UNIVERSITY OF LJUBLJANA
SCHOOL OF ECONOMICS AND BUSINESS

EDONA HAXHIU

THE IMPACT OF MANAGEMENT CONTROL ON MANAGING OPERATIONAL RISK IN BANKS

DOCTORAL DISSERTATION

Ljubljana, 2026

AUTHORSHIP STATEMENT

The undersigned Edona Haxhiu a student at the University of Ljubljana, School of Economics and Business, (hereafter: SEB LU), author of this written final work of studies with the title, THE IMPACT OF MANAGEMENT CONTROL ON MANAGING OPERATIONAL RISK IN BANKS, prepared under supervision of Associate Professor MOJCA MARC.

D E C L A R E

1. this doctoral dissertation to be based on the results of my own research;
2. the printed form of this doctoral dissertation to be identical to its electronic form;
3. the text of this doctoral dissertation to be language-edited and technically in adherence with the SEB LU's Technical Guidelines for Written Works, which means that I cited and / or quoted works and opinions of other authors in this written final work of studies in accordance with the SEB LU's Technical Guidelines for Written Works;
4. to be aware of the fact that plagiarism (in written or graphical form) is a criminal offence and can be prosecuted in accordance with the Criminal Code of the Republic of Slovenia;
5. to be aware of the consequences a proven plagiarism charge based on this doctoral dissertation could have for my status at the SEB LU in accordance with the relevant SEB LU Rules;
6. to have obtained all the necessary permits to use the data and works of other authors which are (in written or graphical form) referred to in this doctoral dissertation and to have clearly marked them;
7. to have acted in accordance with ethical principles during the preparation of this doctoral dissertation and to have, where necessary, obtained permission of the Ethics Committee;
8. my consent to use the electronic form of this doctoral dissertation for the detection of content similarity with other written works, using similarity detection software that is connected with the SEB LU Study Information System;
9. to transfer to the University of Ljubljana free of charge, non-exclusively, geographically and time-wise unlimited the right of saving this doctoral dissertation in the electronic form, the right of its reproduction, as well as the right of making this doctoral dissertation available to the public on the World Wide Web via the Repository of the University of Ljubljana;
10. my consent to publication of my personal data that are included in this doctoral dissertation and in this declaration, when this doctoral dissertation is published;
11. that I have verified the authenticity of the information derived from the records using artificial intelligence tools.

Ljubljana, July 17th, 2026 Author's signature: _____

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to my supervisor, Prof. Mojca Marc, for her exceptional mentorship, continuous guidance, and support throughout this doctoral journey. Her expertise, scholarly insight, and patience have been invaluable to the successful completion of this dissertation. I am profoundly thankful for her continued encouragement, trust, and dedication, which have not only enriched this research but have also left a lasting impact on my development as a scholar. Working under her supervision has been both a privilege and a source of inspiration.

I would also like to express my sincere appreciation to the members of my doctoral committee, Prof. Darja Peljhan, Prof. Matej Marinč, and Prof. Marika Arena, for their insightful feedback, valuable suggestions, and support throughout this process.

Thank you to the management and employees of the case bank for their openness, time, and willingness to participate in this research. Their valuable cooperation and engagement made it possible to translate theoretical concepts into meaningful empirical insights but also greatly enriched this study, for which I am deeply grateful.

My immense gratitude goes to my family for their unwavering support and understanding.

To my beloved parents, thank you for the values, motivation, and strength you instilled in me, which have shaped both my personal and academic development. This dissertation is dedicated to them with love and profound gratitude.

Finally, I extend my heartfelt appreciation to my fiancé, Bujan, for his constant support, encouragement, patience, and understanding, especially during the most demanding periods of this research.

SUMMARY

Management control systems are fundamental to directing behaviour, ensuring accountability, and safeguarding organisational performance. However, research increasingly recognises that these same systems can generate dysfunctional responses that undermine organisational objectives. In the banking sector, these unintended consequences are particularly important because failures arising from behaviour, processes, or organisational controls translate directly into operational risk. The dissertation therefore examines how management control problems emerge and how they influence operational risk in banking.

The dissertation first synthesises existing academic knowledge by conducting a systematic literature review of how result, action, personnel, and cultural controls generate dysfunctional outcomes. The analysis shows that control problems arise when controls are rigid, misaligned with employee values, poorly coordinated, or used symbolically rather than substantively. These problems manifest through behaviours such as gaming, data manipulation, workarounds, withdrawal, ethical erosion, and intentional rule violations, and are shaped by contextual influences including organisational design, leadership style, and the broader control environment.

Building on these insights, the dissertation then examines how management control problems relate to operational risk management. The literature review clarifies how management control systems, when misaligned with organisational context or behavioural dynamics, become sources of operational vulnerability. In doing so, it bridges the conceptual divide between management control and risk management literatures and offers an integrative understanding of how formal control architectures and human behaviour jointly shape operational resilience in banking.

The dissertation further provides an in-depth qualitative examination of how management control systems function in practice within the case bank and how control-related vulnerabilities translate into operational risk. Drawing on insights obtained from managers across key organisational units, the analysis identifies the mechanisms through which the bank's control system operates in everyday work. It also shows how these mechanisms correspond to established Basel II/III operational risk categories. This analysis demonstrates that operational risk does not arise solely from failures in processes or systems, but also from how controls are interpreted, enacted, and adapted within organisational settings.

In addition, a quantitative survey was conducted with bank employees to examine how management controls are associated with the frequency of people-risk behaviours. The study focuses on the relationship between tight results controls and tight action controls and three behavioural categories commonly linked to operational risk: unintentional slips and lapses, routine violations of rules, and exceptional violations of rules. This analysis offers a behavioural assessment of how formal control mechanisms relate to observable conduct in

day-to-day operations and provides evidence on how organisational context and psychological dispositions shape employees' responses to management control demands. By linking management control mechanisms to clearly defined behavioural outcomes, the study extends the understanding of how operational risk develops at the employee level and highlights the importance of aligning control practices with behavioural dynamics in banking.

The dissertation clarifies how management control systems generate behavioural vulnerabilities that influence operational risk in banking. By combining systematic literature review and synthesis, qualitative analysis, and quantitative analysis, it clarifies the mechanisms through which organisational design, culture, and behavioural responses interact to shape risk outcomes. The insights offer a foundation for designing management control systems that reduce operational risk not only through formal procedures, but through alignment with employee capability, cultural expectations, and behavioural regulation.

Keywords: management control systems, control problems, operational risk, risk culture, self-control, people-risk behaviour, banking sector

POVZETEK

Sistemi managerske kontrole predstavljajo temelj za usmerjanje vedenja, zagotavljanje odgovornosti ter zaščito organizacijske uspešnosti. Kljub temu raziskave vse pogosteje opozarjajo, da lahko ti sistemi hkrati povzročajo disfunkcionalne odzive, ki ogrožajo doseganje organizacijskih ciljev. V bančnem sektorju so takšni neželeni učinki še posebej pomembni, saj napake v vedenju in ravnanju ljudi, procesih ali organizacijskih kontrolah neposredno prehajajo v operativno tveganje. Doktorska disertacija se tako osredotoča na razumevanje nastajanja problemov managerske kontrole in njihovega vpliva na operativno tveganje v bankah.

V diseratciji je bil najprej izveden sistematični pregled literature za sintezo obstoječega akademskega znanja o tem, kako kontrola rezultatov, kontrola dejanj, kontrola osebja in kontrola kulture ustvarjajo disfunkcionalne posledice. Analiza pokaže, da se problemi kontrol pojavijo, kadar so kontrole toge, neskladne z vrednotami zaposlenih, slabo med sabo usklajene ali uporabljene simbolično namesto vsebinsko. Ti problemi se odražajo v vedenjih, kot so izigravanje sistema, manipulacija kazalnikov, iskanje obvodov in bližnjic, umik iz aktivnosti, erozija etičnih norm in namerne kršitve pravil, pri čemer imajo ključno vlogo tudi kontekstualni dejavniki, kot so organizacijska struktura, slog vodenja in širše okolje kontrole.

Na tej podlagi disertacija v nadaljevanju preučuje odnos med problemi managerske kontrole in obvladovanjem operativnega tveganja. Pregled literature pojasni, da sistemi managerske kontrole, kadar so neskladni z organizacijskim kontekstom ali vedenjsko dinamiko, postanejo vir operativne ranljivosti. S tem se premosti vrzel med literaturo s področja managerske kontrole in literaturo s področja obvladovanja tveganj ter poda celovito razumevanje učinkov skupnega delovanja formalne kontrolne arhitekture in vedenja zaposlenih na operativno odpornost v bančnem sektorju.

V nadaljevanju disertacija poda poglobljeno kvalitativno analizo delovanja sistemov managerske kontrole v izbrani banki ter pokaže, kako se ranljivosti kontrol prevajajo v operativno tveganje. Na podlagi vpogledov managerjev ključnih organizacijskih enot analiza identificira mehanizme, prek katerih sistem kontrol v banki deluje v vsakodnevnih postopkih. Pokaže tudi, kako ti mehanizmi ustrezajo uveljavljenim kategorijam operativnega tveganja po okvirih Basel II/III. Analiza potrjuje, da operativno tveganje ne izhaja zgolj iz procesnih ali sistemskih napak, temveč tudi iz interpretacije, izvajanja in prilagajanja kontrolnih mehanizmov v organizacijskem okolju.

Poleg tega je bila izvedena kvantitativna raziskava med zaposlenimi v banki, katere cilj je bil preučiti povezanost med formalnimi kontrolami in pogostostjo vedenj, ki vodijo do tveganj, povezanih z ljudmi. Raziskava se osredotoča na povezavo med strogo kontrolo rezultatov ali strogo kontrolo dejanj ter tremi kategorijami vedenja, ki so tipično povezane z operativnim tveganjem: nenamerne napake zaradi nepozornosti, rutinske kršitve pravil in

kršitve pravil v izjemnih situacijah. Analiza poda vedenjski vpogled v to, kako formalni kontrolni mehanizmi vplivajo na konkretno ravnanje zaposlenih pri vsakodnevnih nalogah ter kako organizacijski kontekst in psihološke dispozicije oblikujejo odzive zaposlenih na zahteve managerske kontrole. S tem se razširi razumevanje razvoja operativnega tveganja na ravni posameznika, in poudari pomen usklajenosti med kontrolnimi mehanizmi in vedenjsko dinamiko v bankah.

Disertacija pojasni, kako sistemi managerske kontrole generirajo vedenjske ranljivosti, ki vplivajo na operativno tveganje v bankah. S kombinacijo sistematičnega pregleda in sinteze literature, kvalitativne analize in kvantitativnega pristopa pojasni mehanizme, prek katerih organizacijska zasnova, kultura in vedenjski odzivi sooblikujejo tveganja. Pridobljeni vpogledi podajo podlago za oblikovanje sistemov managerske kontrole, ki zmanjšujejo operativno tveganje ne le preko formalnih postopkov, temveč tudi s prilagajanjem kontrolnih praks zmogljivostim zaposlenih, kulturnim pričakovanjem in vedenjski samoregulaciji.

Ključne besede: sistemi managerske kontrole, problemi kontrole, operativno tveganje, kultura tveganj, samokontrola, tvegano vedenje zaposlenih, bančni sektor.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATIONS

AC – Action Controls

LOC – Levers of Control

MCS – Management Control Systems

OOC – Object of Control

ORM – Operational Risk Management

PM – Performance Management

PMS – Performance Management Systems

RC – Result Controls

RM – Risk Management

RMS – Risk Management Systems

1 INTRODUCTION

Management Control Systems (MCS) have traditionally been described as mechanisms for shaping managerial behaviour, coordinating organisational efforts, and reinforcing accountability (Anthony, 1965; Malmi & Brown, 2008; Simons, 1995). Their primary role is to support the achievement of strategic objectives by translating them into coordinated action, clarifying roles and expectations, and supporting decision-making. Prior research shows that, when appropriately designed and used, MCS contribute to organisational alignment, communication, learning, and performance (Anthony, 1965; Malmi & Brown, 2008; Merchant & Van der Stede, 2017; Otley, 1999; Simons, 1995). Because organisations operate under varying strategic demands and uncertainty conditions, they require different configurations of control systems to guide behaviour effectively (Ferreira & Otley, 2009). This is particulary evident in complex and highly regulated environments, MCS play a central role in maintaining operational discipline and supporting managerial oversight. Against this backdrop, this dissertation examines how systems intended to deliver these benefits may, under certain conditions, also give rise to control problems and unintended behavioural responses.

In line with this concern, a growing stream of research shows that MCS may simultaneously give rise to adverse and unintended outcomes, commonly labelled as control problems. According to Merchant and Van der Stede (2017), control problems emerge when individuals face ambiguity regarding expected behaviour, experience motivational difficulties, or encounter capability limitations. They conceptualise these situations as lack of direction, motivational problems, and personal limitations. In such situations, dysfunctional responses may arise, which can include budgetary slack, gaming practices, or symbolic compliance, which can undermine the integrity and effectiveness of control systems (De Baerdemaeker & Bruggeman, 2015; Dunk, 1993; Libby & Lindsay, 2013; Merchant, 1990; Merchant & Van der Stede, 2017; Onsi, 1973; Otley, 1978; Schiff & Lewin, 1970; Van der Stede, 2000; Young, 1985).

Although early literature acknowledged these behavioural responses (e.g., Hopwood, 1972; Ridgway, 1956; Van der Stede, 2000), a structured understanding of how specific control types contribute to distinct dysfunctional patterns remained limited. More recently, the academic discourse has increasingly drawn attention to this "darker side" of control. Fiolleau et al. (2018) explicitly encourage deeper inquiry into how and why control systems induce unintended behavioural responses. Franco-Santos et al. (2012) similarly highlight that performance measurement systems may trigger both desirable and undesirable behaviours, underscoring the need for further empirical and conceptual work. Bromwich and Scapens (2016) further argue that management accounting research must build cumulative knowledge by examining behavioural side-effects of control mechanisms that have historically been overlooked or under-conceptualised.

These control problems have particular implications in banking, where the consequences of behavioural deviations materialise as operational risk exposure. The Basel Committee on Banking Supervision defines operational risk as the risk of loss resulting from inadequate or failed internal processes, people, systems, or from external events (Basel Committee, 2003, 2006, 2011). Unlike manufacturing environments, where dysfunctional control responses primarily affect productivity or cost efficiency (Van der Kolk, 2019), in banking they can lead to financial losses, regulatory breaches, customer detriment, or reputational damage (Rad, 2016; Ringgaard et al., 2025).

The choice of the banking sector for this study is motivated not only by its distinctive economic functions but also by the central organisational role that risk plays in banking activity. Unlike firms in most other industries, banks perform core financial intermediation functions that are essential for the allocation of capital in the economy. In particular, they channel funds from savers to borrowers, reduce transaction costs, and mitigate information asymmetries that would otherwise hinder efficient exchange and investment (Diamond, 1984; Bhattacharya & Thakor, 1993; Greenbaum et al., 2019). In doing so, banks do not primarily produce goods or services for final consumption; rather, they facilitate the transformation of savings into productive investment and support the financing of households and firms (Committee for the Prize in Economic Sciences in Memory of Alfred Nobel, 2022).

Beyond their role in capital allocation, a second and equally defining feature that distinguishes banks from non-financial firms is their role in liquidity provision and financial claim transformation. Banks create liquid liabilities, such as deposits, while holding relatively illiquid assets, such as loans, thereby enabling depositors to access funds on demand while providing longer-term financing to borrowers (Greenbaum et al., 2019). Berger and Boot (2024) emphasise that the value of financial intermediation lies precisely in this transformation of financial claims, which redistributes risk and generates liquidity for the broader economy. Similarly, Kashyap et al. (2002) show that deposit-taking and lending are jointly organised within banks because both activities support the provision of liquidity on demand. These functions imply that banks operate with highly leveraged balance sheets and must continuously manage uncertainty related to credit quality, liquidity needs, and market conditions.

Together, these functions imply that banks operate with highly leveraged balance sheets and must continuously manage uncertainty, making them intrinsically fragile. Because banks fund long-term, illiquid assets with short-term, withdrawable liabilities, they are exposed to maturity transformation risk. Diamond and Dybvig (1983) demonstrate that such balance-sheet structures can give rise to self-fulfilling bank runs even in the absence of underlying insolvency. The Nobel Committee's scientific background similarly highlights that liquidity transformation is inherently unstable, as deposits can be withdrawn on demand while loans cannot be liquidated without loss (Committee for the Prize in Economic Sciences in Memory of Alfred Nobel, 2022). Moreover, by performing delegated monitoring on behalf of

dispersed depositors, banks concentrate informational and credit risk within their organisational boundaries (Committee for the Prize in Economic Sciences in Memory of Alfred Nobel, 2022; Diamond, 1984). Consequently, failures in banking organisations may disrupt not only individual institutions but also credit provision, payment systems, and broader economic activity.

These characteristics explain why banking is subject to extensive prudential regulation. Because bank failures generate systemic externalities, regulatory frameworks such as the Basel Accords focus on capital adequacy, liquidity management, and risk governance to enhance financial system resilience (Greenbaum et al., 2019).Cross-country evidence further suggests that the effectiveness of regulatory and supervisory arrangements depends not only on formal oversight but also on broader institutional conditions and monitoring mechanisms (Barth et al., 2004). In recent decades, regulatory attention has increasingly extended to operational risk, recognising that failures in internal processes, systems, and human behaviour can generate substantial losses and threaten institutional stability. In this respect, operational failures in banks differ from those in many other industries, where their consequences are more likely to remain contained at the firm level.

This institutional context is particularly relevant for the present dissertation because it highlights the coexistence of two distinct but interrelated control logics within banking organisations. Management control systems are designed from a managerial perspective to align behaviour with strategic objectives and support organisational performance. Operational risk management frameworks, by contrast, reflect a prudential perspective focused on resilience, compliance, and the prevention of failures in processes, systems, and people. Although these perspectives differ in their primary objectives, they are closely interconnected in practice. When functioning effectively, management control systems can therefore support the prudential objectives of operational risk management by shaping employee behaviour, reinforcing process discipline, and creating organisational conditions that reduce the likelihood of operational failures. Weaknesses in management control such as misaligned incentives, poorly designed procedures, or ineffective monitoring may generate behavioural responses and process breakdowns that materialise as operational risk events. In banking organisations, therefore, control failures are not merely internal inefficiencies but potential sources of financial vulnerability.

This coexistence of managerial and prudential control logics is also what makes banking an analytically advantageous empirical setting for the present study. Risk in banking is not merely an external condition but a central organisational object that must be measured, monitored, and governed. Compared with many firms in other industries, banks develop extensive risk infrastructures that render risk visible and actionable within the organisation. These include formal risk policies, internal loss databases, model-based measurement systems, regulatory reporting frameworks, and dedicated risk management functions that routinely review exposures and incidents. Prudential regulation further reinforces this institutionalisation of risk by requiring banks to establish structured processes for

identifying, quantifying, and reporting operational risk (Cruz, 2002). As a result, employees are socialised into risk-aware practices, risk events are systematically documented, and behavioural expectations regarding risk-taking are explicitly articulated. This high degree of formalisation provides unusually rich empirical access to both control mechanisms and risk outcomes, making banks an analytically advantageous setting for examining how management control systems influence behaviour and how control failures translate into operational risk exposures.

Research on operational risk has predominantly focused on its quantification and capital measurement dimension, particularly after the Basel II and Basel III frameworks established structured approaches for identifying, classifying, and evaluating operational losses (Basel Committee, 2003, 2006, 2011). As a result, operational risk has often been treated as a technical category linked to indicators, loss data, and regulatory monitoring. However, emerging work highlights that operational risk does not arise solely from breakdowns in systems or procedures, but is shaped by how individuals interpret, enact, or adapt organisational controls in practice (Mikes, 2009; Power, 2007). This shift points to the need to understand behavioural and organisational drivers of operational exposure, rather than relying only on measurement-based perspectives.

In management accounting research, studies have documented that formal controls can lead to unintended behavioural outcomes when targets are rigid, when rules limit judgment, when employee values are misaligned with system demands, or when controls are layered without coordination (Bromwich & Scapens, 2016; Fiolleau et al., 2018; Franco-Santos et al., 2012; Van Camp & Braet, 2016). More recent research has argued that these dysfunctional consequences often have risk implications, particularly where behavioural distortions translate into errors, shortcuts, omission of checks, suppression of risk signals, or concealment of irregularities (Li & Evans, 2022; Müller et al., 2025).

Despite these developments, academic work linking management control systems specifically to operational risk remains limited and fragmented. While management control studies diagnose behavioural consequences (Jensen, 2003), and operational risk studies examine failures and loss events (Chapelle et al., 2004), the underlying mechanisms that connect both streams remain insufficiently integrated. In particular, empirical understanding of how specific control types relate to observable risk behaviour, and how employee responses shape operational vulnerabilities in banking organisations, remains limited.

This dissertation positions itself within this scholarly conversation by examining how management control problems emerge and how these problems relate to operational risk in banking. To address this objective, the dissertation combines systematic literature synthesis, qualitative inquiry in a real banking institution, and quantitative analysis of behavioural mechanisms. This multi-stage approach enables an integrated understanding of how formal control structures, behavioural responses, and organisational context jointly shape operational risk outcomes.

This tendency is especially pronounced in banking contexts marked by strong regulatory pressure, extensive documentation, and interdependent processes. In these settings, even small departures from required procedures, whether unintentional or deliberate, can create exposure to financial loss, regulatory consequences, or reputational harm. The functioning of management controls is therefore directly connected to the organisation's ability to manage operational risk (Ringgaard et al., 2025). When controls operate as intended, by guiding rule compliance, employee discipline, performance alignment, and information accuracy, they reinforce organisational reliability (Merchant & Van der Stede, 2017). However, when controls become burdensome, rigid, or symbolically used, they may inadvertently weaken the organisation's risk posture by stimulating avoidance, short-cutting, inconsistent execution, or concealment (Fiolleau et al., 2018; Franco-Santos et al., 2012; Li & Evans, 2022).

Building on this observation, a more specific gap concerns the absence of an integrated, mechanism-based explanation linking different types of management controls to operational risk outcomes. While existing studies provide valuable insights into the unintended behavioural consequences of controls and into operational risk frameworks in banking, they do not systematically explain how distinct control types generate specific control problems, how these problems manifest in organisational practice, and how they translate into operational vulnerabilities and risk-related behaviours. This dissertation addresses this gap by examining how result, action, personnel, and cultural controls contribute to control-related vulnerabilities and people-risk behaviour through a combination of literature synthesis, qualitative inquiry, and quantitative behavioural analysis.

Recent work has begun to address parts of this connection. For example, Ringgaard et al. (2025) show how Anti-Money Laundering practices can function as a boundary system supporting risk mitigation within a specific regulatory domain. However, their focus remains confined to one risk category and does not yet explain more broadly how different types of controls generate distinct behavioural responses and how these responses translate into wider operational risk exposures within organisational settings.

In particular, there is limited cumulative evidence on (i) which types of controls give rise to which forms of control problems, (ii) how these problems manifest within banking practice, and (iii) how these mechanisms lead to observable risk-related behaviours.

Furthermore, despite extensive attention to operational risk frameworks, there is limited empirical work examining how employees experience controls, interpret risk-related policies, or navigate tensions arising from competing performance and compliance demands. Similarly, while banking institutions invest extensively in internal audit, procedural documentation, risk reporting systems, and automated controls (Lim et al., 2017), research shows that behavioural adjustments often occur beneath formal structures, creating a gap between intended and enacted control use.

This dissertation advances existing knowledge by linking management control research with the operational risk domain and examining how control problems influence risk-related employee behaviour within a banking environment. By tracing how management control systems are designed, how they function in organisational practice, and how employees adapt to them, the dissertation provides a behavioural perspective on how operational risk emerges. The overarching aim of the dissertation is to explain how management control problems emerge and how these problems influence operational risk in banking. Drawing on Merchant and Van der Stede's classification of control systems into result, action, personnel, and cultural controls, the dissertation first examines how different control types relate to distinct patterns of control problems. It then explains how these problems become linked to operational risk within the banking context, examines how these dynamics unfold empirically within a case-study bank, and finally tests a focused behavioural pathway through quantitative analysis. This focus establishes a conceptual basis for understanding the behavioural origins of dysfunctional responses to controls and clarifies why control mechanisms may not always operate in the way organisations intend.

The dissertation is guided by three central research questions:

RQ1: How does a management control system (result control, action control, personnel control, and cultural control) relate to the type of management control problem?

RQ2: How do management control problems relate to operational risk management?

RQ3: How do management control problems affect the frequency and severity of operational risk events?

The dissertation addressed these three overarching research questions through four interrelated research stages. The first stage addressed RQ1 by synthesising evidence from prior research on the unintended consequences of result, action, personnel, and cultural controls. This stage organised prior findings into a structured mapping between control types and the behavioural responses associated with them. This then provided a conceptual framework linking specific control systems with corresponding control problems

The second stage addressed RQ2 through conceptual analysis supported by a targeted literature review. Two auxiliary questions guided this stage: (i) How do management control problems arise from the design and use of control systems in the context of operational risk management? and (ii) Through which organisational and behavioural mechanisms do these control problems shape operational risk outcomes in banking institutions? Examining prior studies through these analytical lenses enabled the literature review to clarify how control problems translate into operational exposure and to link management control design and use to operational risk in banking.

The third stage further addressed RQ2 in an empirical setting through qualitative analysis. It applied two auxiliary questions as analytical lenses: (i) How do different types of

management control systems generate control problems within a bank? and (ii) How do these control problems contribute to the emergence of operational risk within the bank? These auxiliary questions were not separate research questions but served to structure the empirical investigation in a way that directly informed RQ2. These questions structured the case study inquiry and allowed the empirical evidence to be interpreted in relation to formal risk categories used in banking.

