zoom	1 hour
P6	Operator- unit Beta (transportation)	Online via Zoom	1 hour
P7	Operator- unit Beta (transportation)	Online via Zoom	53 minutes
Participant ID	**Position**	**Location**	**Duration**

P8	Unit A rep – Integration	Online via Zoom	30 minutes
P9	Unit A rep – Integration	Online via Zoom	30 minutes
P10	Operator – Unit Beta (environment)	Online via Zoom	42 minutes
P11	Operator- unit Beta (transportation)	Online via Zoom	50 minutes
P12	Operator – Unit Beta (environment)	Online via Zoom	56 minutes
P13	Director	Online via Zoom	30 minutes
P16	Quality team representative - operations and materialisation – road construction beneficiary	Online via Zoom	42 minutes
Participant ID	**Position**	**Location**	**Duration**

P17	Director of project and project monitoring – road construction beneficiary	Online via Zoom	42 minutes
P20	Beneficiary director – Road construction beneficiary in Crete	Online via Zoom	1 hour and 10 minutes
P21	Regulatory director	Online via Zoom	44 minutes

Appendix 6: Participant information table-focus groups

Participant IDs	Position	Location	Duration
P1 and P2, initial gatekeeper focus group	CRO and QAO	Online via Zoom	1 hour
P15 and P15	Fraud risk management team representatives	Online via Zoom	50 minutes
P18 and P19	Subway construction beneficiary representatives, risk team and operations	Online via Zoom	34 minutes
P1 – P12	Various participants from risk management team	Online via Zoom	50 minutes
P1 and P2, final gatekeeper focus group	CRO and QAO	Online via Zoom	41 minutes