The fourth stage addressed RQ3, which required refinement following empirical observations. During data collection, it became evident that employees' experiences did not meaningfully differentiate between levels of severity in operational consequences, making severity an unsuitable analytical criterion. Therefore, the research question was reformulated to focus on the frequency of risk-related behaviours, which aligned more closely with how operational exposures materialised in daily work. This adjustment enabled the analysis to operationalise RQ3 in a manner consistent with behavioural evidence emerging from practice and provided a measurable basis for linking management control problems to people-risk behaviour within the banking environment.

By structuring the research around these three overarching questions, the dissertation establishes a coherent analytical progression. First, it clarifies how management control problems emerge conceptually and develops a structured understanding of their behavioural origins. Second, it examines how these control problems become linked to operational risk in the banking context through a focused review of the literature. Third, it explores how these dynamics unfold in organisational practice through qualitative evidence, offering insight into how control mechanisms are interpreted, enacted, and adapted by employees. Finally, it examines how these dynamics translate into behavioural patterns that represent precursors to operational risk.

To address the research questions, the dissertation followed a sequential multimethod research design that progressed from conceptual synthesis to empirical qualitative and quantitative observation. This design ensured that the phenomenon was explored cumulatively, with each stage directly informing the next.

The first stage involved a systematic literature review of prior research, in which 95 scholarly publications were analysed to clarify how different management control systems give rise to distinct patterns of control problems. By organising findings according to control type and associated dysfunctional responses, this stage offered the conceptual basis for analysing how control problems emerge.

A second, subsequent and more targeted literature review focused on 44 additional studies linking management control problems specifically to operational risk in banking settings. This review synthesised evidence on risk governance, process breakdowns, and behavioural responses in regulated financial institutions, thereby clarifying how weaknesses in control design and use have been linked to operational risk exposure.

The third stage examined these relationships empirically through an in-depth case study of a banking institution. Data were collected through semi-structured interviews with managers across key organisational units. Using the Gioia method for data analysis, this stage explored how control demands are interpreted in practice, how organisational processes shape behavioural responses, and how control-related vulnerabilities materialise in day-to-day operations. This stage provided contextual grounding for understanding how theoretical mechanisms translate into organisational reality.

The fourth stage further extended the empirical investigation by analysing how control problems relate to observable employee behaviour. A questionnaire was developed and deployed in an online survey within the same organisational context to capture employees' perceptions of control practices and risk-related behaviours. The resulting dataset was analysed using PLS-SEM, allowing for a systematic assessment of how variations in control systems' tightness correspond to the frequency of behaviours that contribute to operational risk. This stage enabled a systematic examination of behavioural outcomes and strengthened the empirical link between management control problems and operational risk exposure.

Together, these four stages constitute an integrated research design. The literature reviews established the conceptual foundation, the qualitative case study demonstrated how control problems materialise within organisational practice, and the quantitative analysis tested how these dynamics are reflected in employee behaviour. Through these stages, the dissertation advances from theoretical formulation to empirical examination and provides a coherent explanation of how management control systems influence operational risk within banking organisations.

The dissertation contributes to the academic and practical understanding of management control systems and operational risk by combining conceptual synthesis, qualitative organisational analysis, and quantitative behavioural evidence. The contributions arise at three levels: theoretical advancement, empirical clarification, and practical application concerning risk-related behaviour in banks.

From a theoretical perspective, the dissertation advances knowledge on the dysfunctional consequences of management control systems by systematically mapping how result, action, personnel, and cultural controls relate to distinct categories of control problems. The structured synthesis demonstrates that behavioural responses are not random side effects, but arise through identifiable mechanisms, such as rigid procedural enforcement, misaligned incentives, symbolic implementation of controls, and erosion of ethical norms. This mechanism-based view moves beyond descriptive cataloguing of unintended consequences and provides a more explanatory understanding of why control systems fail under certain contextual conditions. Furthermore, by showing how management control problems become sources of operational vulnerability, the dissertation integrates two previously separate conversations: research on dysfunctional control effects and research on operational risk exposures in banks.

At the empirical level, the dissertation contributes by demonstrating how the theoretical mechanisms identified in the literature translate into observable organisational phenomena within a banking setting. The qualitative analysis revealed that structural segmentation, prescriptive procedural routines, workforce capacity constraints, incentive tensions, and cultural inconsistencies function as recurring pathways through which control systems generate exposure to operational risk. These organisational mechanisms were subsequently linked to Basel II/III operational risk categories, thereby situating the findings within an established regulatory classification. The quantitative analysis further extended this understanding by examining how these organisational conditions relate to behavioural tendencies that precede operational risk. The results provided evidence that behavioural expressions of risk are influenced by variations in tightness of controls and by organisational context that affects self-regulation and conformity to procedures.

The dissertation also provides implications for practice, especially for organisations operating in environments characterised by high regulatory expectations and extensive use of formal controls. The findings show that strengthening rules, tightening supervision, or reinforcing performance targets does not uniformly improve behavioural reliability; instead, such measures can exacerbate workload pressure or encourage discretionary workarounds. The analysis highlights that how employees interpret and internalise controls depends on their perception of fairness, capability, cultural norms, and learning expectations. For practitioners, this suggests that operational resilience develops not simply through intensifying control architecture, but through alignment between formal control design and the behavioural capacities needed to enact them consistently.

This dissertation thus contributes to academic and practical understanding of management control systems and operational risk by integrating evidence from conceptual synthesis, qualitative organisational inquiry, and behavioural analysis. Its contributions emerge across three complementary domains. Theoretically, it advances explanation of how different types of controls can give rise to behavioural vulnerabilities and how these mechanisms relate to operational exposure. Empirically, it investigates how control problems materialise within a real banking organisation and how control requirements are experienced in everyday operational work. Practically, it offers insights into mechanisms that shape people-related risk behaviour in banks, thereby informing managerial decisions regarding the design and use of control systems aimed at strengthening operational reliability.

The dissertation is organised into seven chapters, each focusing on a specific aspect of the research aim. Following the indroduction chapter, Chapter 2 presents a systematic literature review of the unintended consequences of management control systems. Chapter 3 builds on this foundation by examining how these control problems become linked to operational risk in the banking sector. Chapter 4 provides a qualitative examination of how management control systems function in practice within a banking organisation. Chapter 5 quantitatively examines a focused part of the broader framework by analysing how management control problems and tighter formal controls relate to the frequency of people-risk behaviour.

Chapter 6 discusses the overall impact of management control systems on operational risk in banking and elaborates the dissertation's theoretical and practical contributions. The final chapter concludes the dissertation by summarising the key findings, limitations, and directions for future research.

2 UNINTENDED CONSEQUENCES OF MANAGEMENT CONTROL SYSTEMS: A SYSTEMATIC REVIEW AND CONCEPTUAL FRAMEWORK

Management Control Systems (MCS) have traditionally been conceptualized as tools for aligning managerial behavior with organizational objectives, facilitating strategic coordination, and ensuring accountability (Anthony, 1965; Malmi & Brown, 2008; Simons, 1995). When appropriately designed and used, they are generally expected to enhance organizational functioning by improving communication, supporting consistency in action, and contributing to performance. While their primary aim is to support goal achievement and improve performance, an emerging body of literature demonstrates that they may also generate adverse, unintended and dysfunctional consequences, a phenomenon increasingly referred to as control problems. Control problems, as defined by Merchant and Van der Stede (2024**)**, occur when individuals within organizations experience a lack of direction, motivational problems, or personal limitations; and can manifest as e.g., budgetary slack, gaming, or other types of dysfunctional behavior. That compromises the integrity and effectiveness of MCS.

Although earlier studies acknowledged such issues (e.g., Hopwood, 1972; Van der Stede, 2000), a systematic understanding of how different types of control systems contribute to specific forms of dysfunction remains underdeveloped. This darker side of control has gained increasing scholarly attention, and recent studies have highlighted and explicitly called for integrative research that goes beyond examining control systems in isolation. Fiolleau et al. (2018) call for a deeper understanding of how and why MCS induce dysfunctional behavior. Franco-Santos et al. (2012) emphasize that performance measurement systems affect both positive and negative employee behaviors, calling for further research to explore the unintended consequences of control. Similarly, Bromwich and Scapens (2016) stress the importance of building cumulative knowledge in management accounting by addressing overlooked behavioral consequences of control systems.

Despite these calls, current research often remains fragmented. While valuable insights have emerged from sector-specific studies (e.g., Fiolleau et al., 2018; Li & Evans, 2022), the literature lacks a synthesized view that connects different control types to recurring behavioral issues they produce. Few studies have attempted to develop a consistent theoretical framework to uncover the deeper origins of control problems that can be taken into consideration in practice either when designing or using MCS (e.g., Franco-Santos & Otley, 2018; Müller et al., 2025). While prior reviews have identified and classified various unintended consequences of MCS, most focus on performance management systems (PMS)

(e.g., Franco-Santos et al., 2012; Van Camp & Braet, 2016) and none of them systematically mapped how these outcomes relate to specific control types. What also remains largely underexplored is how particular control mechanisms contribute to dysfunctional outcomes, and what underlying drivers or contextual factors shape these dynamics. Addressing this gap is essential for advancing both theoretical clarity and practical application.

To that end, we investigate how different types of MCS relate to distinct manifestations of control problems. The research question guiding our study is: *How does the type of management control system relate to the type of control problem?* To explore this question, we conduct a systematic literature review of 95 peer-reviewed studies focused on the dysfunctional consequences of MCS, drawing on research from management, accounting, and organizational behavior disciplines. Unlike earlier works such as Müller et al. (2025), which use Simons' (1995) Levers of Control framework, or Franco-Santos and Otley (2018), which use a systems theory perspective, our review adopts the Object-of-Control (OOC) framework by Merchant and Van der Stede (2024). The OOC framework categorizes controls into four types: result controls, action controls, personnel controls, and cultural controls. Each control type targets a distinct behavioral object, making this framework particularly suited for analyzing the behavioral implications of control systems. Its widespread acceptance and frequent citation in the MCS literature (e.g., Kunz & Heitz, 2021) further enhance the generalizability and relevance of our findings to other contexts.

Through this theoretically grounded lens, we map various control problems to specific types of controls. The first contribution of our research is an evidence-based categorization of which control problems are most commonly associated with particular types of control systems. This contributes to the literature by offering direct mappings that complement findings from similarly rigorous reviews, such as Franco-Santos et al. (2012), Franco-Santos and Otley (2018), and Müller et al. (2025), which do not distinguish between control types with such granularity.

Second, by focusing on identifying common root causes rather than merely listing consequences, we go beyond previous taxonomies (e.g., Van Camp & Braet, 2016). Our study highlights the systemic drivers (i.e., common origins) of control failures, including contextual variables such as organizational culture, design choices, and employee psychology, which are critical in shaping how control problems manifest. This analytical shift from consequences to cause sharpens both theoretical and practical understanding of why MCS fail.

Third, our study introduces a novel conceptual and diagnostic framework that explains not only *what* dysfunctions occur, but also *why* they occur and *how* they may be mitigated. The framework incorporates causal logic and offers practical insights for both researchers and practitioners. It advances the literature by offering a design-oriented logic that can inform the development (or reform) of MCS in ways that anticipate and reduce dysfunctional outcomes. Similar to Müller et al. (2025), who identify intermediate variables such as

psychological or demographic factors, we integrate systemic origins and contextual drivers into a unified model. In doing so, our research responds to the call by Van Camp and Braet (2016) for more diagnostic granularity in understanding control failure patterns. It provides actionable insights by identifying specific configurations of control that tend to fail and mapping their typical triggers.

Overall, our study complements existing literature by not only cataloguing the unintended consequences linked to each control type but also by identifying their common underlying drivers and proposing a comprehensive framework for understating MCS failures. As such, it makes a dual contribution: it advances academic research on MCS and offers a diagnostic tool for practitioners tasked with designing or revising control systems. Ultimately, the study contributes to a more critical and behaviourally informed understanding of management control, addressing long-standing calls for research into the darker side of control and guiding future research into effective and ethical application of MCS.

The chapter begins with a theoretical overview that traces how literature has come to recognize control problems, reviews prior studies on the negative consequences of MCS, and outlines the conceptual frameworks used to study them, including the one adopted in this review. This is followed by an explanation of the systematic methodology used in the literature review. The findings are then presented and organized into six themes that emerged from the data. Drawing on these findings, the chapter introduces a conceptual framework and discusses key insights, including implications for practice. The conclusion summarizes the key contributions and outlines the study's limitations.

2.1 Literature review

Management control systems (MCS) have long been recognized as essential tools for aligning employee behaviour with organizational goals (Anthony, 1965). Early views, grounded in formal, accounting-based tools such as budgets and incentives, were shaped by cybernetic thinking (Hofstede, 1978) but later critiqued for overlooking informal and behavioural dynamics (Berry et al., 2009; Otley et al., 1995). Over time, MCS research expanded to include both formal and informal controls (Langfield-Smith, 1997), incorporating cultural, psychological, and strategic dimensions. A critical shift occurred as scholars began to explore not just how control systems function, but how they may fail. Ridgway (1956) and Hopwood (1972) were early to warn that control mechanisms could produce unintended and dysfunctional behaviours. Subsequent studies identified a range of control problems, including gaming, slack, lying, symbolic compliance, and ethical disengagement (e.g., Rosanas & Velilla, 2005; Schweitzer et al., 2002; Van der Stede, 2000), noting that these often arise not from the absence of control but from poorly designed, misapplied, or overly rigid control systems.

Previous literature has made notable progress in examining the consequences of MCS. While many studies focus on broader systems (e.g., PMS/PM) rather than MCS alone, they include MCS within their scope. For instance, Franco-Santos et al. (2012) conducted a literature review of 76 empirical studies (published between 1992 – 2011) and proposed a multidimensional framework categorizing both functional and dysfunctional outcomes. Although they acknowledge dysfunctional behaviour, their primary focus is on positive effects, and they call for further exploration of unintended consequences. Van Camp and Braet (2016) analysed over 250 papers to develop a taxonomy of 36 PMS failures at three levels: the metric, framework and management level. As an important contribution they highlighted systemic risks emanating from fragmented implementation and implementation flaws. Bromwich and Scapens (2016) further emphasized the need for cumulative knowledge about control problems in management accounting and advocated for integrative syntheses to build conceptual clarity. Across these studies, common manifestations of dysfunction include gaming, tunnel vision, morale loss, data manipulation, control system misuse, and behavioural displacement. More recently, Müller et al. (2025) sought to move beyond categorization by examining drivers of dysfunctional behaviour linked to MCS. Using the LOC framework for a systematic literature review (on 82 articles, published between 2014 - 2024) and ProKnow-C method, they find that using isolated control levers increases dysfunction, whereas integrated use can reduce it.

Other prior studies have taken more sector-specific research focus. Li and Evans (2022), for example, reviewed 41 papers and conducted 147 qualitative interviews to explore unintended consequences of PMS in healthcare, and provided a typology of 48 unintended consequences, highlighting the mutually reinforcing dysfunctions. Fiolleau et al. (2018) carried out a focused literature review of dysfunctional behaviours in auditing (44 papers, published between 2003 – 2016). Drawing on the fraud triangle; opportunity, motivation, and rationalization, they demonstrated that misaligned signals or manipulative use of MCS contribute to unethical behaviour. While these studies contribute valuable sector-specific insights, they do not systematically link the dysfunctions to specific MCS types, leaving a gap in understanding how control problems systematically emerge from different control mechanisms.

Most existing reviews emphasize categorization over causal linkage (e.g., Franco-Santos et al., 2012; Li & Evans, 2022; Van Camp & Braet, 2016), their analysis remains largely thematic and does not connect specific control types to dysfunctions. Franco-Santos and Otley (2018) advance this by theorizing systemic mechanisms explaining how unintended consequences emerge over time (e.g., decoupling, overload), but the focus is theoretical and less anchored in operational control structures. Similarly, Müller et al. (2025) employ Simons' LOC framework to examine dysfunctional behaviours and provide valuable insight into the synergistic use of controls. However, they do not systematically associate types of control systems with the particular manifestations of control problems observed in practice.

Our study directly addresses this gap by using the OOC framework (Merchant & Van der Stede, 2024), which categorizes MCS based on the object being controlled: actions, results, personnel, or culture. Specifically, action controls aim to ensure that employees perform designated behaviours; result controls focus on achieving defined goals; personnel controls target hiring and development of capable individuals; and cultural controls foster shared norms and beliefs (Merchant & Otley, 2006; Van der Kolk, 2019). This functional classification is particularly well-suited for behavioural analysis, as it enables analysis of dysfunctional behaviours at the level where they most often manifest, i.e. in the design and implementation of specific control types. The OOC framework allows us to move beyond broad conceptual typologies and provides structure to evidence-based mapping of how distinct control types relate to recurrent dysfunctional behaviours. It integrates earlier behavioural insights into a unified structure, offering theoretical clarity and practical diagnostic utility (Merchant & Van der Stede, 2024). It also provides explicit guidance on the advantages, limitations, and potential costs of each control mechanism, enhancing its relevance for both researchers and practitioners.

While alternative possible frameworks, such as Simons' (1995) LOC, Malmi and Brown's (2008) MCS package model, and Ferreira and Otley's (2009) extended PMS design and use model offer valuable insights into system interdependencies, trade-offs, and managerial tensions, they are less well-suited for isolating how specific intended control targets are systematically associated with particular unintended outcomes. In contrast, the OOC framework retains a focus on the behavioural object of control, offering greater behavioural granularity that supports a more precise diagnostic mapping. While our analytical lens is intentionally narrow, this specificity complements the broader systemic or integrative approaches of prior research. Moreover, the OOC framework has been successfully applied across diverse settings, including multinationals, nonprofits, and high-uncertainty environments (Kunz & Heitz, 2021; Merchant & Van der Stede, 2024; Van der Kolk, 2019) which supports the relevance and transferability of our findings to other contexts.

2.2 Method

We employ a systematic literature review (SLR) approach, following Tranfield et al. (2003) and refinements by Massaro et al. (2016), Snyder (2019), and Kuckertz and Block (2021). The choice of a systematic literature review (SLR) approach was guided by the specific objectives of Chapter 2. The aim of this chapter was not to provide a broad descriptive mapping of the literature, but to identify and synthesise existing research on management control systems and the control problems associated with them in a structured and transparent manner. In particular, the review seeks to consolidate fragmented insights on how different types of controls relate to specific behavioural and organisational dysfunctions.

In this context, the SLR approach is considered appropriate in the methodological literature because it provides a clear, transparent, and replicable process for selecting, evaluating, and synthesising relevant studies, while reducing the risk of ad hoc or selective interpretation (Rojon et al., 2021; Snyder, 2019). This is especially important given the conceptual diversity of the management control literature, where studies vary in terms of theoretical framing, empirical context, and terminology used to describe control problems.

With regard to alternative approaches, such as bibliometric reviews, these are highly valuable for mapping research trends, citation networks, and the overall structure of a field. However, as noted by Mukherjee et al. (2022), they are less suited for in-depth interpretation of underlying mechanisms and for theory-driven synthesis. Given that the focus of this chapter is on understanding how different management control systems give rise to specific control problems, a systematic and conceptually guided review was considered more appropriate for addressing the research objective.

To ensure transparency and replicability, we co-developed review protocol, operationalized search terms, and used iterative coder agreement. Positioned as a theory- and phenomenon-focused SLR (Block et al., 2025), this review synthesizes fragmented evidence on unintended behavioural consequences of MCS using the OOC framework.

We defined the research problem around how MCS types (result, action, personnel, cultural) relate to distinct control problems (e.g., gaming, slack, dishonesty, resistance). The OOC framework was used to bound and code the literature, and leading MCS textbooks (Anthony & Govindarajan, 2007; Merchant & Van der Stede, 2024; Simons, 2000) informed both primary keyword development and coding structure. A review protocol was established (Massaro et al., 2016) detailing the research question, search strategy, databases, eligibility criteria, and coding framework. This protocol was co-developed and agreed by both researchers to reduce subjectivity and enable replication.

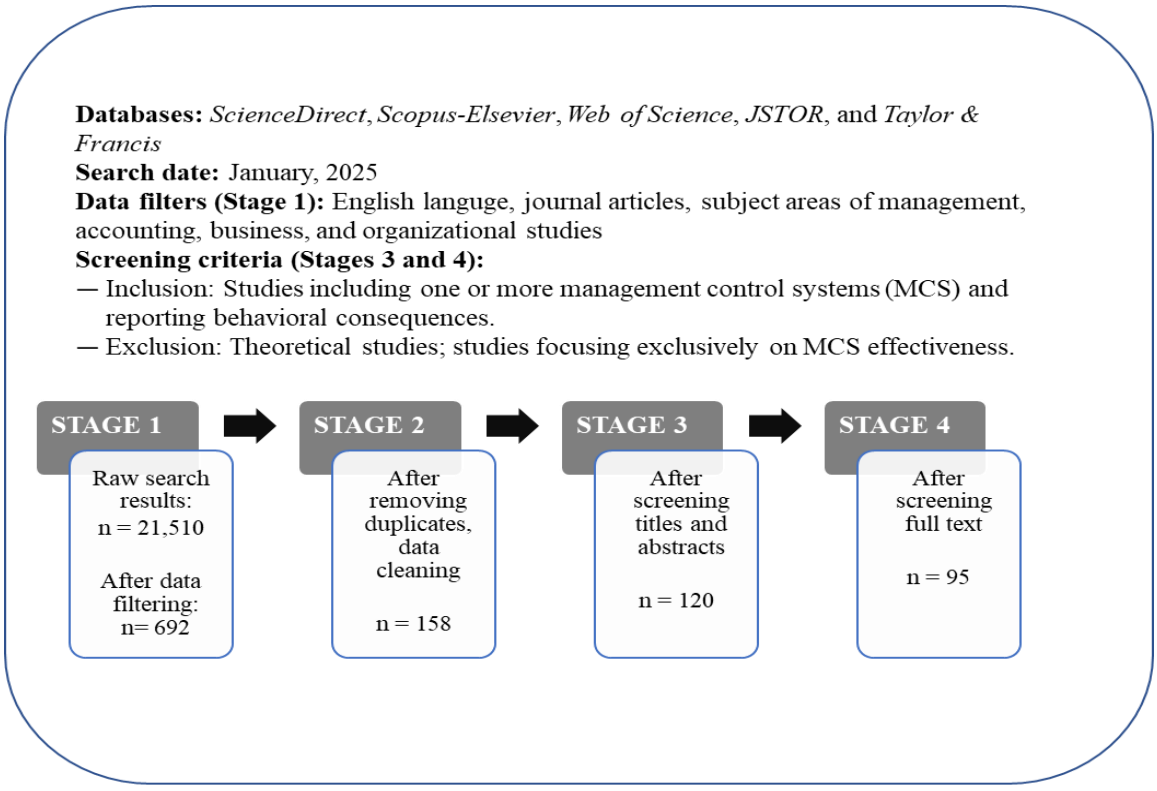
To operationalize the research question for the systematic search, we translated its conceptual components into specific, database-friendly search terms. While the initial search included general terms such as “management control systems” and “control problems,” it became evident that the key challenge was the inconsistent terminology used in the literature to describe both types of management control systems (MCS) and their associated behavioural consequences. To address this, keywords were iteratively refined to map each control type to a set of conceptually equivalent keywords commonly used in empirical and theoretical studies. Specifically, "performance measurement systems" was used to represent result controls, while "organizational rules" and "behavioural controls" reflected action controls. Personnel controls were captured via terms such as "staff control" and "human resource management," and cultural controls were operationalized using "organizational culture." For the behavioural side of the question, we included terms such as “dysfunctional behaviour,” “gaming behaviour”, “data manipulation”. Boolean operators and wildcard functions were used where supported by the database. This translation followed the CIMO

logic (Context, Intervention, Mechanism, Outcome) as recommended by Denyer and Tranfield (2009) and further elaborated by Kuckertz and Block (2021).

Final searches were conducted in January 2025 using five major databases: ScienceDirect, Scopus-Elsevier, Web of Science, JSTOR, and Taylor & Francis. These databases were selected due to their extensive coverage of management, accounting, and behavioural research. Appendix 2 presents search strings and results for each database.

After refining the search results by applying filters (peer-reviewed journals, English language, and subject areas of management, accounting, business, and organizational studies) and removing duplicates, we screened the records based on predefined inclusion and exclusion criteria as illustrated in Figure 1. The final corpus consisted of 95 papers, published in the period between 1956 and 2024.

Figure 1: Search and Screening Process

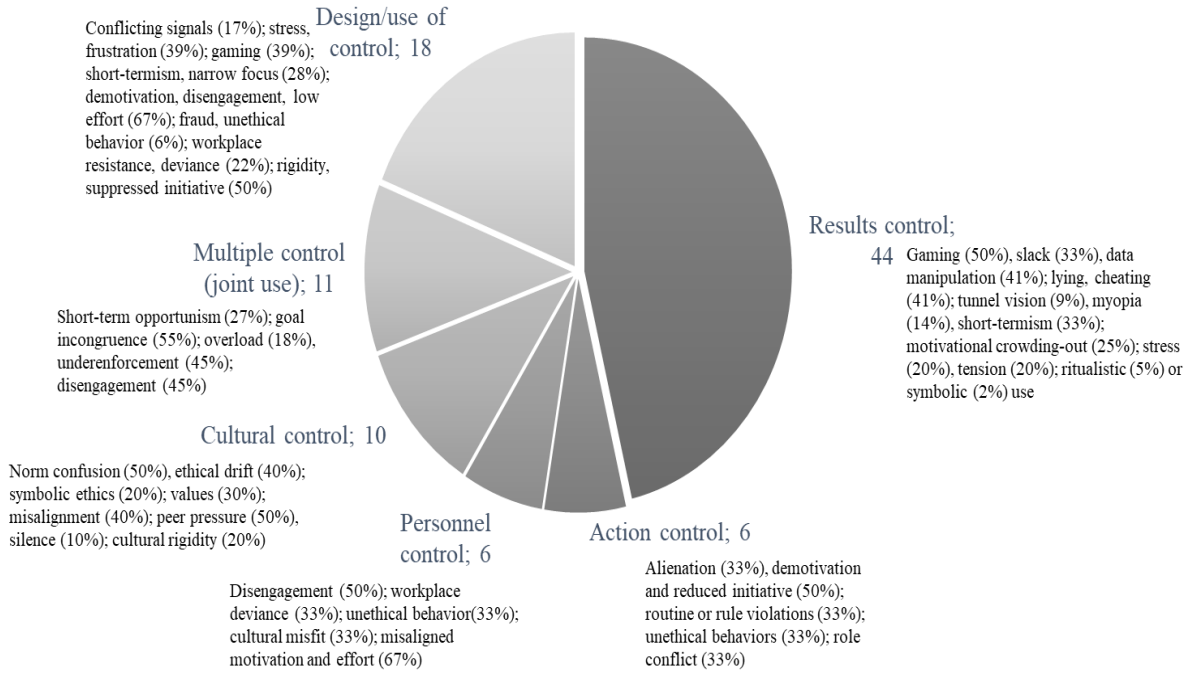


Source: Own work.

In line with Bonner et al. (2006) and Balstad and Berg (2020), particular attention in thematic analysis was given to papers published in top-tier management accounting journals, including: Accounting, Organizations and Society; Management Accounting Research; Journal of Management Accounting Research; The British Accounting Review; Accounting, Auditing & Accountability Journal. Data were extracted via a structured matrix in Excel, capturing for each paper i) MCS type, ii) type of manifested control problem (e.g., gaming,

ethical erosion, resistance), iii) descriptions of problem drivers and contexts were recorded. Preliminary thematic analysis revealed two additional cross-cutting themes alongside the four OOC control types: problems arising from the joint use of multiple controls, and problems arising from design–use misalignments. These themes are not additional control types, but analytical overlays capturing interaction effects and enactment problems that occur across the four OOC categories. To ensure reliability, authors independently assigned the 95 papers to these 6 themes. Agreement was reached in 88 cases (92.6%), with the remaining seven disagreements (7.4%) resolved through discussion. Following this step, we jointly coded the reported control problems of each paper to ensure a consistent application of the coding framework. Codes were initially based on prior literature and updated iteratively. Given the collaborative approach to coding within themes, interrater reliability statistics were not calculated at this stage. Results are summarized in Appendix 3, illustrated in Figure 2, and presented in detail in the following sections.

Figure 2: Results of Thematic Analysis and Conding for Control Problems



Source: Own work.

Notes: Total n = 95 studies; numbers next to control type are number of studies assigned to each theme; percentages are calculated based on the number of studies within each theme; control problem codes are not mutually exclusive.

By and large, most studies in our review focused on the dysfunctions of result controls (performance management systems, budgeting, or outcome-based controls in general) – 44 studies (46%). Action controls and personnel controls were each examined in 6 studies (6%), cultural controls in 10 studies (11%), multiple controls in 11 studies (12%), and issues of

control design or use in 18 studies (19%). The most frequently discussed dysfunctions within each category were as follows: in result controls, *gaming* (50% of studies in this theme); in action controls, *demotivation* (50%); in personnel controls, *misaligned motivation and effort* (67%); in cultural controls, *norm confusion* (50%) and *peer pressure* (50%); in multiple controls, *goal incongruence* (55%); and in control design/use, *demotivation* (67%). In further analysis, conceptually overlapping codes were consolidated into broader categories of manifested control problems (e.g., *gaming* and *slack* merged under *Gaming*; *data manipulation* and *lying/cheating* under *Unethical conduct*; *tunnel vision*, *myopia*, and *short-termism* under *Tunnel vision*) to enhance analytical clarity and parsimony.

2.3 Findings

We present the findings in six main themes of control problems associated with different types or configurations of MCS. For each theme, we distinguish the *manifested control problems* (observable dysfunctional behaviours), the *underlying mechanisms* (how and why the control leads to those problems), and relevant *contextual influences* (situational factors that exacerbate or mitigate the issues). Appendix 3 presents an overview of all reviewed studies and the identified dysfunctional behaviours.

2.3.1 Theme 1: Result Controls

Result controls guide behaviour by tying rewards or sanctions to the achievement of specific performance outcomes (Merchant & Van der Stede, 2024). They are intended to align employee actions with organisational goals by holding individuals accountable for results. However, 44 studies in our review document that result controls can generate dysfunctions when targets and incentives are poorly designed or applied rigidly (summarized in Figure 3):

*Gaming and misreporting***.** Employees manipulate results or actions to meet performance targets without genuine improvement (Carroll & Marginson, 2021; Franco-Santos et al., 2012). Examples include gaming the metrics (intentionally distorting data or activities to "look good" on paper; Adnan et al., 2013; Cugueró-Escofet & Rosanas, 2017; Goebel & Weißenberger, 2016; Grizzle, 2002; Merchant, 1990; Ridgway, 1956; Speklé & Verbeeten, 2014) and budgetary slack (understating targets to easily achieve them; De Baerdemaeker & Bruggeman, 2015; Dunk, 1993; Onsi, 1973; Schiff & Lewin, 1970; Young, 1985). Such behavior can involve misrepresenting figures, concealing unfavorable data, or timing transactions to hit benchmarks (Libby & Lindsay, 2013; Merchant, 1990; Otley, 1978; Van der Stede, 2000).

Unethical conduct. High-pressure result controls can induce dishonesty (lying, cheating) and other unethical acts to avoid sanctions or gain rewards (Heitger et al., 2021; Jensen, 2003). Unmet goals tied to large rewards increase the likelihood of unethical behaviors such as

lying and cheating (Schweitzer et al., 2002). If failure is punished severely, individuals may rationalise unethical choices to avoid negative consequences (Jacobs et al., 2013). Deore et al. (2023) demonstrate how dishonest reporting arises from budgetary pressure and a lack of managerial support.

*Tunnel vision***.** A narrow focus on measured performance indicators often causes employees to concentrate on those measures at the expense of broader objectives. This tunnel vision (or myopia) means important but unmeasured aspects (like long-term innovation, service quality, or strategic responsiveness) are neglected (Vakkuri & Meklin, 2006) or immediate targets are prioritised over long-term value (Hansen & Van der Stede, 2004; Hunton et al., 2008; Van der Stede, 2001).

*Crowding-out intrinsic motivation***.** Excessive reliance on extrinsic incentives (e.g., result-based pay) can erode intrinsic motivation (employees' natural enthusiasm or ethical standards). When tasks are heavily monetised, individuals lose some intrinsic interest in the work, leading to lower engagement and effort, reduced creativity, and even short-termism (Gneezy et al., 2011; Siverbo et al., 2019).

Psychological stress and tension. Rigid and high-stakes performance targets, in particular when perceived as unfair or beyond one's control, create pressure that can harm well-being due to job-related stress, anxiety, and tension (Becker & Green, 1962; Linder et al., 2020) and may manifest as fear of failure, cognitive overload, or burnout. In some cases, stress leads to resistance – employees push back or disengage from the control system to cope (Hirst, 1983; López-Valeiras et al., 2024), especially when the systems are perceived as irrelevant or misaligned (Elmassri & Harris, 2011; Merchant, 1981).

Ritualistic use. When budgeting becomes a symbolic or ceremonial activity, performed to satisfy external expectations rather than guide internal decision-making, it can reinforce "comfort zones" and foster resistance to change (Bourmistrov & Kaarbøe, 2013) and induce symbolic compliance, detaching budgeting from operational reality (Hussain, 2005; Sponem & Lambert, 2016). These ritualistic patterns hinder innovation and promote formality over functionality.

Several mechanisms explain why result controls breed these problems. Unrealistic or rigid performance targets are a primary culprit – when goals are inflexible or misaligned with actual capabilities, employees feel compelled to cheat or cut corners (e.g., Khajehnejad & Linder, 2022). Incentive schemes that overemphasise quantitative metrics encourage a "win at all costs" mentality (e.g., Jensen, 2003; Lopez-Valeiras et al., 2024), rewarding the appearance of success over genuine performance. When used punitively, they can create a climate of fear, prompting individuals to hide failures and distort figures (Merchant, 1990; Schweitzer et al., 2002). Often, they erode autonomy and intrinsic purpose: employees view tasks as merely a way to hit numbers, not as intrinsically meaningful. In sum, result controls

tend to fail when they are overly rigid, financially driven, and disconnected from those being controlled.

The behavioural effects of result controls are highly context-dependent. In environments with complex or unpredictable tasks rigid result targets are less credible and more stressful (Brownell & Hirst, 1986). When outputs are hard to measure or outcomes uncertain, result-based accountability increases frustration and gaming. Organisational structure and culture also matter: decentralised or knowledge-driven organisations often resist top-down targets, e.g., coercive budgeting provokes greater pushback and cynicism in flexible, creative settings (Elmassri & Harris, 2011; Merchant, 1981). Involving employees in setting targets or budgets improves commitment and reduces dysfunctional responses like slack creation (Dunk, 1993; Lau & Eggleton, 2004; Onsi, 1973), whereas exclusion fosters alienation and opportunism. Leadership approach also plays a role: when result controls are used mainly for surveillance and punishment (rather than feedback and support) perceptions of unfairness and threat intensify (López-Valeiras et al., 2024).

Table 1: Overview of Findings for Result Controls

Dysfunctional Behavior	Description	Example studies
Gaming & misreporting (30 studies)	Metric manipulation, budgetary slack, timing/cover-ups Key driver: Unrealistic/rigid targets, imposed top-down (without participation); metric overemphasis	Merchant, 1981; Becker & Green, 1962; Jensen, 2003; Elmassri & Harris, 2011; Adnan et al., 2013; Bourmistrov & Kaarbøe, 2013; Libby & Lindsay, 2013; Speklé & Verbeeten, 2014; De Baerdemaeker & Bruggeman, 2015; Goebel & Weißenberger, 2016; Sponem & Lambert, 2016; Cugueró-Escofet & Rosanas, 2017;
Unethical conduct (18 studies)	Lying, cheating, dishonest reporting Key driver: high-stakes incentives; punitive sanctions	Schweitzer et al., 2002; Grizzle, 2002; Jensen, 2003; Heitger et al, 2021; Deore et al., 2023;
Tunnel vision (16 study)	Narrow focus on KPIs; myopia, neglect of long-term/broader goals Key driver: narrow KPI design, overemphasis on financial measures	Hopwood, 1972; Hansen & Van der Stede, 2004; Vakkuri & Meklin, 2006; Hunton et al. 2008; Goebel & Weißenberger, 2016
Crowding-out intrinsic motivation (11 studies)	Extrinsic rewards erode intrinsic interest/ethics Key driver: over-reliance on extrinsic (financial) reward,	Hunton et al. 2008; Gneezy et al., 2011; Goebel & Weißenberger, 2016
Psychological stress & tension (15 studies)	Pressure, anxiety, burnout; resistance when perceived unfair Key driver: rigid, unfair goals; punitive use, lack of participation	Becker & Green, 1962; Otley, 1978; Hirst, 1981, 1983; Merchant, 1981; Hunton et al 2008; Elmassri & Harris, 2011; Linder et al., 2020; López-Valeiras et al., 2024;
Ritualistic use (3 studies)	Symbolic/ceremonial budgeting; formal compliance over function Key driver: symbolic practice to satisfy external expectation	Hussain, 2005; Bourmistrov & Kaarbøe, 2013; Sponem & Lambert, 2016;
Contexts: complex/unpredictable tasks, including creative/innovation; hard-to-measure outputs; decentralised/knowledge-driven organisations; participative vs coercive leadership		

Source: Own work.

2.3.2 Theme 2: Action Controls

Action controls aim to secure desirable behaviours by stipulating specific actions (e.g., rules, procedures, direct supervision) rather than measuring end results. The intention is to prevent and reduce risk by ensuring employees follow defined steps or policies. Our review (summarized in Figure 4) includes 6 studies which collectively demonstrate that action controls can backfire if implemented in a rigid, coercive manner or without regard for employees' need for autonomy as they give rise to problems such as:

*Employee alienation and demotivation***.** When rules and supervision become overbearing (i.e., micromanagement), employees often feel alienated and disengaged. Adler and Borys (1996) note that coercive bureaucratic systems, with their rigid procedures and restricted autonomy, weaken morale and initiative. Christ et al. (2012) show that preventive action controls can suppress intrinsic motivation, particularly when employees feel micromanaged. Lagios et al. (2023) find that too many unnecessary rules (i.e., red tape) is perceived as dehumanizing, which in turn leads to passive resistance, disengagement. and decreased performance.

Routine violations and workarounds. Extremely strict action controls can lead employees to routinely violate or bypass rules in order to get work done. Especially under high time pressure, people take shortcuts to cope with an unsustainable number of rules (Reason et al., 1998).

Unethical behaviours. Dishonesty and rule-breaking may increase in response to harsh, detective control and treating staff as untrusted subjects (Christ et al., 2012). Poor leadership and overly hierarchical control structures can breed ethical dysfunction (e.g., behaviours like distrust, cynicism, or egoistic actions; Jurkiewicz & Giacalone, 2014).

Role conflict. In occupations requiring professional judgement (e.g., healthcare, R&D), action controls may produce role conflict. Abernethy and Stoelwinder (1995) documented this tension in hospitals: doctors experience stress and reduced performance when administrative rules intrude on their clinical autonomy. Rigid protocols or red tape may clash with professional norms or expertise, giving rise to resentment and psychosomatic strain, leading to turnover among skilled staff (Lagios et al., 2023).

Dysfunctional outcomes from action controls typically arise when these controls are implemented coercively (Adler & Borys, 1996). If every minor decision requires approval or every process is standardized, employees are expected to obey rather than contribute which leads to alienation instead of engagement. Inflexible rules that fail to accommodate judgement, exceptions, or task variability push employees into either mindless compliance or even non-compliance. Another trigger may be over-monitoring: when employees feel overly scrutinised, they may withold information or behave opportunistically. Additionally, controls that conflict with professional judgement or values provoke psychological resistance by undermining autonomy. Finally, participation in rule-setting (or at least

understanding the rationale) enhances perception of legitimacy, promoting compliance and reducing workarounds.

The effects of action controls are moderated by contextual factors. Where tasks are complex, unpredictable or creative, rigid rules are more likely to misfit and frustrate, whereas in highly routine or safety-critical contexts (e.g., assembly lines, aviation), detailed procedures may be expected and even valued, reducing resistance. Organisational culture also shapes response. In strong professional cultures (e.g., doctors, academics), externally imposed rules often clash with norms of autonomy and increase role conflict (Abernethy & Stoelwinder, 1995), while in a culture of discipline (e.g., military units) or high compliance, employees might accept extensive action controls (Lagios et al., 2023). Leadership and communication style significantly influence outcomes. If rules are introduced with clear justification, training, and managers follow the rules themselves, employees perceive them as more legitimate and cynicism is less likely (Jurkiewicz and Giacalone, 2014).

Table 2: Overview of Findings for Action Controls

Dysfunctional Behavior	Description	Authors
Employee alienation & demotivation (3)	Suppressed morale, initiative, and engagement Key driver: rigid, coercive rule enforcement; excessive monitoring (micromanagement); lack of participation/justification	Adler & Borys, 1996; Christ et al., 2012; Lagios et al, 2023
Routine violations & workarounds (2)	Rules perceived as excessive or unnecessary are bypassed; shortcuts arise Key driver: overly strict rules; procedural overload (red tape)	Adler & Borys, 1996; Reason et al., 1998
Unethical behaviour (2)	Dishonesty, cynicism, opportunistic behaviour Key driver: distrustful control; tight monitoring, lack of justification;	Christ et al, 2012; Jurkiewicz & Giacalone, 2014
Role conflict (2)	Professional strain when forced to overrule professional judgement Key driver: administrative rules clash with professional norms leading to reduced autonomy; administrative overload	Abernethy & Stoelwinder, 1995; Lagios et al, 2023.
Contexts: complex/unpredictable tasks; creative/professional work; time pressure; professional culture; leadership communication and ethical leadership		

Source: Own work.

2.3.3 Theme 3: Personnel Controls

Personnel controls seek to align behaviour by selecting and developing the "right" people, rather than by monitoring or prescribing actions. Hiring, training, job design, and socialisation practices are intended to ensure employees possess the values, skills, and self-regulation needed to behave in the organisation's best interest (Merchant & Van der Stede, 2024). Personnel controls are often assumed to be positive or preventative, but our review found 6 studies highlighting they, too, can give rise to control problems if misapplied or not supported by other systems (summarized in Figure 5):

Mistrust and disengagement. Even when suitable candidates are hired and formally empowered, they may become passive rather than proactive, if they distrust their superiors or are uncertain about their discretion (Campbell, 2012).

Workplace deviance. If personnel selection fails to filter out unethical or unmotivated individuals, the risk of counterproductive work behaviors (e.g., theft, misuse of resources, or absenteeism) increases. MacLane and Walmsley (2010) find that hiring employees with certain personality traits (e.g., low conscientiousness) is linked to higher incidents of counterproductive work behaviors. Moreover, once employed, these individuals may exploit the autonomy granted to them, undermining control from within.

Cultural misfit and value misalignment. When selection procedures ignore cultural differences in motivation, communication styles and work-values, particularly in international contexts, cultural misfit leads to counterproductive behavior. Riyono (1998) found that Western managers applying home-country hiring criteria in a collectivist country ended up with personnel who could not adapt to local team norms. If training and career development programs (personnel control tools to indoctrinate shared values) are weak or inconsistent, the result can be counterproductive behaviours and norm violations. MacKenzie et al. (2011) show that poor onboarding, vague feedback systems, or inconsistent reinforcement allow negative behavioral norms to spread unchecked. In such cases, employees do not receive or accept the organisation's expected norms, and they may even form their own subcultures opposed to management intent.

Misaligned motivation and effort. Even with good hiring, motivation can fade if performance evaluation and incentives are poorly matched to task requirements or roles (Strauss, 2015). Abernethy et al. (2015) show that when selected professionals face noisy or ambiguous performance measures, their motivation suffers. They become frustrated that their contributions are not accurately measured or rewarded, which leads to reduced effort or exit.

Dysfunctional outcomes related to personnel controls often stem from misalignment with other system elements or contexts. Hiring talented people is insufficient if complementary controls (e.g., performance measurement, culture) send conflicting signals – we explore this more in Theme 5. For instance, an organisation may recruit for creativity and initiative but then impose bureaucratic procedures and rigid targets that stifle such traits (Strauss, 2015).

Another driver is inadequate selection processes – if hiring criteria fail to assess crucial qualities needed (e.g., integrity, cultural fit), personnel controls are compromised from the outset. For example, prioritising candidates with technical skills while overlooking values or attitudes may lead to cultural misfits. Lack of ongoing support is another common issue. Even well-selected employees need reinforcement through training, mentoring, and feedback to maintain alignment with organizational values. When organisations rely only on hiring, neglecting socialization processes, employees may adopt undesirable norms or be influenced by misaligned colleagues. Moreover, if management does not genuinely empower employees (by micromanaging or second-guessing), trust deteriorates and people respond by withdrawing or defaulting to safe, minimal behaviours (Campbell, 2012).

The effectiveness of personnel controls is highly context dependent. Cultural norms, task and environment complexity, and leadership behaviour all shape outcomes. For example, national or regional culture influences whether selection and socialisation practices are effective (Riyono, 1998). A method successful in one cultural context may generate misfits in another. In highly uncertain or creative environments, where outputs are hard to measure (e.g., creative R&D jobs), standard evaluation systems may demotivate even the best hires. Conversely, in stable settings with measurable tasks and clear performance metrics, employees with the right skills may thrive. Finally, leadership plays a critical role: insincere or inconsistent leadership can undermine personnel controls as employees tend to follow actual behavior rather than formal training or stated values.

Table 3: Overview of Findings for Personnel Controls

Dysfunctional Behavior	Description	Authors
Mistrust & disengagement (3)	Employees do not trust superiors, withdraw or act passively Key driver: poor onboarding; lack of reinforcement; lack of empowerment; inconsistent leadership	Campbell, 2012; Abernethy et al., 2015; Strauss, 2015
Workplace deviance (3)	Theft, absenteeism, or misuse of resources Key driver: inadequate selection processes (focusing on technical over ethical/motivation fit)	MacLane & Walmsley, 2010; MacKenzie et al., 2011; Strauss, 2015
Cultural misfit & value misalignment (2)	Misfit, resistance, subcultures because individuals have different cultural values than the organization Key driver: Inadequate selection processes (focusing on technical over cultural fit); lack of reinforcement or socialisation	Riyono, 1998; MacKenzie et al., 2011
Misaligned motivation & effort (4)	Reduced motivation and effort due to wrong incentives Key driver: Misalignment between personnel and other controls; ambiguous performance metrics	Abernethy et al. 2015; Strauss, 2015
Contexts: creative and complex tasks, hard-to-measure output, international/multinational contexts, cultural distance, bureaucratic organizations, leadership style		

Source: Own work.

2.3.4 Theme 4: Cultural Controls

Cultural controls shape behaviour by cultivating shared values, norms, and beliefs within the organisation through socialisation processes, peer influence, and leadership example (Merchant & Van der Stede, 2024; Ouchi, 1980). Strong culture can reduce the need for formal rules by internally aligning behaviour. However, our synthesis of 10 papers reveals that the following dysfunctional outcomes can arise when there is misalignment, or when culture is used in a superficial way (summarized in Figure 6):

Norm confusion and ethical drift. In weak or fragmented organisational culture, employees receive mixed signals about acceptable behaviour and small unethical acts may be tolerated, but over time they become normalized through a process of ethical drift (Payne, 1980). Trust-based controls can deteriorate over time, resulting in confusion and conflict as informal understandings break down (Langfield-Smith & Smith, 2003).

Symbolic ethics and cynicism. Cultural control tools (e.g., codes of ethics, values statements, ethics training) can breed employee cynicism and lose credibility if they are perceived as merely symbolic. Weaver et al. (1999) report that when organisations implement ethics programs without genuine leadership commitment, employees view them as mere window dressing, whereas Applebaum and Shapiro (2006) emphasize that modelling ethical leadership is crucial for preventing norm violations. This scepticism manifests in disengagement – employees might mock or ignore the stated values, since they see no substance behind the slogans.

Values misalignment and resistance. A clash between employees' personal values and the organisation's declared values, can provoke resistance, withdrawal, and motivational crowding-out (Tayler & Bloomfield, 2011). Weaver et al. (1999) argue that if staff perceive the company's norms as unethical or inconsistent with their own moral compass, they will not internalise those norms.

Peer pressure and silence. In some cultures, peer norms may encourage silence or conformity even when wrongdoing occurs, especially if employees perceive retaliation risk (Kaptein, 2011; Van Fleet & Griffin, 2006). This undermines honesty as a cultural control and allows misconduct to persist. because employees do not challenge or report it. Over time, honest employees either adapt or exit, reinforcing the dysfunctional norm.

Cultural rigidity. A strong established culture can become rigid, rejecting new control initiatives (Malmi et al., 2022). Employees deeply attached to "how things have always been," might collectively reject formal control systems that feel alien. Marc and Peljhan (2019) find that when MCS are implemented in environments that lack a particular "calculative culture," employees may resist or underutilize these systems because the misalignment between system logic (e.g., quantification, measurement, analysis) and dominant values (e.g., intuition, flexibility, informal knowledge) leads to rejection and undermining the effectiveness of MCS.

Cultural control problems often arise from inconsistencies within the control environment. One mechanism is the gap between promoted values and actual behavior. When leaders publicly promote values like integrity but privately tolerate unethical behavior from high-performers, employees perceive the disconnect (Weaver et al., 1999). Another driver is the failure to institutionalise values: without embedding them into hiring, promotion, and reward systems, values remain superficial. Under pressure (say, a performance crisis), people may abandon unreinforced values in favour of measurable goals, accelerating ethical erosion (Langfield-Smith & Smith, 2003). Finally, extremely strong cultures can become dysfunctional by resisting change – employees may rely so heavily on ingrained norms that they dismiss formal controls or novelties as irrelevant.

Table 4: Overview of Findings for Cultural Controls

Dysfunctional Behavior	Description	Authors
Norm confusion & ethical drift (9)	Ambiguity about acceptable behaviour, leading to gradual normalization of misconduct. Key driver: weak institutionalization of values; lack of formal support systems, gap between stated vs. enacted norms.	Payne 1980; Weaver et al. 1999; Langfield-Smith & Smith, 2003; Applebaum & Shapiro, 2006; Van Fleet & Griffin, 2006; Kaptein, 2011; Tayler & Bloomfield, 2011; Malmi et al, 2022
Symbolic ethics & cynicism (2)	Cynical attitude to ethics programs or values statements perceived as symbolic or insincere. Key driver: gap between stated vs. enacted norms; lack of genuine leadership commitment; cultural heterogeneity (subcultures).	Weaver et al. 1999; Applebaum & Shapiro, 2006
Values misalignment & resistance (6)	Resistance, withdrawal, or motivational crowding-out because personal values are not aligned with organizational. Key driver: Clash between employee values and organizational values; gap between stated vs. enacted norms; strong ingrained culture; cultural heterogeneity (subcultures).	Daley et al, 1985; Weaver et al. 1999; Applebaum & Shapiro, 2006; Kaptein, 2011; Tayler & Bloomfield, 2011; Malmi et al., 2022
Peer pressure & silence (5)	Peer conformity discourages whistleblowing or dissent, allowing wrongdoing to persist. Key driver: over-reliance on trust-based control (no formal support systems); fear of retaliation.	Van Fleet & Griffin, 2006; Kaptein, 2011
Cultural rigidity (2)	Rejection of new controls because they differ from existing. Key driver: Strong traditions and deeply ingrained norms resist change.	Marc & Peljhan 2019; Malmi et al., 2022
Contexts: leadership style, international/multinational contexts, national and professional culture, organizational culture and maturity, high-pressure context.		

Source: Own work.

Cultural controls are also shaped by context. Leadership behaviour is central: when leaders consistently model desired values, cultural controls are legitimized and truly guide behaviour (Van Fleet & Griffin, 2006). In contrast, unethical or inconsistent leadership sabotages these controls regardless of stated principles (Applebaum & Shapiro, 2006). National and professional culture provide additional context (Daley et al., 1985): for instance, a high power-distance culture may discourage employee voice, whereas professions like engineering emphasize safety and precision, aligning with certain control values. Cultural heterogeneity (multiple subcultures or diverse backgrounds) can dilute shared norms if not

explicitly acknowledged and integrated. Organisational history and lifecycle further affect cultural control dynamics. Long-established companies often have entrenched norms that resist change, whereas start-ups may be more open to shaping culture intentionally. External pressures, such as crises or scandals, can fracture even strong cultures if fear overrides trust; however, adaptive cultures can buffer such shocks, sustaining cohesion and guiding ethical behaviour under stress.

2.3.5 Theme 5: Multiple Controls (Joint Use of Controls)

In practice, organisations often deploy multiple controls concurrently (Bedford, 2020; Malmi & Brown, 2008). For example, a company may use result controls (performance-based pay) alongside action controls (standard procedures) and cultural controls (core values). The intention is that these controls complement each other and provide a coherent system of behavioural governance (e.g., formal rules supported by a strong ethical culture). However, our review (drawing on 11 papers) finds that the interactions among multiple controls can themselves become a source of control problems when the controls are not well aligned (summarized in Figure 7). We identified several dysfunctional patterns in the joint use of controls:

Short-term focus and opportunism. Using an unbalanced formal control mix can inadvertently increase pressure and rigidity. Madhani (2016) shows that when employees are tightly supervised on their behaviours and intensely rewarded on outcomes, they often resort to short-term opportunism. Individuals trying to juggle multiple demanding controls simultaneously can yield gaming, information distortion, and neglect of long-term objectives (Ramaswami, 1996).

Goal confusion and overload. Multiple controls sometimes send conflicting signals to employees, causing confusion about priorities. If one system emphasizes cost minimisation and another emphasizes customer service, employees are uncertain which to prioritise or become overloaded trying to meet all expectations (Cravens et al., 1993). Malmi and Brown (2008) and Bedford (2020) discuss how poorly integrated control systems create overlap and redundancy that confuse users and reduce accountability, while Cravens et al. (2004) find that consistency across multiple types provides more clarity, so there will be less dysfunctional behaviour.

Underenforcement and ethical drift. Relying on multiple informal controls (e.g., personnel and cultural controls together) can create a false sense of security when managers assume that "values will suffice" and formal discipline is neglected. Without structural reinforcement, ethical norms start to drift and erode over time (Sorauren, 2000). Strong extrinsic incentives can overshadow informal cues, prompting rationalisation of unethical behaviour. Ethical culture deteriorates when not consistently supported by hiring, training, and leadership (Goebel & Weißenberger, 2017). Even well-intended systems can fail if peer

norms shift toward deviance or self-interest (Bellora-Bienengräber et al., 2022), weakening the effectiveness of control.

Moral disengagement. When formal controls (e.g., strict targets, rules) conflict with informal controls (e.g., values, norms), employees may experience cognitive dissonance. Fiolleau et al. (2018) show that strong result controls, unsupported by ethical norms, lead employees to rationalise gaming and slack as acceptable. This misalignment provided psychological freedom to prioritize rewards over values. The gap between "hard" metrics and "soft" values thus enables unethical behaviour and undermines control effectiveness.

Table 5: Overview of Findings for Multiple (jointly used) Controls

Dysfunctional Behavior	Description	Authors
Short-term focus & opportunism (3)	Combined pressure from strong result + action controls fosters short-termism, gaming, and neglect of long-term goals. Key driver: excessive control layering (too many formal mechanisms); absence of overarching control philosophy.	Ramaswami, 1996; Madhani, 2016; Goebel & Weißenberger, 2017
Goal confusion & overload (6)	Mixed and conflicting priorities, creating overload and reduced accountability. Key driver: misalignment across control types (isolated design, conflicting metrics); absence of overarching control philosophy.	Cravens et al, 1993; Sorauren, 2000; Cravens et al, 2004; Malmi & Brown 2008; Fiolleau et al., 2017; Bedford 2020
Underenforcement & ethical drift (5)	Underenforced discipline and ethical decay Key driver: over-reliance on informal (trust-based) controls, gap between „soft" (values) and „hard" (formal) control.	Sorauren, 2000; Alvesson & Kärreman, 2004; Fiolleau et al., 2017; Goebel & Weißenberger, 2017; Bellora-Bienengräber et al., 2022
Moral disengagement (5)	Rationalisation of unethical acts Key driver: gap between „soft" (values) and „hard" (formal) control.	Sorauren, 2000; Alvesson & Kärreman, 2004; Fiolleau et al., 2017; Goebel & Weißenberger, 2017; Bellora-Bienengräber et al., 2022
Contexts: leadership style and consistency, organizational structure (cross-functional coordination), organizational life-cycle stage and maturity, regulated/compliance-heavy industries		

Source: Own work.

Dysfunctional dynamics in multiple-control settings often arises from a lack of coherence and reinforcement among controls. A primary driver is misalignment – controls are frequently designed or implemented in isolation, without regard for their interaction (Bedford, 2020). For instance, different departments might introduce uncoordinated systems (a quality control system in production, a separate performance appraisal in HR) resulting in overlap or contradiction. This fragmentation allows issues to "fall through the cracks" and creates opportunities for employees to exploit gaps.

In mixed formal-informal setups, a key mechanism is the decoupling of promoted values from actual practices or formal controls (Alvesson & Kärreman, 2004). This fosters moral

licensing (rationalizing unethical behaviour on metrics since one has symbolically complied with values) or outright disregard for one set of controls. Excessive control layering also creates complexity, prompting employees to selectively comply with those tied to reward. Finally, a lack of overarching control philosophy contributes to dysfunction. Without clear guidance on how multiple controls should operate together or be prioritized, employees make their own interpretations, often favouring short-term or self-serving goals. In summary, without deliberate design and coordination of control systems, multiple controls can interfere with each other and encourage exactly the behaviours they were meant to prevent.

Contextual factors determine whether multiple controls align or conflict. Poor cross-functional communication fosters siloed control development, while coherent objectives and metrics across units mitigate misalignment. Environmental and strategic context also matter in stable environments with a clear strategies, alignment is easier, whereas turbulent contexts or strategic change often cause controls to evolve unevenly. Leadership consistency is crucial - if leaders emphasize one control dimension to the neglect of others, employees will do the same. Open cultures can surface and resolve misalignments, whereas fear-based cultures suppress such feedback. Regulatory pressures may also impose formal controls (compliance requirements) that clash with internal norms, particularly in heavily regulated industries. Control system maturity matters, too, as newly implemented and incumbent controls might clash. Misalignments are common during transitions but can improve over time with deliberate integration and ongoing realignment.

2.3.6 Theme 6: Design and Use Misalignments

The final theme addresses control problems arising not from any particular type of control, but from the inherent design features or patterns of use across systems. Based on 18 reviewed papers, this theme highlights how the way controls are structured and used can itself generate unintended consequences (summarized in Figure 8). Misalignments between the design and use tend to produce manifested problems similar to those discussed in previous themes (e.g., gaming, ethical erosion, resistance), but these manifestations emerge specifically from how controls are conceived or executed.

One common mechanism is employee perception of controls as coercive, punitive, or unjust, which often invites resistance and deviant responses, such as fraud, sabotage or withdrawal (Litzky et al., 2006). Restrictive or authoritarian framing may intensify fraudulent behaviour (Liu et al., 2015) or emotional resistance (Duarte et al., 2018). When systems lack ethical legitimacy or appear imposed without justification, employees may feel morally justified in circumventing or undermining them (Rosanas & Velilla, 2005).

A common design issue is lack of contextual fit**,** making MCS ineffective, irrelevant or even counterproductive (Baliga & Jaeger, 1984; Suh, 2019). Chenhall (2003) and Davila (2000) emphasize that rigid MCS become irrelevant in dynamic environments, where managers

either ignore them (and rely on informal adjustments) or suffer poor performance because the control is out of sync with reality. Similarly, misfit with task requirements can provoke stress, frustration, and gaming (Jaworski, 1988; Tannenbaum; 1962).

Table 6: Overview of Findings for Design and Use misalignments

Dysfunctional Behavior	Description	Authors
Confusion, conflicting signals (3)	Unclear and ambiguous priorities and accountability Key driver: fragmentation of control systems, poor metric design	Davila (2000); Hussain & Gunasekaran (2002); Ferreira & Otley (2009)
Stress, frustration (7)	Strain and cognitive overload because of misfit between control requirement and task reality Key driver: contextual misfit (control type – task misalignment)	Tannenbaum, 1962; Jaworski, 1988; Shields et al., 2000; Chenhall, 2003; Litzky et al. 2006; Willert et al, 2017; Duarte et al., 2018;
Gaming (7)	Opportunistic data or behavioural distortion Key driver: contextual misfit (control type – -task), poor metric design	Baliga & Jaeger, 1984; Anderson & Oliver, 1987; Jaworski, 1988; Shields et al., 2000; Rosanas, & Velilla, 2005; Litzky et al., 2006; Ferreira & Otley, 2009
Short-termism, narrow focus (5)	Crowding-out exploration and long-term learning Key driver: excessive and rigid diagnostic use of controls	Anderson & Oliver, 1987; Davila, 2000; Rosanas & Velilla, 2005; Henri, 2006; Suh, 2019
Demotivation, disengagement. low effort (12)	Reduced autonomy and intrinsic motivation leading to low effort Key driver: inadequate feedback and learning loops (weak interactive use); contextual misfit (control type – task or environment misalignment), irrelevant systems	Tannenbaum, 1962; Baliga & Jaeger, 1984; Eisenhardt, 1985; Anderson & Oliver, 1987; Jaworski, 1988; Davila, 2000; Shields et al., 2000; Hussain & Gunasekaran, 2002; Rosanas & Velilla, 2005; Henri, 2006; Suh, 2019; Abubakar et al., 2022
Fraud, workplace resistance, deviance (5)	Unethical and counter productive behaviours (sabotage, withdrawal) Key driver: perceived unfairness or coercion; lack of participation; punitive framing	Tannenbaum, 1962; Chenhall, 2003; Litzky et al., 2006; Liu et al., 2015; Duarte et al., 2018
Rigidity, suppressed initiative (9)	Reduced adaptability, creativity, and innovation. Key driver: rigid diagnostic use of controls	Baliga & Jaeger, 1984; Eisenhardt, 1985; Davila, 2000, Chenhall, 2003; Henri, 2006; Willert et al., 2017; Duarte et al., 2018; Suh, 2019; Abubakar et al., 2022
Contexts: task uncertainty, complexity; external (market/industry) pressure, leadership style; organizational structure		

Source: Own work.

Fragmentation or contradiction in MCS design further drives dysfunction. Uncoordinated controls may overlap, conflict, or send mixed signals (Ferreira & Otley, 2009), reducing accountability mismatched control types and tasks are also problematic: using behaviour-based controls where outcomes are measurable, or vice versa. Using behaviour controls in innovation-driven tasks stifles initiative (Anderson & Oliver, 1987; Eisenhardt, 1985), while relying on outcome controls in contexts with high-uncertainty or team-based work fosters short-termism, gaming, and demotivation (Shields et al., 2000).

Simons (1995) distinguishes between diagnostic (monitoring, correction) and interactive (learning, adaptation) use of control. Overemphasis on diagnostic use narrows managerial focus and discourages exploration (Abubakar et al., 2022; Henri, 2006), fosters rigidity and slow adaptation (Willert et al., 2017). Design flaws in the metrics (performance indicators) themselves can yield gaming and misinterpretation: non-financial indicators, when unclear or disconnected from strategy, are either ignored or misused, and the intended benefits of broadening the control (beyond financials) are lost (Hussain & Gunasekaran, 2002). More

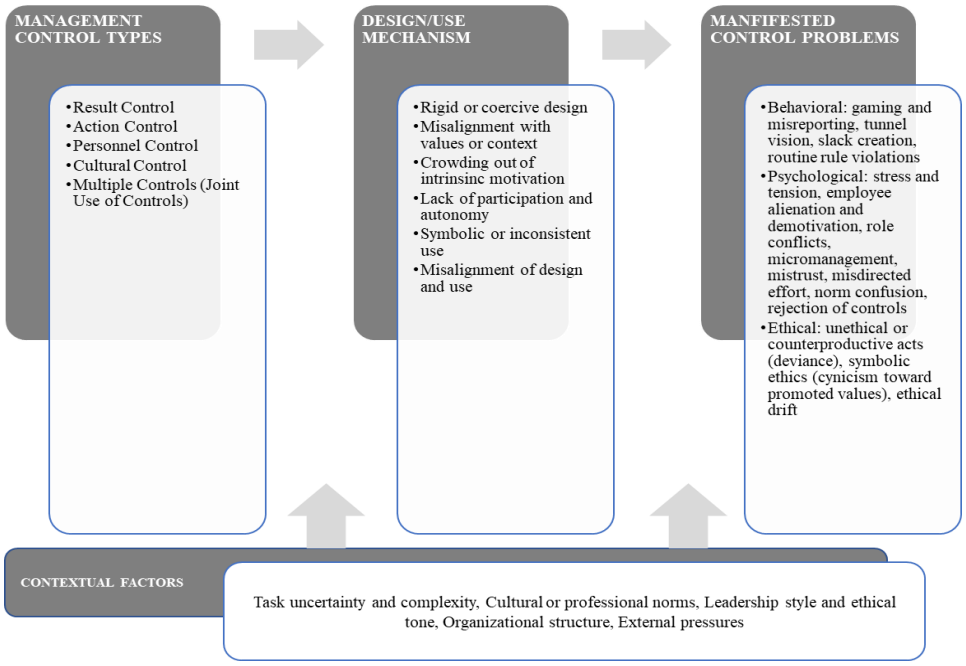
broadly, indicators (financial or not) without clear definitions, targets, or accountability links create confusion and promote opportunistic behaviour.

2.4 Discussion

Drawing from above findings, we propose a conceptual framework that integrates the six themes and explains how MCS give rise to control problems. The core proposition is that MCS – whether result controls, action controls, personnel controls, cultural controls, or combinations thereof, can induce dysfunctional behaviours when they are poorly designed or misaligned with their context and with each other. In other words, the *darker side* of controls emerges not randomly, but through identifiable mechanisms triggered by design/use flaws and moderated by context.

Figure 3 illustrates the relationships between control types, underlying mechanisms, manifested problems, and context. The four basic control types (and their joint use, as well as design and use features) feed into a set of six underlying problem-generating mechanisms. These mechanisms in turn lead to various manifested control problems (the identified dysfunctional behaviours) grouped in three categories: behavioural, psychological and ethical. Surrounding this core, the framework includes key contextual factors that influence the strength and nature of these effects. Together, the figure summarises our review's insights: it is not simply the presence of a control system, but how it is designed, combined, and enacted in context that determines whether it will function as intended or produce adverse outcomes.

Figure 3: A Conceptual Framework of Management Control Problems



Source: Own work.

Figure 3 provides an overview of the most common dysfunctional behaviours (manifested control problems) mapped to each control type. Each category of control tends to be associated with certain recurring dysfunctional behaviours and distinct risk profiles. By mapping these, we offer new insight to both researchers and managers when diagnosing control issues. For example, result controls often lead to issues like gaming, data manipulation, tunnel vision, slack creation, and stress, whereas action controls commonly provoke employee alienation, routine rule violations, micromanagement (excessive supervisory control), and role conflicts. Personnel controls, when problematic, manifest issues such as mistrust, deviance (unethical or counterproductive acts), and motivation misfit (demotivated or misdirected effort). Cultural control failures are linked to norm confusion, symbolic ethics (cynicism toward promoted values), ethical drift, and rejection of controls. By recognizing these behavioural, psychological or ethical patterns, managers can anticipate what might go wrong with a given control approach, and researchers can better pinpoint which dysfunctional behaviours to look for under each control regime.

Table 7: Mapping Control Problems' Manifestation to Control Types

Result controls →	Gaming, data manipulation, dishonesty, demotivation, tunnel vision, stress, slack, resistance
Supporting studies (44): Ridgway (1956); Becker & Green (1962); Schiff & Lewin (1970); Hopwood (1972); Onsi (1973); Otley (1978); Merchant (1981); Hirst (1981); Hirst (1983); Young (1985); Brownell & Hirst (1986); Merchant (1990); Dunk (1993); Grizzle (2002); Schweitzer et al. (2002); Jensen (2003); Hansen & Van der Stede (2004); Hussain (2005); Vakkuri & Meklin (2006); Hunton et al. (2008); Elmassri & Harris (2011); Gneezy et al. (2011); Franco-Santos et al. (2012); Adnan et al. (2013); Bourmistrov & Kaarbøe (2013); Jacobs et al. (2013); Libby & Lindsay (2013); Cheng & Coyte (2014); Speklé & Verbeeten (2014); De Baerdemaeker & Bruggeman (2015); Goebel & Weißenberger (2016); Sponem & Lambert (2016); Cugueró-Escofet & Rosanas (2017); Franco-Santos & Otley (2018); Siverbo et al. (2019); Linder et al. (2020); Van der Stede (2000); Van der Stede (2001); Carroll & Marginson (2021); Heitger et al. (2021); Khajehnejad & Linder (2022); Deore et al. (2023); Lopez-Valeiras et al. (2024)	
Action controls →	Alienation, routine violations, micromanagement, dishonesty, ethical dysfunction, role conflict
Supporting studies (6): Abernethy & Stoelwinder (1995); Adler & Borys (1996); Reason et al. (1998); Christ et al. (2012); Jurkiewicz & Giacalone (2014); Lagio et al. (2023)	
Personnel controls →	Mistrust and disengagment, workplace deviance, motivation/culture misfit, counterproductive behavior
Supporting studies (6): Riyono (1998); MacLane & Walmsley (2010); MacKenzie et al. (2011); Campbell (2012); Abernethy et al. (2015); Strauss (2015)	
Cultural controls →	Norm confusion, symbolic ethics, value misalignment, ethical drift, rejection of controls, resistance
Supporting studies (10): Payne (1980); Daley et al. (1985); Weaver et al. (1999); Langfield-Smith & Smith (2003); Appelbaum & Shapiro (2006); Van Fleet & Griffin (2006); Kaptein (2011), Tayler & Bloomfield (2011); Marc & Peljhan (2019); Malmi et al. (2022).	

Source: Own work.

Beyond listing these manifestations, our review reveals several common sources or mechanisms through which controls turn dysfunctional. These were noted across multiple

studies and control types, suggesting they are generalizable drivers. We grouped them into six key mechanisms, summarized and linked to control types in Table 8.

1) Overly rigid or coercive design. Controls designed with very tight standards, inflexible rules, or an exclusively punitive orientation tend to generate resistance and manipulative behaviours. When employees feel they have no margin of safety and the system is unforgiving, they either break rules (secretly) or comply habitually without real engagement. Excessive rigidity was a theme in result controls (e.g., tight budget targets causing stress and data fudging), action controls (micromanaging rules leading to alienation). This mechanism aligns with findings by Linder et al. (2020) on stress from tight controls and Adler and Borys (1996) on the harms of coercive procedures.

2) Misfit with values or context. A control system can be sound in principle but incompatible with the environment or people. Examples include a sophisticated MCS imposed in a small start-up, or a results-driven control introduced in a culture that prioritises relationships. The maturity and design of existing control systems also play a role as newly introduced controls may clash with established systems. Misfits cause controls to either be ignored, or to create friction and frustration (Jaworski, 1988). We saw this mechanism in multiple themes: cultural misalignment (Theme 4) leading to rejection of controls, and contextual misfit (Theme 6) where controls in dynamic contexts became irrelevant or demotivating. Essentially, when controls ill fit the task, culture, or structure, they lose effectiveness and invite workarounds or opposition.

3) Crowding out of intrinsic motivation. Many control problems emerge when extrinsic motivators overshadow intrinsic drives. This mechanism was evident in result controls (employees losing intrinsic interest due to heavy incentives), in action controls (red tape and preventive rules reducing the satisfaction of doing good work), and even in multiple-control situations (monetary incentives diluting ethical norms, Sorauren, 2000). When a MCS relies too much on carrots and sticks, employees may start doing the minimum for the reward or, worse, bend rules to obtain it, rather than taking initiative or upholding ethical standards. Over time, the workforce becomes more mercenary and less committed to organisational values, undermining long-term performance.

4) Lack of participation and autonomy. A recurring theme is that control systems imposed without employee involvement or that excessively restrict autonomy tend to backfire. When people have no say in goals, rules, or values, they are less committed and more likely to feel resentful or powerless which are conditions ripe for deviance or withdrawal (Elmassri & Harris, 2011; Onsi, 1973). Lack of participation was cited as a factor in budgeting slack and resistance (Theme 1) and in employees' reluctance to engage with controls (Themes 2 and 3). This mechanism basically captures the importance of voice and agency: controls work better when those controlled have some degree of influence or at least understanding of the system's design and purpose. Without it, the controls feel like arbitrary impositions, and people either disengage or game them to reclaim a sense of control.

5) Symbolic or inconsistent use of controls. When control systems are used only ceremonially or applied unevenly, they lose credibility. This mechanism was clear in cultural controls (Theme 4), where symbolic ethics programs led to cynicism, and in multiple controls (Theme 5), where formal controls without informal support led to moral disengagement. Inconsistent use can mean managers enforce rules selectively or leaders exempt themselves from the controls, in both they are sending a message that the control is not truly important or fair. Under such circumstances, employees often comply superficially (symbolic compliance) but do not genuinely adapt their behaviour, or they exploit the inconsistency.

6) Design–use misalignment. This mechanism refers to situations where a control's intended function is undermined by how it is enacted in day-to-day practice. For example, a performance measurement system meant to encourage learning (design intent) might end up being used strictly for punishment (use reality), leading to fear and hiding of data. Or an interactive control (like project workshop) might degrade into a checkbox exercise, failing to be truly interactive. This disconnect might come from middle-management translating systems into practice in a rigid way, or from organisations not training managers in the proper use of new controls. We saw hints of this in Theme 6 (diagnostic vs interactive use issues; in principle, the same MCS can produce very different outcomes depending on use style; Henri, 2006) and a variation of it in Theme 4 (cultural control's gap between promoted values and enacted behavior). Thus, even well-designed controls require alignment in usage; otherwise, employees experience them as off-key which generates distrust and avoidance behaviours.

Table 8: Mechanisms of Dysfunctional Behaviours and Control Types

Mechanism	Description	Control Themes Affected
Overly rigid or coercive design	Controls with tight rules, punishment orientation, or zero tolerance provoke stress, resistance, or superficial compliance.	Result (1), Action (2), Design/use (6)
	Examples: Adler & Borys (1996); Linder et al. (2020); Liu et al. (2015); Duarte et al. (2018)	
Misfit with values or context	Controls misaligned with culture, structure, or task become irrelevant or provoke frustration and gaming	Action (2), Personnel (3), Cultural (4), Design/use (6), Joint (5)
	Examples: Abernethy & Stoelwinder (1995); Riyono (1998), Jaworski (1988); Chenhall (2003); Davila (2000); Marc & Peljhan (2019)	
Crowding out intrinsic motivation	Excessive external incentives reduce intrinsic drive and ethical behavior; controls feel manipulative. Some roles may require strong extrinsic incentives.	Result (1), Action (2), Joint (5)
	Examples: Gneezy et al. (2011); Sorauren (2000); Tayler & Bloomfield (2011)	
Lack of participation and autonomy	Controls imposed without input reduce commitment, trigger resistance, or lead to passive disengagement. Participation isn't always feasible in high-risk settings; participation in budgeting increases slack.	Result (1), Action (2), Personnel (3)
	Examples: Onsi (1973); Elmassri & Harris (2011); Adler & Borys (1996)	
Symbolic or inconsistent use of controls	Controls used for appearance (e.g., ethics codes) or applied unevenly (e.g. gap between soft and hard control) lead to cynicism and superficial compliance. Regulatory frameworks sometimes impose inconsistent controls.	Results (1), Cultural (4), Joint (5)
	Examples: Bourmistrov & Kaarbøe, 2013; Weaver et al. (1999); Sorauren (2000); Goebel & Weißenberger (2017)	
Design–use misalignment	A system's intended function is undermined by how it is designed (e.g. design misaligned to context, absence of overarching control philosophy) and applied (e.g., learning controls used punitively).	Joint (5), Design/use (6), Cultural (4)
	Examples: Henri (2006); Simons (1995); Hussain & Gunasekaran (2002); Langfield-Smith & Smith (2003)	

Source: Own work.

In practice, these mechanisms might interact. For instance, a rigid design can coincide with lack of participation and can spur both motivational crowding-out and perceptions of injustice, if inconsistently applied. By identifying these links between control systems and the observed problems, our review contributes to a deeper understanding of why control problems occur, moving beyond simply cataloguing problem types.

While our review focused on studies documenting dysfunctional effects, we note that adverse outcomes do not occur in all contexts. Franco-Santos et al. (2012) find that some unintended consequences of PMS can be even positive, for example innovation, learning, and motivation. Cravens et al. (2004) finds for salespeople that consistent high control across multiple types provides more clarity, so there will be less dysfunctional behaviour. Linder et al. (2020) find that strong ethical infrastructure (codes of conduct and consistent enforcement) appears to reduce the stress associated with tight performance standards, while Cheng and Coyte (2014) highlight the importance of clear strategy communication for reducing misalignments. These findings suggest that contextual factors reported in the studies act as boundary conditions shaping the extent and severity of dysfunction, even if they do not entirely eliminate it. Indeed, the majority of reviewed studies found contextual factors that significantly accounted for when and why similar controls produced divergent outcomes. We identified five major contextual influences, which are summarized and mapped to control types in Table 9:

1) *Task uncertainty and complexity*. High uncertainty or complex tasks make simplistic or rigid controls more prone to failure. In such contexts, employees need flexibility and adaptive feedback; if controls don't allow that, dysfunction rises (e.g., stress, workarounds). By contrast, in stable, simple tasks, the same controls might function smoothly. This factor was evident in multiple studies (e.g., Brownell & Hirst, 1986) and highlights that managers should adjust control tightness to the nature of the work. Related to this is also organizational maturity. Younger firms are more susceptible to rapid misalignment due to informal practices becoming insufficient as complexity grows, while older/mature firms risk rigidity and resistance to adapting controls, causing misalignments.

2) *Cultural or professional norms*. The prevailing norms in a group or profession can either reinforce or undermine a control system. If an MCS aligns with professional standards (e.g. a safety checklist in an engineering firm), it will be embraced and likely improve behaviour. But if it clashes (e.g., strict time clocks in a creative design studio), it may be undermined. Moreover, national culture affects how controls are perceived (for example, attitudes toward hierarchy will influence acceptance of supervisory controls). Organisations operating in diverse cultural settings must adapt controls accordingly to avoid conflicts that lead to control breakdowns.

3) *Leadership style and ethical tone*. Leaders set the tone for how controls are viewed – whether as helpful tools or repressive inspection. Ethical leadership can amplify the positive effects of controls (by demonstrating fairness, using controls to support rather than looking

for scapegoats) and mitigate dysfunctional outcomes. Conversely, if leaders engage in unethical behaviour or use control information opportunistically (blaming subordinates for failures, etc.), employees will mirror these attitudes, likely leading to more gaming, cover-ups, and resentment. The literature (e.g., Kaptein, 2011; Weaver et al., 1999) repeatedly points to the importance of management example in making control systems work as intended.

4) *Organizational structure*. Organizations with siloed structures or poor cross-functional communication experience greater control conflicts, as isolated departments may implement controls independently without considering the broader organizational alignment (Bedford, 2020; Ferreira & Otley, 2009; Malmi & Brown, 2008). Effective management involves ensuring consistent control logic, objectives and metrics across departments to mitigate such issues.

5) *External pressures*. Whether regulatory, market-, competition- or crisis-driven, external pressure on top management leads to intensification of result-based dysfunctional behaviours (gaming, unethical conduct) or reinforcement of coercive use of action controls, increasing stress and rule-breaking behaviours. Regulatory and market contexts often impose formal controls (e.g., compliance mandates, financial benchmarks) that may conflict with internal cultural values and challenge trust-based, open cultures.

Table 9: Contextual Factors Affecting Control Types

Contextual Factor	Description	Control Themes Affected
Task Uncertainty and Complexity	High task complexity or uncertainty increases the need for flexibility. Rigid controls tend to fail in such contexts, leading to stress or workarounds. Stable, simple tasks tolerate tighter control. Examples: Brownell & Hirst (1986); Abernethy & Stoelwinder (1995); Jaworski (1988); Davila (2000); Chenhall (2003)	Result (1), Action (2), Personnel (3), Design/use (6)
Cultural or Professional Norms	Organisational, national, or professional norms shape control acceptance. Misaligned controls provoke resistance or detachment. Examples: Riyono (1998); Weaver et al. (1999);	Action (2), Personnel (3), Cultural (4), Joint (5)
Leadership Style and Ethical Tone	Leaders' actions model how controls are interpreted. Ethical leadership enhances control legitimacy; unethical leadership undermines trust. Examples: Kaptein (2011); Weaver et al. (1999); Sorauren (2000)	Action (2), Personnel (3), Cultural (4), Joint (5), Design/use (6),
Organisational Structure	Fragmented or siloed structures foster control misalignment. Poor coordination leads to redundancy or contradictions. Examples: Ferreira & Otley (2009); Malmi & Brown (2008); Bedford (2020)	Cultural (4), Joint (5), Design/use (6)
External Pressures (Regulatory, Market, Crisis)	External demands intensify reliance on formal controls and may override internal values, triggering gaming or ethical erosion. Examples: Jensen (2003); Sponem & Lambert (2016); Goebel & Weißenberger (2017); Reason et al. (1998); Weaver et al. (1999)	Result (1), Action (2), Cultural (4), Joint (5), Design/use (6)

Source: Own work.

2.4.1 Managerial implications

Our framework highlights that mitigating control problems requires managers to focus not just on what control type is used, but how it is designed and used, and where (in what context) it operates. Many dysfunctional consequences can be traced to a misalignment between control mechanisms and the behavioural, cultural, or task-specific context in which they are applied. By minding the contextual conditions and addressing the underlying mechanisms, such as excess rigidity, poor value alignment, or lack of participation, organisations can mitigate many control problems. In line with many reviewed studies, practical implications thus include adding flexibility to rule-based systems, designing controls resonating with the prevailing culture, and involving employees in control design. But our findings also imply that this is far from an easy task. To avoid dehumanizing organizations (Lagios et al., 2023), managers must exercise careful judgement in deciding when and which rules should be strictly followed and when interpretative flexibility is more appropriate. Such judgement relies on emotional intelligence, social awareness, and a deep understanding not only of professional tasks but also of interpersonal dynamics. This view is supported also by Müller et al. (2025), who find that integrated use of levers of control can mitigate dysfunctional outcomes. Yet, such competencies are rarely formalized in decision-making procedures or extensively taught in traditional accounting or management education.

Moreover, in complex social systems, control is inherently bounded and unintended consequences are not just possible, but inevitable. Thus, a key managerial question is how to balance the intended and unintended consequences. When can unintended consequences be tolerated or ignored and when must they be actively managed? In cases where unintended outcomes do not significantly compromise the control's objective, they may be acceptable (e.g., minor symbolic compliance in non-critical tasks). But when such consequences undermine core goals (e.g., ethical conduct, financial integrity, or safety), they require deliberate and strategic mitigation. Drawing on the risk management logic, managers could treat dysfunctional control outcomes as behavioural risks to be anticipated, monitored, and mitigated rather than fully prevented. Similar to the aim of risk management, which seeks not to create risk-free conditions but to manage it within acceptable bounds (Power, 2007). Management control should anticipate, monitor, and mitigate dysfunctional outcomes rather than attempt to prevent them entirely. In some contexts (e.g., banking, aviation, healthcare), operational risk management systems already incorporate control-related behavioural risks (e.g., human error, policy circumvention). Such approaches could be adapted more broadly to flag and respond early to dysfunctional behaviours, for instance by monitoring the severity and frequency of unintended outcomes and intervening when they exceed acceptable thresholds.

Building on this logic, approaches increasing organizational adaptiveness and learning complement risk-based thinking. Rather than only preventing dysfunctions, organizations can also create conditions fostering serendipity, i.e. favourable unintended outcomes. Balzano (2022) argues that to increase serendipity, firms should adopt an adaptive paradigm

rather than rigidly executing predefined controls. This entails establishing warning systems that not only detect emerging problems but also continuously question whether existing MCS still operate as intended. Embedding such reflexive feedback loops encourage ongoing learning and ensures that control designs remain aligned with organizational goals and changing environmental conditions.

2.4.2 Future research agenda

These insights point to several future research directions. More work is needed to understand how managers perceive and balance trade-offs between intended and unintended control outcomes, and how context (e.g., organizational culture, industry norms, or regulatory environment) shapes the tolerance for unintended consequences. The intersection between risk management and behavioural control also deserves further investigation to help managers anticipate and respond to control failures systematically. In addition, future research might explore how judgment-based control, rooted in soft skills and interpretive flexibility, can be enabled or complemented by formal systems.

Our study reveals that results controls have received the most attention, while action and personnel controls remain comparatively underexplored. Future research could address this gap by empirically investigating the effects of these control types on behaviour over time. For example, longitudinal and experimental studies could examine how personnel controls (e.g., socialization practices) affect ethical decision-making or peer-monitoring in different contexts. Also, each identified mechanism (and their combinations) could be tested empirically to uncover the limits of their domains. Future research could also investigate more the interaction between different types of control, which also surfaced as an underexplored theme.

2.5 Conclusion

This literature review responds to calls for more clarity regarding control problems created by MCS. While earlier works such as Franco-Santos et al. (2012), Van Camp and Braet (2016), and Müller et al. (2025) offer broad typologies or focus on PMS more generally, our study specifically examines how distinct types of MCS; result controls, action controls, personnel controls, cultural controls, as well as their combinations, and their design and use, are linked to recurring dysfunctional behaviours. Drawing on a systematic literature review of 95 studies (published between 1956 – 2024), we offer an evidence-based mapping that connects control types to manifested control problems, such as gaming, data manipulation, ethical erosion, motivational crowding-out, and symbolic compliance.

Conceptually, we move beyond thematic categorization by identifying the underlying drivers and contextual moderators that influence when and why specific dysfunctions arise.

This yields a unifying framework that contributes both to theory development and to the design of more behaviourally resilient control systems.

A key contribution lies in identifying the mechanisms through which these control problems emerge. Recurring patterns such as excessive rigidity, contextual misfit, lack of participatory design, and symbolic use of controls are integrated into a conceptual framework that also accounts for key contextual moderators, such as task uncertainty, cultural norms, ethical leadership, external pressures, and organizational structure. Moreover, this chapter extends the literature on control packages and control system coherence by exploring how combinations of controls can reinforce or weaken behavioural alignment. This was especially salient in studies on multiple control systems (e.g., Bedford, 2020; Malmi & Brown, 2008), where fragmented or overlapping systems led to increased confusion, accountability gaps, and ethical ambiguity.

Like all review studies, this chapter faces certain limitations. One concern is the potential omission of relevant literature. To mitigate this, we employed broad search terms and accessed multiple databases. While we cannot fully exclude the possibility of having missed some relevant studies, we believe that any such omissions are unlikely to significantly alter our conclusions. A second limitation involves a certain degree of subjectivity in the coding process. We addressed this by using theoretically grounded coding schemes, clear working definitions of concepts, and limiting the number of emergent categories.

Despite these limitations, this review provides novel insights for both theoretical and practical advances in the field of MCS. It supports the development of more adaptive, coherent, and ethically grounded control systems by emphasizing the behavioural consequences of control design and use. Future research can build on this framework by empirically testing its propositions, addressing the identified gaps, and further exploring how managers navigate the balance between intended and unintended consequences of control.

3 WHEN CONTROLS CREATE RISK: A REVIEW OF CONTROL PROBLEMS UNDERLYING OPERATIONAL RISK IN BANKING[1]

3.1 Introduction

In recent years, banks have continued to incur substantial operational losses, illustrating that control failures remain a persistent source of financial and reputational damage. According to the European Banking Authority (2023), materialized losses from new operational risk

[1] This chapter is based on the article "When Controls Create Risk: A Review of Control Problems Underlying Operational Risk in Banking," accepted for publication in Dynamic Relationships Management Journal (DRMJ)

events in 2023 reached EUR17.5 billion, an increase of 27 % over 2022, with loss events rising by 3.7 %. The ORX Annual Banking Operational Risk Loss Data Report 2025 similarly reports that although aggregate loss volumes have declined to their lowest level in a decade, incidents driven by human error and control breakdowns remain widespread. Citigroup's USD 139 million trading loss caused by a "fat-finger" input error and Barclays' USD 1.5 billion data-entry failure are only recent reminders that operational risk continues to emerge from internal process, system, and behavioural weaknesses rather than from external shocks alone. These figures underscore that operational risk is far from diminishing and that a deeper understanding of control problems is essential to strengthen organizational resilience and governance in modern banking.

Driven by both recurring losses and the regulatory momentum of the Basel II and III Accords, financial institutions have intensified efforts to identify and mitigate operational risk arising from internal operations. Chapelle et al. (2004) emphasize that operational risk is endogenous to the organization, rooted in the complexity of processes, systems, and managerial quality. Weak internal controls have been repeatedly linked to high loss frequencies (Chernobai et al., 2011; Ferreira & Dickason-Koekemoer, 2019), while Raghavan (2003) associates major banking failures with control lapses and human misconduct. Although operational risk management (ORM) frameworks have matured substantially since Basel II, their focus has remained largely technical and compliance-driven, leaving limited understanding of how management control systems (MCS) contribute to the generation or mitigation of operational risk.

Early ORM research prioritized quantitative modelling and capital allocation (e.g., Cornalba & Giudici, 2004; Cruz et al., 1998; Fontnouvelle et al., 2005; Moosa, 2007; Power, 2005), with limited attention to the organizational mechanisms underpinning risk. Subsequent studies recognize that operational risk is inseparable from managerial behaviour, incentive design, and governance structures. Soin et al. (2020) identify deficiencies in risk culture and control integration as key sources of failure, while van den Tillaart et al. (2003, p. 141) argue that operational risk "can best be managed within the domain of management control," where behaviour and decision-making are shaped by control practices. This insight has broadened the view of operational risk from a purely statistical construct to a managerial and behavioural phenomenon embedded in control systems.

Over the past two decades, risk management has evolved from a specialized financial discipline into an integral component of management control (Arena & Arnaboldi, 2014; Lueg & Knapik, 2016; Merchant & Otley, 2006; Mikes, 2009; Peljhan et al., 2018; Soin & Collier, 2013). Building on Anthony's (1965) foundational definition of MCS as "the process by which managers assure that resources are obtained and used effectively and efficiently in the accomplishment of organizational objectives" (p. 17), Merchant and Van der Stede (2017) proposed the *Object of Control Framework*, which distinguishes four types of control: result, action, personnel, and cultural, each addressing distinct behavioural mechanisms. This framework provides a comprehensive foundation for examining how the

design and **use** of controls influence organizational behaviour, learning, and performance. In the banking context, where systems are heavily shaped by regulation and hierarchy (Rad, 2016), the persistence of operational losses despite sophisticated formal control infrastructures suggests that risk emerges not only from system failures but from the ways in which controls are conceived, implemented, and enacted.

The global financial crisis of 2008 renewed attention to the behavioural underpinnings of control and risk. Post-crisis reforms strengthened governance, reporting, and compliance frameworks, yet the persistence of control-related losses demonstrates that technical refinements alone are insufficient. This calls for a more integrative perspective, one that views operational risk management as embedded within broader systems of managerial control and organizational behaviour. Understanding *how* control problems emerge within these systems and *through which mechanisms* they shape operational outcomes is therefore critical for explaining why formally robust control architectures continue to produce unexpected failures.

To address this gap, this study systematically reviews the literature on management control systems and operational risk management in the banking sector. Drawing on Merchant and Van der Stede's (2017) Object of Control Framework, it categorizes and synthesizes evidence on how control problems influence operational risk. The review is guided by two overarching research questions:

RQ1: How do management control problems emerge within the design and use of control systems in the context of operational risk management?

RQ2: Through which organizational and behavioural mechanisms do these control problems shape operational risk outcomes in banking institutions?

In this chapter, a systematic review of literature from 1995 to 2025 is conducted to examine how management control systems relate to operational risk in banking. The chapter begins by outlining the theoretical foundations that link management control and operational risk, clarifying the relevant concepts and positioning the study within existing research. The methodology applied in the review is then presented, followed by a structured synthesis of the selected literature. The final part of the chapter provides a discussion of the reviewed evidence, highlighting its relevance for understanding how management control systems function within operational risk contexts.

3.2 Theoretical Background: Management Control and Operational Risk

A deeper understanding of how management control problems shape operational risk requires an integrated theoretical foundation that links the fields of management control systems (MCS) and operational risk management (ORM). Both domains address how organizations seek to influence behaviour, ensure accountability, and manage uncertainty.

However, they have evolved largely in parallel, with MCS developing within management accounting and organizational control, and ORM developing within banking regulation and financial risk governance. This section therefore establishes the conceptual bridge between the two, defining the core constructs examined in the review, outlining what is already known about their relationship, and identifying the unresolved issues that motivate further inquiry.

MCS are traditionally defined as mechanisms for directing employee behaviour toward the achievement of organizational objectives, ensuring coordination and accountability (Anthony, 1965; Malmi & Brown, 2008; Simons, 1995). Over time, this instrumental view has broadened to include the behavioural and organizational dimensions of control, acknowledging that control systems can both enable and constrain performance. While control systems are intended to enhance effectiveness, a growing body of literature shows that they can also generate unintended and dysfunctional outcomes. Merchant and Van der Stede (2012) define such *control problems* as situations arising from lack of direction, motivational issues, or personal limitations, leading to behaviours such as gaming, budgetary slack, or manipulation of key indicators. These behaviours not only distort performance measurement but also affect how organizations perceive and manage risk. In this sense, the behavioural dimension of control becomes crucial for explaining persistent control failures within highly regulated sectors such as banking.

ORM, by contrast, emerged from financial regulation, particularly Basel II (BCBS, 2006), which established a systemic framework for identifying, assessing, and mitigating risks arising from internal processes, people, and systems. While its early development focused on measurement and capital adequacy, subsequent research (Mikes, 2009, 2011; Power, 2005, 2009) highlighted that operational risk is also behavioural and cultural in nature, shaped by how formal control systems are designed and enacted. ORM therefore represents both a technical and a behavioural system. Conceptually, ORM can be understood as a component of broader management control, interacting with the same design principles, behavioural drivers, and organizational dynamics that characterize traditional MCS.

To analyse how control problems become operationally relevant in banking, the review organises the literature into four manifestation domains: rules and procedures, structure and governance, incentives, and culture. These domains are informed by Merchant and Van der Stede's OOC framework, but they are not intended as one-to-one equivalents of the original control types. Rather, they capture the principal organisational arenas in which control problems become visible within operational risk management. Rules and procedures often reflect action-control-related issues, incentives commonly relate to result-control tensions, and culture aligns closely with cultural control. Personnel control remains part of the underlying theoretical lens, but in the ORM literature it is reflected more broadly through issues such as capability, training, role clarity, and staffing conditions. These issues often interact with structure and governance arrangements that shape how personnel-related controls are implemented in practice. By synthesising and presenting the empirical findings

through these manifestation domains, the review examines how control problems identified in Chapter 2 translate into operational risk vulnerabilities in banking. This shift from control types to manifestation domains reflects the way operational risk is documented and analysed in banking practice, where control problems are observed through organisational processes and governance arrangements rather than through abstract control categories.

Table 10 summarises the manifestation domains used to structure the review and illustrates how different organisational arenas in banking ORM are associated with distinct types of control problems.

Table 10: Manifestation Domains of Management Control Problems in Operational Risk Management

Manifestation domain in ORM	Relation to OOC control types	Observable indicators of control problems in ORM
Rules and Procedures	Mainly associated with action controls	Rigid procedures, excessive formalisation, limited discretion, checklist compliance, procedural overload, weakened judgment
Structure and governance	Organisational conditions shaping the implementation and enactment of multiple control types	Unclear responsibilities, fragmented reporting lines, coordination failures, segregation-of-duties tensions, weak escalation channels, governance arrangements
Incentives	Primarily associated with result controls	Target pressure, reward misalignment, short-termism, performance bias, risk-taking, concealment
Cultural Controls	Closely related to cultural controls	Weak ethical climate, symbolic compliance, normalisation of deviance, low speak-up behaviour, weak learning

Source: Own work.

Together, these control types form a holistic architecture for influencing conduct and reducing uncertainty. Yet each can also become a source of dysfunction. Overly rigid action controls may stifle innovation and judgment (Gurd & Helliar, 2017), misaligned result controls can encourage excessive risk-taking (Acrey et al., 2011), weak personnel controls may lead to fatigue or skill mismatches, and fragile cultural controls can erode ethical awareness (Cohn et al., 2014; Lui, 2015). These dysfunctional tendencies help explain why control problems become visible in different organisational arenas within banking ORM.

Existing literature demonstrates that MCS and ORM share the fundamental purpose of aligning individual behaviour with organizational objectives and managing performance under uncertainty. ORM offers the risk infrastructure, rules, procedures, and escalation processes, while MCS provides the behavioural infrastructure, such as incentives,

accountability, and cultural reinforcement. When these systems are coherent and mutually reinforcing, they create a resilient organizational control environment. However, a number of studies show that misalignment between them can undermine both performance and resilience. Arena et al. (2010), Mikes (2011), and Soin and Collier (2013) highlight that risk management systems often generate information that fails to influence decision-making when incentive structures reward short-term financial outcomes over prudent risk behaviour. Similarly, Lim et al. (2017) demonstrate that diagnostic use of risk controls and hierarchical communication barriers limit learning, while Rad (2016) finds that regulatory templates imposed from above frequently misfit local process logic, producing redundancy and fragmentation. More recent work by Ringgaard et al. (2025) illustrates that boundary and belief systems can strengthen ORM effectiveness only when interactively used, suggesting that the way controls are enacted may be as important as their formal design.

Complementary insights arise from internal control and governance research. Abdul Rahim et al. (2018) show that risk assessment and monitoring activities significantly enhance perceived ORM effectiveness, whereas Chernobai et al. (2020) provide large-sample evidence linking operational losses to weaknesses in internal governance and oversight. Studies in emerging economies, such as Siaw Ofori et al. (2025), further demonstrate that board expertise and independence contribute to risk resilience, while Butler and Brooks (2024) call for an integrative approach that combines governance, culture, and control perspectives. Taken together, this literature shows that operational risk emerges not only from technical system flaws but from behavioural dynamics embedded within organizational control environments.

Despite these advances, significant gaps remain. Research on MCS and ORM remains conceptually fragmented, with the two systems often treated as distinct domains, one managerial, and the other regulatory, rather than as interdependent layers of control. The behavioural dimension of operational risk is still under-specified; while dysfunctions such as gaming or symbolic compliance are acknowledged, few studies trace *how* these arise from the design or use of specific control mechanisms. Finally, the contextual particularities of banking, including its strong regulatory oversight, information asymmetries, and layered governance, remain under-theorized as drivers of control problems. Addressing these gaps requires an integrative approach that combines the behavioural richness of MCS theory with the institutional insights of ORM research.

An important but often overlooked aspect of this banking context is the internal heterogeneity of the sector. Banking should not be treated as a uniform setting, as different banking activities involve distinct business models, risk profiles, organisational structures, and externalities for the real economy. In particular, the distinction between commercial banking and investment banking is conceptually important. Commercial banking is primarily centred on deposit-taking, lending, and payment services, whereas investment banking is more strongly associated with underwriting, trading, market-making, and other market-based activities (Greenbaum et al., 2019). These differences matter not only because

they imply different financial risks, but also because they shape the control environment, the role of discretion, the nature of performance pressures, and the forms through which control problems may emerge (Greenbaum et al., 2019; Mikes, 2009).

These differences extend beyond business activities to organisational culture and risk-taking behaviour. Market-based banking activities are typically associated with stronger performance pressures, greater exposure to calculative risk-taking logics, and more intensive use of market-based incentives, whereas commercial banking is more closely linked to operational reliability, process discipline, and continuity in customer relationships (Mikes, 2009). More broadly, prior literature suggests that risk culture in banks is closely intertwined with management control arrangements, indicating that differences in organisational setting and control environment are likely to affect how risk is interpreted, communicated, and governed across banking activities (Kunz et al., 2021). As a result, control environments differ across banking activities, including the role of discretion, the intensity of performance pressures, and the way in which risk is perceived, managed, and normalised within the organisation.

The externalities associated with these activities also differ. Disruptions in commercial banking primarily affect credit provision, payment systems, and the functioning of the real economy, whereas failures in investment banking are more closely linked to market instability, leverage cycles, and risk transmission through financial markets (Greenbaum et al., 2019). These differences imply that the relationship between management control systems and operational risk management cannot be assumed to be uniform across banking contexts. Instead, variations in business models, incentive structures, and organisational environments are likely to shape how control systems are designed and used, and how control problems translate into operational risk outcomes (Greenbaum et al., 2019; Kunz et al., 2021; Mikes, 2009).

Against this backdrop, this study responds to that need by linking the OOC to ORM. It interprets operational risk as a manifestation of management control problems and categorizes these problems into five interrelated domains: design and use, rules, structure, incentives, and culture. Through this synthesis, the review contributes to a more holistic understanding of why control systems intended to ensure stability and compliance can, under certain conditions, become sources of rigidity, misalignment, and behavioural drift. By examining the interplay between formal control architectures and human behaviour, the study seeks to explain how management control problems shape operational risk outcomes in the banking sector and why they persist despite increasingly sophisticated risk management systems.

3.3 Method

3.3.1 Research Design

Given the fragmentation and disciplinary dispersion of research on MCS and ORM, a systematic literature review was undertaken to consolidate and critically synthesize existing evidence. This approach provides methodological transparency, reproducibility, and analytical rigor while allowing integration across theoretical and empirical traditions (Denyer & Tranfield, 2009; Tranfield et al., 2003). It is particularly appropriate for examining complex, multi-level constructs such as MCS and ORM, where research spans accounting, management, and regulatory domains.

The review encompassed peer-reviewed academic publications, working papers, and institutional or regulatory sources (e.g., Basel Committee, European Banking Authority, Financial Stability Board, ORX). Including both scholarly and institutional materials was essential, as ORM in banking is not only an academic topic but also a highly regulated practice (Power, 2005; Soin & Collier, 2013). This inclusive design aligns with Denyer and Tranfield's (2009) recommendation for systematic reviews of practice-oriented domains and enables triangulation between theoretical, empirical, and institutional perspectives to support a holistic understanding of how control design and use interact with operational risk governance.

3.3.2 Search and Selection Strategy

Although the review employed a systematic search strategy to identify and screen the focal body of literature, it did not rely on keyword retrieval alone. Because the dissertation examines operational risk in banks through a management control systems (MCS) lens, the review was also anchored in seminal background literature from this theoretical domain. Foundational works such as Anthony (1965), Simons (1995), Otley (1999), Malmi and Brown (2008), and Merchant and Van der Stede (2017) were used to define the conceptual boundaries of control and to guide the theoretical structuring of the review. In the ORM domain, the review was grounded in prudential regulatory frameworks that define and structure ORM in banking, particularly Basel II and III, complemented by literature examining how risk management practices are organised and governed within firms, including Power (2005, 2009), Mikes (2009, 2011), and Kaplan and Mikes (2012), which informed the interpretation of the behavioural and organisational dimensions of risk control. In addition, relevant banking literature was incorporated to capture the sector-specific characteristics of banks as a research context. In the banking domain, foundational and contextual works such as Diamond and Dybvig (1983), Diamond (1984), Greenbaum et al. (2019), Berger and Boot (2024), which provides an authoritative synthesis of the theoretical foundations of financial intermediation and bank fragility, informed the treatment of banks as a distinct research context. The review was therefore systematic in its article identification

and screening procedures, but theory-driven in its conceptual framing and synthesis. This combination reduced the risk that a purely keyword-based search would overlook foundational contributions that do not always appear under the exact search terms, while still preserving the transparency and replicability expected of a systematic literature review.

The literature search itself was conducted across Scopus, Web of Science, and ScienceDirect, supplemented by Google Scholar and citation tracking to identify additional relevant studies and institutional publications. This ensured comprehensive coverage and reduced database bias.

The search strings, documented in Table 11, were iteratively developed to capture conceptual overlaps between MCS and ORM, combining terms such as *"management control system," "internal control," "risk management system," "operational risk," "behavioral control," "risk culture,"* and *"banking sector."* A representative Scopus query was:

("management control system" OR "internal control system" OR "organizational control") AND ("operational risk" OR "risk management" OR "risk governance") AND ("bank" OR "financial institution").

Table 11: Search Strategy

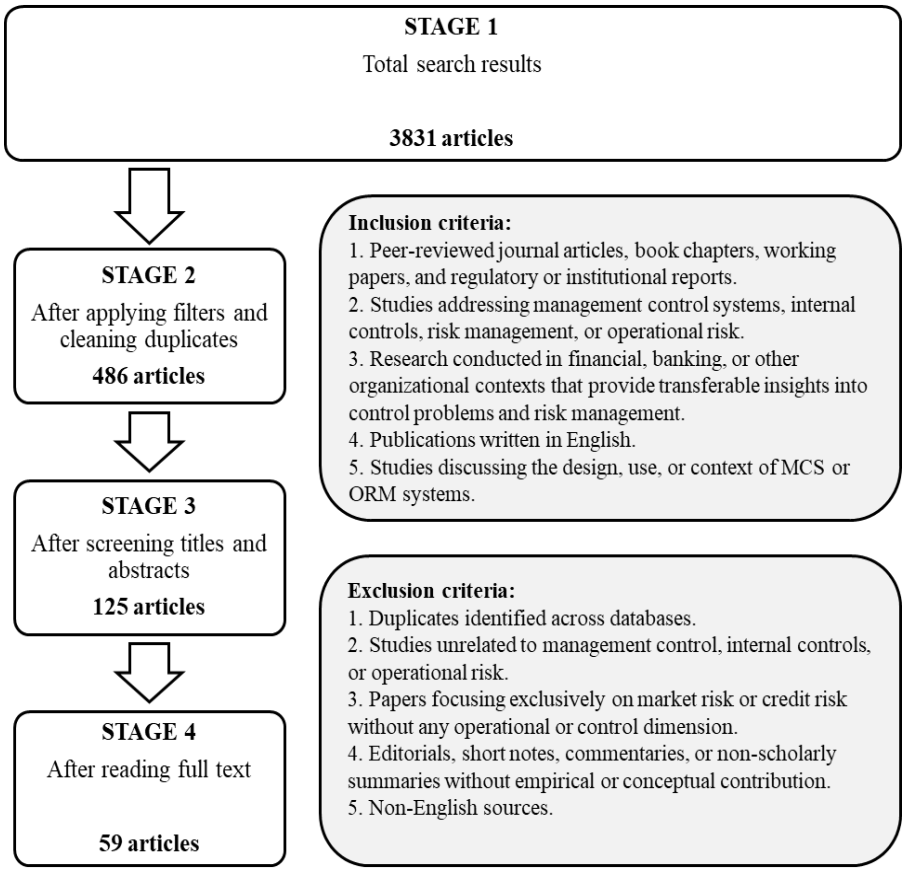
Database	Search String	Results retrieved	Results after filters
Scopus-Elsevier	(TITLE-ABS-KEY (Management control system) AND TITLE-ABS-KEY (Operational Risk) AND TITLE-ABS-KEY (bank) (TITLE-ABS-KEY (Management control system) AND TITLE-ABS-KEY (Operational Risk) AND TITLE-ABS-KEY (behavioral risk) AND TITLE-ABS-KEY (bank) (TITLE-ABS-KEY (Operational risk) AND TITLE-ABS-KEY (behavioral risk) OR TITLE-ABS-KEY (people risk) AND TITLE-ABS-KEY (bank)	1881	162
Science Direct	Management Control System AND Operational Risk Management Control System AND Operational Risk Management AND people risk in banking Operational Risk Management AND people risk in banking	1032	104
Web of Science	TS=((Management Controls * AND Operational risk *) AND banking* TS=((Operational Risk * AND People risk *) AND banking* TS=(Operational Risk * AND Counterproductive work behavior *) AND banking	918	220
	Total	**3831**	**486**

Source: Own work.

Searches were performed between January and July 2025, covering the literature published in the period 1995–2025. This range aligns with the institutionalization of operational risk under Basel II (2004) and the growing behavioural orientation in MCS research (Merchant & Van der Stede, 2003–2017; Simons, 1995). To ensure methodological transparency and replicability, the process followed the PRISMA stages of identification, screening, eligibility, and inclusion (summarized in Figure 4). Inclusion criteria required that studies (a) addressed MCS, internal controls, or ORM; (b) were empirical or conceptual works providing insights into control design, use, or behavioural consequences; and (c) were written in English. Studies focusing exclusively on market or credit risk, lacking conceptual or empirical contribution, or consisting of non-scholarly commentary were excluded.

The initial database search yielded 3,831 records. After removing duplicates, 486 unique studies remained for preliminary screening. Titles and abstracts were subsequently reviewed, resulting in 125 papers that met the eligibility criteria for full-text assessment. Following comprehensive reading and evaluation, 59 publications were retained for final synthesis and coding.

Figure 4: Study Selection Process



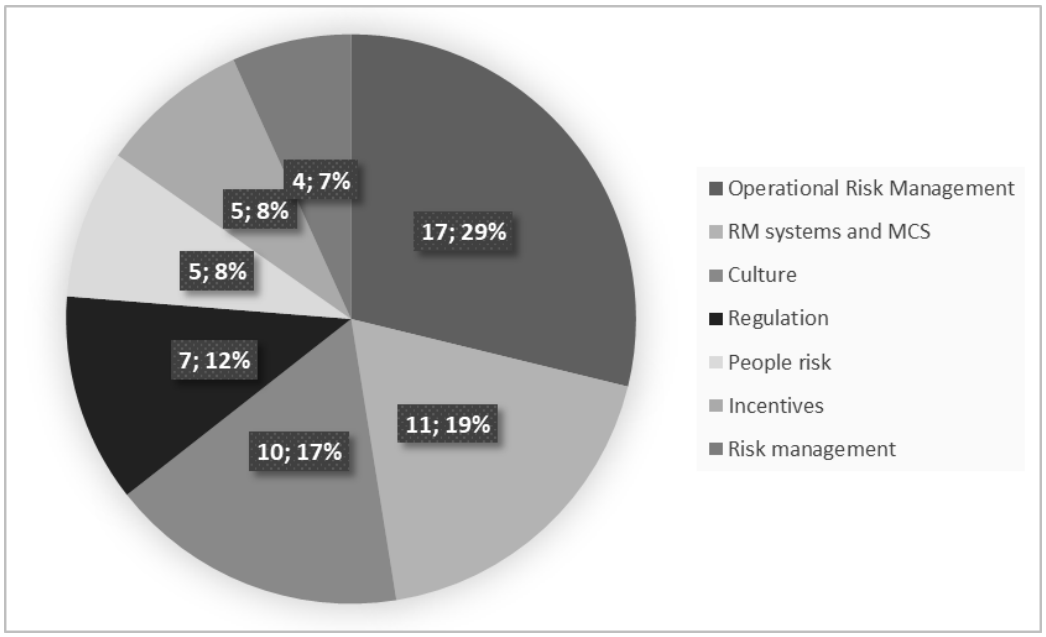
Source: Own work.

3.3.3 Data Analysis and Synthesis

All retained studies were coded manually using a structured framework adapted from Merchant and Van der Stede's (2017) OOC framework and by the mechanism-based insights developed in Chapter 2. Each publication was examined to identify (1) the aspect of ORM addressed (design, use, or organisational context), (2) the manifestation domain in which control problems became visible (rules and procedures, structure and governance, incentives, or culture), (3) the control problem mechanism reported in the study (e.g., misalignment, rigidity, fragmentation, behavioural bias), and (4) the operational risk consequence (e.g., process failure, human error, loss event). Coding categories were informed by prior syntheses of MCS–risk research (Arena et al., 2010; Mikes, 2009; Soin & Collier, 2013) and refined through iterative cross-comparison to ensure consistency and internal validity.

Among the 59 papers retained for analysis, 17 focuses specifically on operational risk management and 4 address risk management more broadly; 7 examine regulatory aspects, 11 explore operational risk management systems within the broader management control framework, 10 adopt a cultural perspective on risk, 5 investigate people or behavioral risk, and 5 analyze incentives-related risk (Figure 5).

Figure 5: Distribution of main topics in the retained records (n= 59)



Source: Own work.

A qualitative thematic synthesis approach was used to integrate findings across studies, focusing on how control problems identified in Chapter 2 become translated into ORM vulnerabilities in banking. Five overarching analytical dimensions guided the synthesis and presentation of findings (see Appendix 4):

Design & Use – how control systems and ORM arrangements are configured and how are they enacted or interacted in practice by managers

- Rules – formal procedures and compliance requirements embedded in ORM.
- Structure – organizational arrangements and governance layers affecting control.
- Incentives – behavioural drivers shaping control effectiveness and risk behaviour.
- Culture – cultural drivers shaping control effectiveness and risk behaviour.

These dimensions were used as manifestation domains through which control problems become visible in banking ORM, rather than as one-to-one substitutes for the OOC control types. Analytical attention centred on recurrent dysfunctions that contribute to operational risk exposure such as information silos, compliance-driven rigidity, and incentive misalignment (Butler & Brooks, 2024; Power, 2009). Rather than merely aggregating results, we aimed to uncover causal and conceptual linkages between management control dysfunctions and operational risk. This process produced an integrative conceptual mapping that explains how management control problems give rise to operational risk in banking organizations.

The next section presents the results of this synthesis, outlining the key conceptual patterns and relationships identified across the reviewed studies.

3.4 Findings

Building on the mechanisms identified in Chapter 2, the findings presented in this section examine how these mechanisms become operationally relevant within the banking context. The findings are organized based on different organisational arenas in which these mechanisms become visible within operational risk management.

3.4.1 Design and Use Issues

Design and use issues represent one of the principal manifestation domains through which control problems become operationally relevant in banking. Building on Chapter 2, this domain captures how recurrent mechanisms such as rigidity, design–use misalignment, symbolic use, and learning deficits become embedded in the formal architecture and day-to-day enactment of ORM. The *design* of MCS refers to formal architecture through which organizations establish structures, procedures, and mechanisms to direct behavior and align risk-taking activities with strategic and regulatory objectives. In contrast, the *use* dimension concerns how these systems are enacted, interpreted, and practiced in day-to-day operations. Together, they determine whether control systems act as instruments for learning and resilience or as rigid compliance mechanisms.

Our review identified 21 studies examining the design and use of risk management systems, including both general frameworks and systems specifically focused on operational risk. In this context, design of ORM systems denotes the configuration of control elements that determine how operational risks are identified, measured, and mitigated. Design issues therefore concern the adequacy, integration, and coherence of systems governing risk identification, internal controls, and oversight structures (Arena et al., 2010; Soin & Collier, 2013). Effective design translates regulatory requirements into actionable routines that enhance control reliability, whereas poor design generates gaps, redundancies, or rigidity that heighten risk exposure. By contrast, the use dimension concerns how control systems are enacted in practice. Simons (1995) conceptualizes the *use* of control systems through the Levers of Control framework, distinguishing between diagnostic, interactive, beliefs, and boundary systems. In the ORM context, these uses shape how managers engage with risk information. Control systems may be applied diagnostically to monitor compliance, or interactively to stimulate dialogue, learning, and adaptive responses to emerging risks.

Empirical studies reveal that the design of ORM in banking frequently struggles to *balance regulatory compliance with managerial discretion*. Power (2005) provides a foundational critique, arguing that the post-Basel II operational risk framework institutionalized a "control of control" mentality that prioritized documentation over learning. His analysis shows that the design logic favoured formal accountability and quantification, but at the expense of behavioral engagement. This "design bias" toward auditable systems produced an illusion of control that paradoxically weakened risk awareness a theme echoed in later research by Mikes (2009, 2011), who distinguishes between calculative and enabling control configurations. In her ethnographic studies of major international banks, Mikes finds that design choices embedded in calculative cultures marginalize interpretive judgment and learning. These configurations create silos between risk experts and operational managers, inhibiting communication and producing latent vulnerabilities in risk reporting and escalation processes. Moreover, Berger et al. (2022) show that operational risk losses are not isolated firm-specific events but systemically interdependent phenomena, partly due to correlated exposures across institutions due to shared operational infrastructures, business practices, and regulatory environments.

Risk management evolved through multiple disconnected domains (insurance, financial, operational, environmental, cyber, supply chain) and regulatory frameworks (COSO, ISO, Basel, FERMA), resulting in fragmented practices (Molamohamadi et al., 2024). Soin and Collier (2013) show that MCS design in financial institutions reflects competing institutional logics, regulatory compliance, market performance, and internal governance each shaping the control structure. Their study of UK banks finds that integration of risk management and management accounting was undermined by *fragmented system design*. Intended to enhance transparency, this fragmentation instead generated inconsistent information flows and diffused accountability. The resulting control failures (i.e., information distortion, duplication of oversight, and diffusion of responsibility) represent classic symptoms of

structural fragmentation as a design flaw. Muermann and Oktem (2002) similarly find that weak feedback and integration among ORM elements leads to "missed learning opportunities" and recurring errors. Rad (2016) extends this reasoning, finding that system misalignment between risk management functions and operational departments weakens control reliability. Because risk management systems were designed around regulatory templates rather than internal process logic, they became rigid and poorly adapted to the operational context a form of procedural rigidity that limited continuous improvement and responsiveness to emerging risks. Xu et al. (2017) further demonstrate that operational risk persists when process designs (technical and procedural) fail to align with human factors, incentives, and behavioral reliability, creating vulnerabilities in inspection, maintenance, and decision making and manifesting as human error, moral hazard, or capacity failure.

Weaknesses in control design also manifest in internal control system architecture. Abdul Rahim et al. (2018) show that while internal control design positively influences perceived ORM effectiveness, the *absence of comprehensive control mapping and feedback mechanisms* constrains risk learning. Their survey of Malaysian banks shows that preventive controls dominate (e.g., authorization procedures, segregation of duties), while detection and corrective design features are often underdeveloped. This imbalance between compliance assurance and performance insight reduces responsiveness to control failures and delays mitigation. Chernobai et al. (2022) show how increased business complexity overwhelms control system's design (and use) leading to ineffective operational risk controls. Similarly, Florio and Leoni (2017) note that Enterprise Risk Management (ERM) design in Italian financial institutions tends to prioritize measurement tools over strategic coordination. This technocratic orientation creates a disconnect between risk data and managerial action, reducing the ability of designed systems to translate risk information into operational decisions. Göstl and Schwaiger (2016) add that the integration of risk-based planning into MCS depends on how effectively risk information feeds into budgeting and performance evaluation; fragmented design prevents such information from influencing strategic choices, revealing persistent integration failures at the design level.

The *use* of MCS further determines whether these systems enhance or impair operational risk management. Several studies (Lim et al., 2017; Ringgaard et al., 2025; Slapničar et al., 2025) show that the operational use of control systems often leads to procedural rigidity, where *frameworks become overly bureaucratic and constrain professional judgment*. Lim et al. (2017) document paradoxes in risk management practice: front-line employees comply with the "three lines of defense," yet over-standardization discourages proactive learning. Ringgaard et al. (2025) observe that risk managers rely heavily on diagnostic controls to demonstrate compliance rather than to stimulate dialogue about emerging risks. Deschamps (2019) also finds that lower-level managers progressively tighten performance boundaries to ensure predictability, which can turn diagnostic systems into rigid or coercive tools that undermine empowerment and learning. In the cyber-risk context, Slapničar et al. (2025) find that the use of quantitative indicators creates an illusion of control, masking uncertainties

and reinforcing rule-based, rather than adaptive, behaviors. These findings indicate that when control use becomes compliance-driven, it erodes an organization's ability to manage complex, evolving operational threats.

Power (2009), Mikes (2011), and Soin and Collier (2013) further argue that risk management practices are often decoupled from broader management control routines. Power (2009) describes the use of ORM systems as a "ritual of verification," emphasizing *documentation over reflection*. Mikes (2011) contrasts calculative cultures, reliant on quantitative models, with enabling cultures that promote interpretive dialogue and collective sensemaking. When these approaches are not integrated, risk information remains technical rather than strategic, producing learning deficits. Hall et al. (2015) highlight that tensions between risk managers and other functional experts (finance, business units) can be resolved if RM tools are designed to support communication between them. Soin and Collier (2013) similarly conclude that unless MCS use bridges functional silos and embeds risk thinking into performance discussions, ORM frameworks remain detached from strategic decision-making. Recent work by Marc, Arena, and Peljhan (2023) highlights that the interactive style of MCS use can substantially improve RM effectiveness. Their study shows that when MCS are used interactively, i.e. facilitating discussion, information exchange, and mutual learning across departments, they enhance risk awareness, foster shared accountability, and reduce behavioral defensiveness. Interactive use transforms control from a compliance exercise into a learning mechanism, integrating risk dialogue into strategic and operational decision-making. Ringgaard et al. (2025) also emphasize that the design orientation (diagnostic versus interactive) determines whether ORM systems evolve as dynamic, adaptive tools or static compliance artifacts.

Collectively, these studies converge on a critical insight: the design and use of MCS are interdependent dimensions shaping the effectiveness of operational risk management. Formal design establishes the structural backbone of control, but its practical value depends on how managers and employees use these systems in daily operations. Design flaws such as fragmentation, rigidity, and misalignment can be amplified when controls are used diagnostically and bureaucratically. Conversely, interactive and integrative use can compensate for design weaknesses by fostering reflexivity, open communication, and cross-functional coordination. Effective ORM, therefore, depends not only on the technical design of systems but also on their enactment as behavioral and learning mechanisms. The literature underscores that banks seeking operational resilience must move beyond compliance-oriented architectures toward adaptive control environments where design and use operate in synergy to support both performance and risk awareness. Across studies, a consistent picture emerges: MCS in banks are often *designed* for external assurance yet *used* in ways that narrow learning.

3.4.2 Rules and Procedure Problems

The reviewed literature identifies rules and procedure problems as one of the most persistent manifestation domains through which control problems become operationally relevant in banking, appearing in 13 studies included in the review. Building on Chapter 2, this domain captures how mechanisms such as rigidity, symbolic compliance, fragmentation, and behavioural resistance become embedded in regulatory frameworks, internal procedures, and risk management policies. Although such procedures are designed to enhance control, compliance, and accountability, the literature shows that they can also become overly prescriptive, bureaucratic, or disconnected from actual operational realities.

Empirical and conceptual studies consistently show that while formalization of risk procedures can improve accountability and standardization, excessive reliance on rules leads to rigidity, reduced adaptability, and weak organizational learning (Lim et al., 2017; Moosa, 2017; Power, 2005; Ringgaard et al., 2025). Four recurring issues emerged from the review: compliance-driven control, overregulation, fragmentation of rules, and behaviooural response to the perception of control.

Compliance-driven issues are mentioned by several studies (e.g., Bardoscia & Bellotti, 2012; Florio & Leoni, 2017; Mabwe et al, 2022). Lim et al. (2017) document paradoxes in the implementation of risk management procedures within large banks. Their study of the Three Lines of Defense model reveals that compliance requirements, while designed to clarify accountability, often create an overly formalistic system that discourages professional judgment and innovation. Risk officers tend to focus on procedural compliance to demonstrate adherence to regulation rather than to foster proactive risk identification. Similar findings are observed by Ringgaard et al. (2025), who show that diagnostic use of MCS produces a "checklist mentality," limiting managerial discretion and reinforcing procedural rigidity. Together, these studies highlight how rigid procedural frameworks though central to regulatory credibility may unintentionally inhibit adaptive operational risk management. Moreover, Power (2009) and Soin and Collier (2013) illustrate how procedural frameworks may be decoupled from the actual management of risk. Power (2009) notes that operational risk management evolved into a symbolic process in which banks demonstrate compliance to satisfy external regulators rather than to inform internal learning. Soin and Collier (2013) reinforce this observation, finding that control procedures are often "performed for legitimacy" rather than used to guide managerial decision-making. These findings reveal that when rules dominate practice, they lose their enabling character and become obstacles to reflexive risk management.

This typically leads to *overregulation issues*. Moosa (2017) offers a critical view of how "bad regulation" can distort operational behavior in banks. His analysis differentiates between good regulation, which enhances transparency and discipline, and bad regulation, which imposes excessive procedural layers without improving actual control effectiveness. Overregulation leads to the diversion of managerial effort from substantive risk management

to documentation and reporting. Power (2005) similarly argues that the emergence of operational risk as a regulatory category under Basel II fostered a ritual of verification a tendency to institutionalize control through paperwork rather than genuine risk insight. Both studies demonstrate that procedural expansion, intended to manage uncertainty, often amplifies it by promoting symbolic rather than substantive control. Rikhardsson et al. (2021) further show that during crises, managers frequently redesign control systems reactively to restore order and legitimacy, a process that initially enhances coordination but gradually reinforces formalization and contributes to overregulation.

Fragmentation of rules due to decentralization intensifies this. Several studies emphasize the disconnection between risk procedures at the corporate and operational levels. In their comparative study of banks, Rad (2016) finds that the translation of formal risk-control procedures into daily practices is uneven, reflecting tensions between headquarters and branch-level interpretations. This fragmentation of procedural ownership undermines coherence and weakens feedback loops essential for effective operational risk mitigation. Similarly, Sabanova and Kudinska (2022) show that when rule systems are inconsistently applied, operational staff struggle to integrate compliance obligations with the realities of customer-facing work, resulting in procedural overload and increased error probability.

Behavioral response to perception of control is another issue highlighted by reviewed studies. While procedures are intended to reduce discretion and cognitive bias (Ranjan, 2025), their practical use depends on individual interpretation and behavior. Studies such as Mabwe et al. (2022) and Gurd and Helliar (2017) show that even well-designed control procedures can fail if employees perceive them as punitive or irrelevant. In the UK banking context, Mabwe et al. (2022) find that employees often comply with people-risk policies superficially, prioritizing procedural completion over substantive understanding. Gurd and Helliar (2017) emphasize that interactive leadership encouraging dialogue around rules can transform procedural systems from coercive to enabling, improving their impact on operational resilience.

Across the literature, rules and procedure problems represent a central manifestation domain through which management control systems influence operational risk outcomes. The reviewed studies show that mechanisms identified in Chapter 2, particularly rigidity, symbolic use, fragmentation, and constrained discretion, become amplified in banking when procedures are extended beyond their enabling purpose and enacted primarily as compliance devices. Excessive procedures lead to rigidity, detachment from practice, and a proliferation of symbolic compliance activities. Conversely, studies highlight that enabling procedures those allowing managerial discretion, feedback, and adaptation can strengthen the learning and responsiveness of operational risk systems. The evidence suggests that banks face a delicate balance: controls must satisfy regulatory expectations while remaining sufficiently flexible to address evolving operational threats. In this sense, the reviewed literature collectively underlines that the challenge of operational risk management lies not in the absence of rules but in their overextension and ritualised use.

3.4.3 Structural and Governance Problems

Across 16 studies in the review, structural and governance problems emerge as a major manifestation domain through which control problems become operationally relevant in banking. Building on Chapter 2, this domain captures how mechanisms such as fragmentation, misalignment, weak coordination, and constrained communication become embedded in organisational hierarchies, reporting arrangements, and governance structures. These problems concern the configuration of authority, communication flows, and functional divisions that shape how management control systems operate across the institution. When structures are fragmented, overly centralised, or poorly coordinated, control systems fail to integrate information effectively, resulting in misaligned risk ownership, weak escalation, and reduced oversight. The literature consistently demonstrates that even well-designed controls can lose effectiveness when embedded within structurally inefficient or siloed organizations (Cornwell et al., 2023; Mabwe et al., 2022; Soin & Collier, 2013). Five recurring issues emerged from the review: excessive fragmentation, unclear boundaries, excessive centralization, disconnection from governance structures, and clashes with cultural or behavioral norms.

Excessive fragmentation is mentioned by numerous studies. A recurrent theme across studies is the persistence of structural silos that isolate risk management from other managerial functions (e.g., Al-Amri & Davydov, 2016; Butler & Brooks, 2024). Soin and Collier (2013) show that in many banks, risk management and management accounting operate as parallel systems, leading to a lack of integrated information flows. This fragmentation undermines both strategic learning and operational responsiveness. Similarly, Cornwell et al. (2023) document how modernization efforts in ORM have not resolved the underlying fragmentation between business lines, risk functions, and internal audit. The separation of risk ownership among departments results in duplication, inconsistent data interpretation, and uncoordinated responses to emerging risk events. The authors argue that this form of structural misalignment prevents risk frameworks from functioning as integrated control mechanisms and weakens the coordination needed for effective operational risk management.

Unclear boundaries between units are often a consequence of fragmentation. The Three Lines of Defense (3LoD) model, designed to clarify responsibilities between business units, risk management, and internal audit, often fails in practice due to unclear boundaries and ineffective coordination. Lim et al. (2017) find that the practical application of 3LoD leads to overlapping mandates and confusion about accountability. This structural ambiguity weakens communication between lines, resulting in both redundancy and control gaps. Mabwe et al. (2022) further report that coordination between human resources, compliance, and operational units remains limited, with people-risk management handled in isolation rather than as part of a holistic ORM framework. These studies show that coordination failures stem not from the absence of formal structures, but from their limited capacity to support meaningful cross-functional interaction and shared accountability.

Several authors highlight that *excessive centralization* of risk management functions can diminish the value of local operational knowledge. Rad (2016) finds that in large banks, head-office control systems dominate the decision space of branch managers, who often perceive central directives as disconnected from on-the-ground realities. This imbalance reduces the effectiveness of local problem-solving and risk identification. Similarly, Sabanova and Kudinska (2022) argue that the implementation of centrally imposed risk frameworks limits front-line discretion and responsiveness, particularly in dynamic service environments. Centralisation thus creates an organizational bottleneck where information flows upward for approval but circulates only weakly laterally or downward for learning and adaptation.

A further recurring issue in the review concerns the disconnection between ORM systems and broader governance structures and decision-making mechanisms (e.g., Cerasi & Oliviero, 2015; Gontarek, 2016; Siaw Ofori et al., 2025). Hartmann and Slapničar (2007) note that in Slovenian banks, internal control systems existed formally but were loosely linked to corporate governance and decision-making processes. This structural decoupling weakened board oversight and reduced accountability for control failures. Similarly, Ringgaard et al. (2025) show that ORM frameworks are often positioned at mid-managerial levels with limited influence on strategic choices. The authors argue that without clear vertical integration between governance and operational layers, ORM remains a compliance exercise rather than a strategic management function.

Finally, some studies argue that structural weaknesses often interact with *cultural and behavioral dimensions of control* (e.g., Yokoi-Arai, 2023; Wright, 2018). Gurd and Helliar (2017) find that hierarchical communication structures discourage open dialogue about risk, limiting the interactive use of MCS. In their study of leadership practices, they show that structural rigidity reinforces a culture of avoidance rather than learning. Likewise, Cohn et al. (2014) demonstrate that organizational hierarchies emphasizing sales pressure and competitive norms can erode ethical awareness, creating environments where control violations proliferate. Wright (2018) further shows that traditional quantitative risk assessment systems overlook cognitive biases and decision errors, reinforcing structural blind spots and encouraging reactive, compliance-oriented control rather than adaptive learning. These findings indicate that structure and governance problems amplify behavioural risks when organisational design fails to support transparent communication, shared accountability, and interactive use of control systems.

Collectively, the reviewed studies emphasise that structure and governance critically mediate the relationship between MCS and operational risk outcomes. Across the literature, this manifestation domain shows how mechanisms identified in Chapter 2, particularly fragmentation, misalignment, constrained communication, and weak coordination, become amplified within banking organisations and undermine the integrative capacity of control systems. Fragmented structures, weak coordination between control lines, and excessive centralisation diminish the ability of ORM systems to function as dynamic and coherent

frameworks. The evidence suggests that effective ORM requires structural coherence where information, accountability, and authority flow seamlessly across organizational levels in a way that supports learing as well as oversight. At the same time, the literature indicates that structural reform alone is insufficient; unless accompanied by cultural openness and interactive control use, formal structures risk reproducing the very silos they are intended to overcome. In this sense, structure and governance problems remain a major pathway through which control systems generate operational risk vulnerability in banking.

3.4.4 Incentive-Related Control Problems

The literature consistently identifies incentive-related control problems as a major manifestation domain through which management control systems become linked to operational risk in banking, appearing in 12 studies included in the review. Building on Chapter 2, this domain captures how mechanisms such as incentive misalignment, crowding out of prudential judgment, and behavioural distortion become embedded in performance and reward systems. Incentive structures, both monetary and non-monetary, are intended to align individual goals with organisational objectives. However, when poorly designed or implemented, they can generate moral hazard, short-termism, and manipulation, thereby contributing directly to operational risk exposure. Empirical and conceptual evidence shows that incentive misalignment not only encourages excessive risk-taking but also distorts information flows and weakens ethical norms (Acrey et al., 2011; Cohn et al., 2014; Murphy, 2001). Four recurring issues emerged from the review: incentive misalignment (return vs risk), cultural "ethical blindness", subjectivity in performance evaluation, and interactions between incentives and regulation.

A central finding across the literature is that *misaligned incentives* increase banks' exposure to operational and reputational risks (e.g., Butler & Brooks, 2024; Caretta et al., 2024; Cerasi & Oliviero, 2015; Faugère & Stul, 2021). Acrey et al. (2011) demonstrate that CEO compensation structures heavily tied to short-term performance measures incentivize risk-taking behaviors that compromise long-term stability. Using U.S. banking data, they find that high sensitivity of pay to performance correlates with greater variability in operational losses. Similarly, Huston and James (1995) reveal that when compensation contracts reward aggressive lending and revenue expansion, managers engage in riskier operational decisions, increasing the probability of control breakdowns. These studies indicate that incentive systems emphasising short-term financial success tend to crowd out prudential risk awareness and weaken behavioural commitment to control.

Cultural reinforcement of misaligned incentives is reported by several studies in our review (e.g., Caretta et al., 2024; Faugère & Stul, 2021; Posch, 2020). Cohn et al. (2014) provide experimental evidence that banking culture itself can amplify the effects of misaligned incentives. Their study finds that when participants identify themselves as "bankers," they exhibit higher levels of dishonesty in incentivized tasks compared to control groups,

suggesting that professional identity and organizational norms interact with performance incentives to promote unethical behavior. This "ethical blindness" is not merely individual but structurally embedded within reward systems that prioritise profits over conduct integrity. The findings imply that operational risk cannot be mitigated through financial controls alone but requires cultural reinforcement of ethical behavior across all hierarchical levels.

The *subjective evaluation of managerial performance* also plays a critical role in shaping operational risk outcomes. Tran et al. (2021) explore how subjective performance evaluation practices influence fairness perceptions and behavioral compliance. They find that when evaluators exercise discretion inconsistently or opaquely, employees experience perceptions of injustice, leading to reduced motivation and opportunistic behavior. This aligns with findings by Merchant and Van der Stede (2017), who emphasize that overly subjective or inconsistent result controls can weaken commitment and increase gaming behaviors. The literature thus links subjective performance appraisal to the erosion of trust and to dysfunctional responses, such as gaming, disengagement, that undermine control reliability.

Finally, a few studies focus on how *incentive mechanisms interact with regulatory expectations* and control frameworks (e.g., Liang et al., 2024). Moosa (2017) and Power (2009) both caution that regulatory-induced formalization of control systems can obscure incentive-driven misconduct. When banks focus on compliance indicators rather than behavioral outcomes, incentives become detached from actual risk mitigation performance. Similarly, Ringgaard et al. (2025) highlight that when diagnostic controls are used to monitor risk metrics without considering behavioral drivers, incentive schemes can reinforce procedural compliance rather than substantive risk awareness. These findings collectively indicate that aligning incentives with ORM objectives requires an integrative control design, one that combines behavioral, cultural, and performance-oriented dimensions.

Across the reviewed literature, incentive-related control problems emerge as a major pathway through which management control systems generate operational risk vulnerability in banking. The studies show that mechanisms identified in Chapter 2, particularly incentive misalignment, crowding-out of prudential judgment, and behavioural drift, become amplified when reward systems prioritise short-term financial performance over risk awareness and control integrity.

Misaligned rewards foster excessive risk-taking, obscure ethical boundaries, and encourage opportunistic behavior, while subjective or inconsistent performance evaluations undermine accountability and trust. The evidence demonstrates that operational risk cannot be effectively managed without addressing the behavioral implications of incentive systems embedded within MCS. In practice, the challenge lies in designing incentive structures that balance financial performance with prudent risk-taking and ethical conduct, and long-term organisational resilience. The synthesis of empirical and conceptual studies confirms that incentive control is not merely a technical issue but a core governance mechanism linking

manasgement control design to operational reliability. Together, these studies suggest that operational risk arises not merely from poor system design but from behavioral drift induced by incentive misalignment, emphasizing the need to integrate motivational, cultural, and governance perspectives within ORM frameworks.

3.4.5 Cultural and Behavioural Problems

Cultural and behavioral problems represent one of the most pervasive manifestation domains through which management control problems become operationally challenging for operational risk management (ORM) in banking. Across 19 studies included in the review, this domain shows how mechanisms identified in Chapter 2, such as symbolic compliance, ethical drift, weak learning, and misalignment between formal control expectations and everyday behaviour, become particularly visible within operational risk management. Organisational culture and individual behaviour shape how formal control systems are interpreted, enacted, and sometimes subverted in practice. A strong control culture promotes integrity, learning, and accountability, while a weak or misaligned culture can normalize deviance, erode ethical standards, and reproduce control failures (Cohn et al., 2014; Faugère & Stul, 2021; Gurd & Helliar, 2017; Kunz & Heitz, 2021; Lui, 2015; Mikes, 2009; Power, 2009; Sabanova & Kudinska, 2023).

The reviewed studies show that cultural and behavioral factors often interact with other MCS elements particularly incentives, rules, and structures to shape how risk is perceived, reported, and managed in daily operations. Misalignment between formal frameworks and behavioral culture leads to failures in control and resilience adoption (Ashraf et al., 2016; Caretta et al., 2024; Channon et al., 2025; Edwards & Wolfe, 2004). Three recurring issues emerged from the review: leadership style (tone at the top), specific banking identity and competitive culture, and a cultural fear of mistakes.

Tone from the top and leadership behavior was mentioned by several studies (e.g., Butler & Brooks, 2024; Carpenter et al., 2021). Brauman et al. (2020) examine how leadership behavior shapes risk awareness and culture within banks. They find that "tone from the top" influences how employees interpret risk policies and prioritize operational safeguards. When senior management communicates risk management as a compliance formality rather than a shared responsibility, it weakens the motivational impact of controls. Conversely, leaders who use MCS interactively, by engaging employees in open discussions of risk and error, foster greater collective vigilance. Gurd and Helliar (2017) demonstrate that leadership style and communication patterns mediate the relationship between control systems and behavior. When leaders emphasize trust, transparency, and open dialogue, employees exhibit higher commitment to risk management practices. In contrast, hierarchical communication and lack of empowerment create behavioral disengagement and passive compliance. The study concludes that interactive control use where discussions about uncertainty and failure are institutionalized supports the development of constructive behavioural routines that reduce

operational exposure. Kunz and Heitz (2021) conduct a systematic review demonstrating that banks' risk culture is a multidimensional construct encompassing leadership tone, shared values, and behavioral consistency across levels of the organization. They emphasize that risk culture acts as an informal control system that both complements and constrains formal MCS. Weak risk cultures characterized by limited psychological safety, low transparency, and overreliance on compliance rituals contribute to concealment of errors and underreporting of incidents. The authors conclude that sustainable ORM depends on cultivating "behavioral control integrity," where learning and accountability are encouraged rather than penalized. These studies demonstrate that leadership behaviour is an important cultural control lever that can either reinforce or undermine ORM effectiveness.

Banking identity and competitive culture were also linked to ORM problems (e.g., Faugère & Stul, 2021; Holland, 2019). Cohn et al. (2014) find that when individuals identify themselves as bankers, they exhibit higher rates of dishonesty in incentivized tasks than control groups, implying that the prevailing culture of competitiveness and profit maximization can override ethical norms. Laguecir and Leca (2022) also find that unethical conduct is not merely an individual failure but a product of the institutionalized behavioral expectations within the banking culture. Such cultural normalization of opportunism directly heightens operational risk exposure by legitimizing minor deviations that can escalate into systemic misconduct. Lui (2015) analyses the culture of five UK banks between 2004 and 2009 and concludes that excessive greed, recklessness, and dishonesty had become normalized across hierarchical levels. The report documents that employees operated under performance cultures emphasizing sales and short-term revenue targets, which in turn fostered tolerance of rule-bending and misreporting. Ethical drift, in which behavioural norms diverge from formal control expectations, emerged as a critical pathway through which control failures develop. This erosion of integrity at both managerial and operational levels increased the frequency of internal loss events, revealing that risk culture failures were both a cause and a symptom of broader control dysfunction.

A cultural fear of mistakes leading to defensive routines was highlighted by some studies in our review (e.g., Carretta et al., 2024; Faugère & Stul, 2021; Frese & Keith, 2015). Mikes (2009) and Power (2009) both highlight that risk management cultures characterized by fear of blame or excessive formalization discourage employees from reporting problems or experimenting with learning-based risk practices. Mikes' ethnographic evidence shows that "calculative cultures" often prioritize risk quantification over dialogue, creating defensive routines that suppress uncertainty. Power (2009) similarly argues that over bureaucratized risk systems create "rituals of verification," where compliance activity substitutes for genuine behavioral engagement. These cultural patterns limit the adaptive learning necessary for effective ORM and transform control systems into mechanisms of symbolic assurance rather than real protection. Sabanova and Kudinska (2023, 2024) analyze the human error mindset among bank employees and identify cognitive biases and complacency as major contributors to operational risk. Their findings indicate that behavioral tendencies

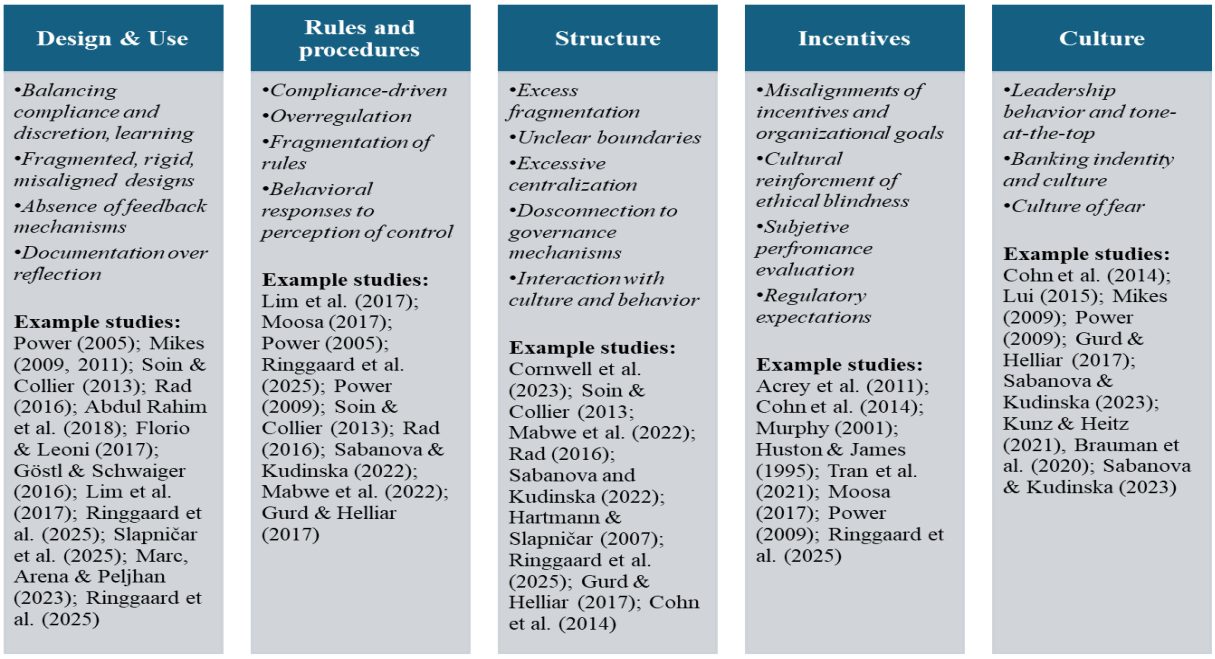
such as overconfidence, fatigue, and normalization of minor errors reduce the effectiveness of control systems. Moreover, error reporting mechanisms were underutilized due to cultural stigma attached to mistakes. The study calls for integrating human error awareness into training and control system design, emphasizing a "learning-oriented" approach to behavioral risk management.

Across the reviewed studies, cultural and behavioural problems emerge as a major pathway through which management control problems translate into operational risk vulnerability in banking. The literature shows that mechanisms identified in Chapter 2, particularly symbolic compliance, misalignment between formal controls and everyday practice, weak learning, and erosion of ethical norms, become amplified when control environments are shaped by excessive performance pressure, fear of mistakes, and weak psychological safety.Effective ORM requires aligning formal controls with supportive cultural mechanisms that promote ethical awareness, open communication, and continuous learning. Without cultural reinforcement, even sophisticated ORM frameworks risk becoming procedural shells, symbolically compliant yet behaviorally fragile.

3.4.6 Summary of findings

Figure 6 summarised the main issues of ORM systems when analysed as a MCS across five analytical dimensions. Building on the mechanism-based insights developed in Chapter 2, this synthesis addresses the first auxiliary research question by showing how management control problems emerge from the design and use of ORM systems, revealing tensions between formal control structures and their practical enactment. At the same time, it advances RQ2 by identifying the organisational and behavioural mechanisms through which these control problems shape operational risk outcomes in banking.

Figure 6: Summary of Findings Accross Five Analytical Dimensions



Source: Own work.

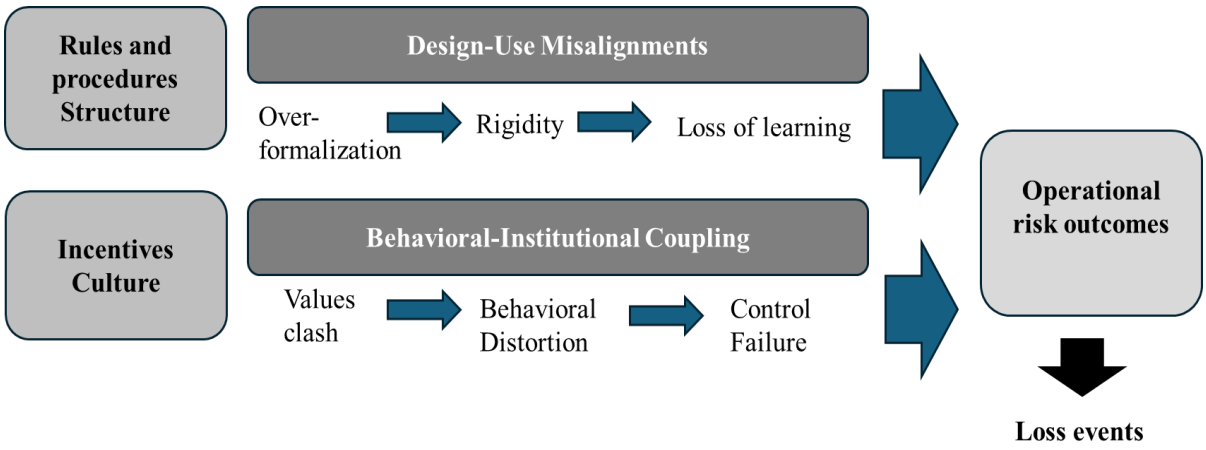
The patterns observed across the five analytical dimensions suggest two integrative pathways through which the design elements and use of ORM systems interact to shape control effectiveness. These pathways explain how structural features, managerial behavior, and institutional pressures jointly influence the balance between compliance and learning in operational risk management.

First, ***design–use misalignment*** captures the tension between the intended and enacted functions of control systems. Across the reviewed literature, formalisation and procedural design appear necessary for regulatory legitimacy, yet excessive proceduralisation often transforms controls from enablers into constraints. Power (2005, 2009) and Lim et al. (2017) show that ORM practices have become increasingly characterized by what they term a "ritual of verification," where visible compliance replaces substantive control effectiveness. Similar dynamics are observed in structural and incentive mechanisms. Too fragmented or too centralized structure also represents a failed design because managers cannot use information for effective control of risks, moreover additional risks can occur due to poor coordination and control gaps. Structural centralization, intended to ensure consistency, can restrict local managerial discretion and hinder timely risk identification (Rad, 2016; Sabanova & Kudinska, 2022), while performance-based incentives designed to align managerial interests may, in practice, induce short-termism and opportunism (Acrey et al., 2011; Cohn et al., 2014). Together, these studies show that misalignment between design and use does not simply reflect implementation failure but a deeper institutional tendency in which the pursuit of control assurance displaces the capacity for adaptive learning.

Contrary to existing research, we conceptualize this misalignment as a systemic and multi-domain phenomenon rather than as an issue confined to procedural or incentive design. This perspective integrates findings across rules, structure, and incentives to show that the reliability-oriented design of MCS can inadvertently suppress the interactive and interpretive practices that enable organizations to detect and respond to emerging risks. We reframe ORM not as a problem of insufficient control, but of *overcontrol*, where the symbolic and procedural demands of legitimacy compromise the system's learning potential. By doing so, the review advances theoretical understanding of ORM as a balancing act between compliance and adaptability, illustrating that the effectiveness of control systems depends less on their formal completeness than on their capacity to be used reflexively.

Second, ***behavioural and institutional coupling***, highlights how control mechanisms are enacted within specific cultural, cognitive, and institutional environments. Empirical studies (Kunz & Heitz, 2021; Mikes, 2009; Sabanova & Kudinska, 2023; Soin & Collier, 2013) consistently show that ORM systems do not operate in isolation but are embedded in organizational logics, professional identities, and social norms that shape their meaning and use. Weak risk cultures are characterized by fear, silence, and compliance-driven reasoning, which undermine ethical conduct and reporting integrity, while cultures of blame discourage open dialogue and experiential learning (Gurd and Helliar, 2017; Power, 2009). Conversely, when risk management systems are used interactively (Marc et al., 2023), they enable sensemaking and collective reflection, turning compliance processes into vehicles for organizational learning. When these mechanisms align toward learning, such as through interactive use, structural coherence, and behaviourally informed incentives, ORM shifts from a compliance ritual to a strategic capability. In such conditions, it supports anticipating disruptions, absorbing their effects, and learning from them. However, when incentives are misaligned and reinforced by ethically dysfunctional cultural norms, the resulting opportunism, misreporting, and manipulation increase operational risk exposure.

Figure 7: Dual Mechanisms Linking Control Systems Failures to Operational Risk



Source: Own work.

Figure 7 illustrates how design-use and behaviour-related pathways translate management control problems into operational risk outcomes. Several issues related to rules and structure contribute to the design–use misalignment, where over formalization leads to rigidity and a gradual loss of learning capacity. Incentives structures and culture interact through behavioural–institutional coupling, where conflicting values and cognitive biases generate behavioural distortion and control failure. Both pathways weaken the organization's ability to anticipate and respond to emerging risks, thereby increasing the likelihood of operational disruptions and, ultimately, loss events for banks. These two pathways thus represent complementary yet compounding routes through which management control failures materialize as operational risk exposures.

3.5 Discussion

The synthesis of the reviewed studies reveals that MCS play a dual role in ORM: they function simultaneously as mechanisms of stability and assurance and as potential sources of rigidity and dysfunction. Building on the mechanism-based insights developed in Chapter 2 and drawing on OOC framework as the broader theoretical lens, the analysis shows how management control problems become operationally relevant in banking when tensions emerge between the formal design of ORM systems and their practical enactment. Chapter 3 organises these dynamics through several manifestation domains, namely rules and procedures, structure and governance, incentives, and culture, in which control problems become visible within banking ORM. Two integrative pathways help explain these dynamics: design–use misalignment and behavioural–institutional coupling. Together, these insights support a more behavioural and interpretive understanding of ORM and move beyond a purely technical view of control systems.

The first contribution of this chapter is to illuminate the paradox of procedural control. While formalisation and procedural design are essential for regulatory legitimacy, the reviewed evidence demonstrates that excessive proceduraliation transforms controls from enablers into constraints. Studies by Power (2005, 2009) and Lim et al. (2017) describe how compliance routines often become "rituals of verification," in which visible conformity substitutes for substantive control effectiveness. This paradox reflects a deeper institutional tension: banks design control systems to satisfy external regulators, yet these same systems can suppress learning, flexibility, and professional judgment. Such procedural rigidity mirrors the evolution of ORM as a technocratic rather than behavioural discipline, where control reliability is measured by audit trails rather than adaptive capability. By conceptualizing proceduralisation as an institutional response that trades adaptive capacity for legitimacy, our study extends prior research on ORM's compliance–learning trade-off and underscores the need to balance regulatory assurance with organizational adaptability.

The second contribution lies in showing how structural design influences the behavioural integration of ORM. Despite the conceptual clarity of the Three Lines of Defense model,

empirical evidence (Cornwell et al., 2023; Mabwe et al., 2022; Soin and Collier, 2013) shows that control and risk functions frequently operate in isolation, leading to coordination failures and fragmented accountability. Structural centralization may enhance oversight, but it often limits local managers' autonomy even if they often possess the operational knowledge necessary for timely risk identification (Rad, 2016; Sabanova & Kudinska, 2022). The synthesis indicates that structural coherence, not merely formal hierarchy, is the critical prerequisite for control effectiveness. By highlighting the need for connective rather than merely vertical structures, our study advances understanding of how organizational design can support interactive learning and information flow about operational risks across functional boundaries, rather than reinforcing administrative separation created by ORM frameworks.

The third contribution concerns the behavioural dynamics of incentive systems. The findings on incentive-related control problems extend the traditional agency perspective by illustrating how misaligned rewards can erode governance integrity and amplify operational risk. Research by Acrey et al. (2011) and Cohn et al. (2014) demonstrates that short-term performance incentives distort managerial judgment and normalize opportunism, while subjective or inconsistent performance evaluations (Merchant & Van der Stede, 2017; Tran et al., 2021) erode perceptions of fairness and control credibility. Our study thus extends existing work by conceptualizing incentives as behavioural controls that are embedded in, and mutually constitutive with, cultural and structural mechanisms. From this perspective, operational risk emerges not only from system failure but from motivational design, repositioning incentive alignment as a key lever of ORM governance.

The fourth contribution lies in reframing organisational culture as a deep control layer rather than a contextual backdrop. Across the reviewed literature (Kunz & Heitz, 2021; Mikes, 2009; Sabanova & Kudinska, 2023), weak risk cultures marked by silence, fear, or excessive competition, undermine reporting integrity and ethical conduct. Cultures of blame (Gurd & Helliar, 2017; Power, 2009) convert control systems into instruments of symbolic assurance, while interactive uses of control that institutionalize open dialogue (Marc et al., 2023) foster trust, accountability, and collective learning. The synthesis therefore shows that cultural alignment is not a residual outcome of control design, but an important condition for its effective enactment. Without supportive norms and leadership tone, even sophisticated MCS architectures risk devolving into procedural shells.

Finally, the chapter contributes by advancing an integrative behavioural systems view of ORM. The evidence across procedural, structural, motivational, and cultural dimensions indicates that fragmentation reflects a failure to view control systems as dynamic social mechanisms evolving through interaction, feedback, and interpretation. Building on studies by Mikes (2011), Ringgaard et al. (2025), and Göstl and Schwaiger (2016), we propose that control effectiveness arises when measurement is linked with meaning and compliance is coupled with sensemaking. By integrating design and use within a feedback-oriented,

learning framework, ORM can be understood as a living system that evolves through interaction and interpretation rather than as a static set of procedures.

Taken together, these contributions move the discussion of ORM beyond the conventional dichotomy of "hard" and "soft" controls. They position MCS as behavioural infrastructures that both shape and are shaped by organizational learning processes. The review thereby contributes to theory by articulating a reflexive model of control, one that acknowledges the interdependence between formal assurance and adaptive capability. Additionally, it highlights how control systems can be designed and used to balance compliance demands with organizational resilience. At the same time, this synthesis provides the conceptual basis for Chapter 4, which examines how these pathways are manifested empirically within a case-study bank.

From a managerial perspective, the findings imply that strengthening ORM requires not more control, but more *reflexive* control. Practitioners should focus on aligning the intended purposes of controls with their day-to-day use, ensuring that compliance processes also facilitate discussion, learning, and local problem-solving. This may involve simplifying procedures, decentralizing decision authority where appropriate, and encouraging open reporting through trust-based cultural initiatives. Moreover, aligning incentive structures with long-term behavioural outcomes rather than short-term metrics can reduce moral hazard and reinforce ethical accountability. Ultimately, ORM effectiveness depends on cultivating organizational conditions in which control systems serve as enablers of informed judgment rather than substitutes for it. For policymakers and regulators, the findings imply that regulatory frameworks should encourage proportionality and reflexivity in compliance design, recognizing that excessive proceduralisation may generate symbolic rather than substantive assurance. Finally, for risk management professionals in regulated industries**,** the study highlights the importance of integrating behavioural and cultural diagnostics into ORM assessment. Rather than focusing solely on procedural completeness or audit conformity, risk officers should evaluate how control systems are actually used and experienced, and how organizational climate and leadership tone influence their functioning.

From a research perspective, this review points toward several directions for future inquiry. First, the behavioural systems view developed here invites empirical investigation of the dynamic interplay between control design and use**,** examining how organizations recalibrate controls in response to feedback, technological change, or regulatory pressure. Longitudinal and ethnographic studies could illuminate how design–use misalignments emerge and evolve over time. Second, the notion of behavioural–institutional coupling calls for multi-level research that connects individual cognition and ethics with institutional logics and organisational fields. Such studies could explore how regulatory expectations, professional norms, and organisational cultures interact to shape the enactment of ORM practices. Third, the growing digitalisation of control systems offers a fertile context for examining how algorithmic oversight, data analytics, and artificial intelligence reshape the behavioural foundations of risk management, potentially reproducing older misalignments in new

technological forms. Finally, comparative research across industries and institutional settings could further clarify the contextual conditions under which reflexive, learning-oriented control becomes possible. These directions also reinforce the need for empirical research that traces how control problems identified conceptually become enacted within concrete organisational settings, which is the focus of the next chapter.

3.6 Conclusion

This systematic literature review examined how management control problems identified in Chapter 2 become operationally relevant within the design and use of control systems and how these problems shape operational risk management in the banking sector. Drawing on Merchant and Van der Stede's (2017) OOC framework as the broader theoretical lens, the review showed that operational risk arises not merely from technical control failures, but from the interaction between control design, control use, and organisational behaviour.

The findings demonstrate that while regulatory-driven control architecture enhances formal accountability, they often create unintended behavioural consequences: procedural rigidity, structural silos, incentive distortion, and cultural erosion. These dynamics reveal that the very systems intended to reduce operational risk can, under certain conditions, become its source. At the same time, the review identifies a growing shift in recent literature toward interactive and integrative control practices, highlighting approaches that emphasize dialogue, shared sensemaking, and cross-functional coordination. When controls are used interactively and supported by strong cultural values of learning and transparency, they can transform ORM from a compliance exercise into a strategic capability.

Theoretically, the review contributes by extending the mechanism-based insights developed in Chapter 2 into the domain of operational risk management. It shows that result, action, personnel, and cultural controls remain a useful theoretical lens for understanding how management control problems emerge, while the banking context reveals how these problems become amplified through design–use misalignment and behavioural–institutional coupling. In this way, the chapter bridges the management control and risk management literatures by demonstrating that operational risk is not merely a stochastic or technical phenomenon, but also a behavioural outcome of control dysfunction. Practically, the review highlights that banks need to view operational risk management as a socio-technical system. Strengthening operational resilience requires not only improving control design but also cultivating behavioural and cultural conditions that support adaptive use. Managers should therefore integrate learning mechanisms, open communication, and cross-functional collaboration into control processes. Regulators and boards, in turn, should recognise that compliance effectiveness depends on behavioural engagement, not solely on procedural completeness. For researchers, the chapter identifies an agenda for longitudinal, multi-level, and cross-sectoral analyses that trace how management control configurations evolve alongside regulatory, technological, and cultural change. Future research should further

examine the cognitive and social mechanisms that mediate the relationship between control design and operational outcomes, linking behavioural insight with measurable indicators of control effectiveness.

As with all literature reviews, the present study faces limitations. The synthesis relies on published studies available in English and in selected databases, which may exclude relevant insights from other linguistic or institutional contexts. Furthermore, the review focuses on the banking sector, where ORM is most developed; comparative research across industries could extend the generalizability of its conclusions. Finally, as an interpretive synthesis, the analysis depends on the conceptual framing applied, and future work using alternative theoretical perspectives could enrich and challenge these interpretations.

In conclusion, the effectiveness of operational risk management depends on balancing formal control assurance with behavioural adaptability. Banks that succeed in aligning control design with control use, and compliance with learning, are better positioned to build resilient systems capable of preventing, absorbing, and learning from operational disruptions. These insights provide the conceptual foundation for Chapter 4, which examines how the mechanisms and pathways identified in this review become manifested empirically within a case-study bank.

4 ORGANISATIONAL MECHANISMS LINKING MANAGEMENT CONTROL PROBLEMS TO OPERATIONAL RISK IN BANKING: A QUALITATIVE CASE STUDY

4.1 Introduction

The systematic literature reviews presented in Chapters 2 and 3 developed the conceptual foundation for this empirical chapter. Chapter 2 identified how different types of management control systems give rise to recurring control problems and dysfunction mechanisms, while Chapter 3 showed how these mechanisms become operationally relevant in banking through their translation into operational risk vulnerabilities. Building on this foundation, Chapter 4 examines how these mechanisms are manifested empirically within a particular organisational setting. In this way, the chapter moves from conceptual synthesis to qualitative observation of how control problems are experienced, enacted, and linked to operational risk within the Bank.

While the mechanisms identified in the literature provide an important conceptual lens, they remain theoretical propositions until examined in organisational practice. Existing research largely theorises operational risk at a systemic level and relies heavily on secondary data, surveys, or conceptual arguments. As a result, the detailed organisational, behavioural, and technological pathways through which controls fail in practice remain under-specified. The

purpose of this chapter is therefore not to test the literature-based model, but to empirically explore, refine and extend through qualitative inquiry within a case-study bank.

This chapter addresses the research questions guiding the empirical study:

RQ1: How do different types of Management Control Systems generate control problems within a bank?

RQ2: How do these control problems contribute to the emergence of operational risk within the bank?

To answer the research questions, qualitative data were collected through 13 semi-structured interviews with managers across key organisational units of one selected bank (hereafter "the Bank"), which serves as the focal case study. The data were analysed using the Gioia methodology (Gehman et al., 2018; Gioia et al., 2013), which enabled a systematic progression from informants' first-order descriptions to second-order theoretical categories and aggregate mechanisms. This approach has been increasingly adopted in accounting and management control research to support inductive theory building based on rich qualitative data (e.g., Kunz, 2025; Marelli, 2024).

The analysis examines how result controls, action controls, personnel controls, and cultural controls are enacted in practice and how they generate structural, behavioural, and ethical vulnerabilities that surface as operational risk. The empirical findings are organised into two aggregate dimensions, i) Design-Driven Control Problems and ii) Human-Capability and Behavioural Control Problems, which capture the principal pathways through which control problems become visible in the Bank's operational environment. In this way, the chapter provides an empirical grounding for the conceptual mechanisms developed in the preceding chapters. This chapter focuses solely on reporting and interpreting empirical findings.

The remainder of this chapter is organised into six sections. Section 4.2 outlines the research design and methodology, including the qualitative approach, data collection procedures, and the use of the Gioia method for inductive analysis. Section 4.3 presents the empirical findings, beginning with the aggregate dimensions that emerged from the coding process and then examining how different types of management control systems generate control-related problems within the Bank. Section 4.4 reports the empirical findings addressing RQ1, detailing how different types of management control systems generate control-related mechanisms within the Bank. Section 4.5 addresses RQ2, examining how these mechanisms map onto specific operational risk categories under the Basel II/III framework. Section 4.6 provides a discussion that connects the empirical evidence to the theoretical model developed in Chapter 3, identifying points of confirmation, refinement, and theoretical extension. Section 4.7 introduces the upgraded conceptual model, integrating the literature-based mechanisms with the empirically derived pathways. Finally, Section 4.8 concludes the chapter by summarising the key contributions of the empirical findings and their implications for the broader thesis.

4.2 Research Design and Methodology

4.2.1 Research design

The research is based on a single-case study design, in which one selected bank serves as the empirical setting. This design was chosen because the aim is to obtain rich, contextualised evidence that allows for an in-depth examination of how different Management Control Systems generate control problems and how these problems translate into operational risk within a real organisational environment. A single case provides the level of detail and access required to uncover behavioural, organisational, and systemic mechanisms that would be difficult to capture through a multiple-case design, where breadth typically comes at the expense of depth (de Vaus, 2001).

Within this design, the Object of Control framework (Merchant & Van der Stede, 2017) is used as the primary lens for analysing the Bank's management control system, while the Basel II/III operational risk categories provide the framework for interpreting risk consequences

The underlying premise is that weaknesses in Result, Action, Personnel, and Cultural Controls manifest as identifiable control problems, which in turn, influence the emergence of operational risk events within the bank. This approach is consistent with the nature of the phenomenon under study: operational risk is inherently behavioural, systemic, and organizational, and therefore requires an analytical approach that examines both the underlying control structures and how they are experienced and enacted in practice.

4.2.2 Case study methodology

The decision to employ a case study methodology is grounded in the nature of the research questions and the characteristics of the phenomenon under investigation. Case studies are particularly well suited for research that seeks to explain complex organizational processes, examine causal mechanisms, and understand phenomena within their real-life context (Yin, 2018). For studies that explore "how" and "why" questions, such as how management control systems generate control problems and why these problems contribute to operational risk case studies enable a level of depth, contextualization, and analytical nuance that alternative methods cannot easily achieve.

The case study approach is appropriate in this research for several reasons. First, the functioning of management control systems in a banking environment is inherently organizational, behavioral, and context dependent (e.g., Gooneratne & Hoque, 2013; Kunz & Heinz, 2024.). As Eisenhardt (1989) and Stake (1995) emphasized, case studies are especially useful when the boundaries between a phenomenon and its context are not clearly defined. In this study, control problems cannot be isolated from the organizational setting in

which they occur, nor can operational risk be understood independently of the control system's design, culture, and behavioral dynamics. The case study method makes it possible to observe these elements as interconnected components of a single system.

Second, case studies allow researchers to investigate organizational phenomena as they unfold in their natural setting (Creswell, 2014), without artificially isolating variables or reducing complexity. Operational risk events, control failures, and the behavioral responses of employees emerge from interdependent processes rather than discrete, observable incidents (e.g., Power, 2005, 2009). Merriam and Tisdell (2016) note that case studies are well suited for uncovering such layered dynamics by integrating information about organizational structures, human behavior, and contextual constraints. This is aligned with the needs of this study, where the aim is to understand the role of Result, Action, Personnel, and Cultural Controls within the actual operational environment of the bank.

Third, the case study methodology is particularly appropriate when the objective is explanatory, not merely descriptive. According to Yin (2018), case studies are the most suitable design when the research aims to explain causal relationships, understand organizational mechanisms, and trace how specific conditions lead to outcomes. This aligns directly with the purpose of this empirical stage of the dissertation: to examine how different types of management control systems generate control problems within the Bank and how these control problems translate into operational risk exposures. Because these dynamics are systemic, behavioural, and embedded within everyday organisational practices, they can be meaningfully captured only through a case study approach that allows in-depth examination of how these pathways unfold in context.

Although the case study method offers deep contextual insight, it is often criticised for subjectivity, researcher bias, and limited generalisability (Stake, 1995; Yin, 2018). In addition, qualitative interview-based research may be affected by informant-related biases, such as social desirability and selective recall, particularly when sensitive organisational issues, such as control failures or operational risk events, are discussed. The reliance on managerial respondents may also introduce elite bias, as perspectives from frontline employees may differ. Furthermore, the interpretive nature of qualitative analysis creates the possibility of researcher bias in coding and theme development.

To address these concerns, this study follows several established safeguards. Data triangulation across interviews, internal documents, and observational insights enhances the credibility and consistency of interpretations (Eisenhardt, 1989; Yin, 2018). The use of the Gioia methodology provides a transparent coding structure that clearly distinguishes informant terms from researcher interpretations, thereby reducing interpretative bias. To enhance reliability, interview transcripts and reconstructed notes were returned to participants for verification (member checking), reducing the risk of misinterpretation and recall-related inaccuraciesTo enhance auditability, the Appendix contains the semi-structured interview protocol and illustrative excerpts of the coding process that document

how first-order codes, second-order themes, and aggregate dimensions were derived (Merriam & Tisdell, 2016; Stake, 1995). In addition, strict confidentiality and anonymisation procedures were applied throughout the research process to encourage open and candid responses from participants.

While case studies are often criticised for limited generalisability, the aim of this research is not statistical generalisation but analytical generalisation, where findings contribute to the refinement of theoretical propositions rather than represent a broader population (Yin, 2018). In qualitative case research, the relevance of insights to other contexts derives not from sample size but from the richness of contextual description and conceptual clarity (Merriam & Tisdell, 2016; Stake, 1995). By offering rich descriptions of the Bank's organisational structure, control environment, and institutional context, this study supports the potential transfer of its insights to comparable banking organisations facing similar management-control and operational-risk challenges.

4.2.3 Case selection and Context

The case for this study was intentionally selected to provide a rich organizational environment in which management control systems and operational risk processes could be examined in depth. The chosen case is the Kosovo-based subsidiary of a large international banking group. Its size, organizational complexity, and strategic importance in the national banking sector make it an ideal setting for addressing the research questions.

The bank holds a 17% market share in total assets, 16.4% in total deposits, 17.7% in total loans, and 20.3% in net profit, positioning it as one of the leading financial institutions in the country. This market position ensures that the bank operates with a fully developed system of controls, structured risk-governance mechanisms, and a comprehensive set of operational risk practices. Because the study examines how Result, Action, Personnel, and Cultural Controls function in practice, the presence of mature organizational processes was an important criterion for case selection.

Financially, the bank demonstrated strong performance in 2024, achieving a record annual profit of €37 million. This performance indicates sustained growth and a high degree of organizational stability, which are essential for studying how management control systems are designed, implemented, and experienced across different levels of the organization. The bank's scale and profitability also suggest the presence of established reporting routines, automated and manual control mechanisms, and a systematic approach to risk monitoring factors that make it possible to observe control problems and operational risk exposures in a real and meaningful context.

The bank employs 478 staff members across a diverse set of operational, managerial, and support functions. This size allows for the inclusion of multiple perspectives in the study, ranging from board-level decision-makers and senior managers to department heads, risk

and compliance officers, and frontline supervisors. Such diversity enhances the analytical depth of the case, enabling insight into how controls operate across functions and how control problems emerge in different parts of the organization.

Additionally, the bank operates within a structured regulatory environment and is required to comply with the operational risk standards applied in the Kosovo financial sector, which are aligned with internationally recognised supervisory frameworks. This makes it possible to map the identified control problems directly into internationally recognized operational risk categories. It also enhances the transferability of the findings because the selected case (the Bank) functions withing a regulatory architecture similar to that of other EU banking jurisdictions. Therefore, the mechanisms identified in this case are likely to be relevant for banks operating under comparable supervisory expectations and institutional conditions.

Additionally, the bank operates within a structured regulatory environment and is required to comply with the operational risk standards applied in the Kosovo financial sector, which are aligned with internationally recognised supervisory frameworks. This makes it possible to map the identified control problems into established operational risk categories and to interpret them within a broader prudential context. At the same time, the value of the selected case (the Bank) lies less in statistical generalisation than in its analytical relevance: the bank operates within a regulatory architecture comparable in important respects to that of other European banking jurisdictions, making it a suitable setting for examining how management control systems and operational risk management interact under formal supervisory expectations. Under comparable supervisory expectations and institutional conditions, some of the mechanisms identified in this case may therefore also be relevant in other banks operating in similar settings.

The choice of a commercial bank was also theoretically important. Commercial banking provides a particularly suitable setting for examining the relationship between management control systems and operational risk management because it combines formal control structures with routine operational processes, customer-facing service delivery, lending activities, payment operations, and strong regulatory oversight. These features make control problems and operational risk highly visible in day-to-day organisational practice, including risks related to employee behaviour, process execution, internal coordination, system reliability, and compliance with formal procedures. This focus also reflects the internal differentiation of the banking sector. Compared with investment banking, commercial banking is more strongly associated with routine service provision, process reliability, customer interaction, and the stable provision of credit and payment services, making it especially suitable for examining how management control problems emerge in everyday organisational processes and become linked to operational risk management in practice (Greenbaum et al., 2019; Kunz et al., 2021; Mikes, 2009).

The Bank was selected because it offers the organisational scale, structural complexity, established control architecture, and operational relevance required to address the two

research questions. Its strong market position, stable performance, and well-developed internal structure provide an environment in which management controls and operational risk processes can be clearly observed and analysed in depth. The case was not selected to represent all banking segments in the same way, but to provide analytically rich insight into the interaction between management control systems and operational risk within a commercial banking context.

4.2.4 Data collection

Data for this study were collected through 13 semi-structured interviews conducted with senior managers and departmental heads at the Bank's head office. Semi-structured interviews are widely used in organisational and management control research because they provide both structure and flexibility, enabling researchers to capture the depth and complexity of lived organisational experience (Kvale & Brinkmann, 2009; Rubin & Rubin, 2012).

The selection of interviewees was driven by the aim of obtaining insights from individuals who hold direct responsibility for designing, implementing, and operating the Bank's management control and operational risk practices. This logic follows the view that risk-related processes are shaped not only by formal procedures but also by the work of specific actors who carry specialized responsibilities. As highlighted by Hiebl (2024), understanding how risk becomes integrated into management control requires attention to sub-organisational levels, particularly teams and individuals, such as risk experts or controllers who exert significant influence over how controls function in practice.

Consistent with this perspective, interviewees were drawn purposefully from organisational units where these responsibilities are concentrated. Purposeful sampling is commonly recommended in qualitative research when the goal is to obtain information-rich cases that illuminate the central questions of the study (Palinkas et al., 2015; Patton, 2015). Accordingly, participants were selected from the Board of Directors, Internal Audit, Risk Management, Operational Risk, Compliance, Internal Controls, Legal, Human Resources, Security, Payment & E-Banking, and three branch offices. These positions represent the core sub-units through which the Bank's control systems are developed, monitored, and enforced, making their holders uniquely positioned to explain how risk is integrated into management control in everyday organisational practice.

In total, 13 semi-structured interviews were conducted with representatives across all key governance and operational departments. This ensured full coverage of the Bank's control architecture and enabled triangulation across managerial levels and functional domains (Flick, 2018). Interviews were conducted in the Albanian language to reflect the linguistic and cultural context of the institution. Each interview lasted approximately 90 minutes, consistent with recommended interview durations for in-depth organisational inquiry

(Seidman, 2013), allowing for a detailed exploration of control design, control use, experienced weaknesses, and the emergence of operational risk events.

Access to interview recording varied, participants from several departments consented to audio recording, while others refused due to internal protocols or personal preferences. Whenever recording was not permitted, extensive field notes were taken during the interview and completed immediately afterward to ensure accuracy. This is an accepted practice in qualitative interviewing when recordings are not feasible (Miles et al., 2014). To enhance interpretive validity, all interview transcripts and reconstructed notes were sent back to the respective participants for verification and clarification through a member-checking procedure, a practice recognised for strengthening credibility in qualitative research (Lincoln & Guba, 1985).

In addition to interviews, observational data were collected during the researcher's time at the Bank's head office. Organisational observations are a valuable complement to interviews, as they allow researchers to capture interactional patterns, routines, and contextual cues that informants may not articulate explicitly (Czarniawska, 2014; Yin, 2018).

Access was granted to one cross-functional meeting related to Current and Savings Account processes, providing direct insight into procedural interactions, workflow coordination, and communication between departments. Although formal access to additional meetings was limited, the sustained presence at the Bank during the interview period enabled the observation of informal interactions, organisational routines, and everyday behavioural dynamics relevant to the study's focus. These observations provided contextual depth and supported triangulation of interview findings.

A semi-structured interview guide was used to ensure consistency across interviews while allowing flexibility to explore emergent issues raised by participants, a distinguishing feature of qualitative interviewing (Kvale & Brinkmann, 2009; Rubin & Rubin, 2012). Questions focused on the structure and use of controls within each unit, challenges associated with these controls, and the operational risk vulnerabilities linked to their responsibilities (See Appendix 7).

As the interviews progressed, it became evident that the data were converging toward a stable set of themes. In line with qualitative research standards (Charmaz, 2014; Glaser, 2001; Locke et al., 2001), theoretical saturation, which is the point at which additional interviews no longer generate new conceptual insights, was reached around the 11th interview. The remaining two interviews served to confirm the emerging themes, strengthen conceptual depth, and validate the cross-departmental relevance of the findings. This pattern of saturation aligns with empirical evidence indicating that thematic completeness in semi-structured interview studies typically emerges within 10–12 interviews when the participant group is relatively homogeneous in expertise (Guest et al., 2006; Saunders et al., 2018).

Table 12: Overview of Interview Participants and Data Collection Details

Position / Department	***Nr. Interview***	***Date of the Interview***	***Recording***
Board of Directors	1	08.10.2024	NO
Operational Risk Management	1	14.06.2024	NO
Risk Management Department	1	17.05.2024	NO
Internal Audit Sector	1	15.04.2024	NO
Internal Controls	1	18.04.2024	YES
Compliance Office	1	17.04.2024	YES
Security Department	1	24.05.2024	YES
Human Resource Department	1	12.04.2024	YES
Branch Manager	1	12.04.2024	NO
Branch Manager	1	16.04.2024	NO
Branch Manager	1	22.04.2024	NO
Payment and E-Banking	1	25.07.2024	YES
Legal Department	1	09.08.2024	YES
Total	13		

Source: Own work.

4.2.5 Ethical Considerations and Confidentiality

Prior to beginning the fieldwork, I signed a formal confidentiality agreement with the Bank, confirming that the institution's name, departmental identifiers, and the identities of all interviewees would not be disclosed in the thesis or in any subsequent publications. All participants were informed that their contributions would remain anonymous and that no information would be reported in a manner that could be traced back to specific individuals or organizational units. Participation was voluntary, and interviewees were informed that they could decline to answer questions or withdraw at any stage without any consequences. All data were handled in accordance with these confidentiality commitments, and anonymization procedures were applied throughout transcription, member checking, analysis, and presentation of findings.

Participants were informed that their contributions would remain anonymous and that no information would be reported in a manner that could be traced back to specific individuals or organisational units. Participation was voluntary, and interviewees were informed that

they could decline to answer questions or withdraw at any stage without any consequences. Particular attention was given to minimising any risk that participants could be exposed to negative consequences for disclosing sensitive information. For this reason, data were handled in a manner that prevented disclosure of identities to organisational actors, including managers, and interview materials were not shared in a form that could enable attribution of statements to particular individuals.

In the thesis, any potentially identifying details, including references to specific departments, functions, or positions, were removed, generalised, or anonymised to ensure that participants could not be traced and to minimise any risk of unintended disclosure. These protections were applied throughout transcription, member checking, coding, analysis, and presentation of findings. The study was conducted in accordance with general ethical principles of voluntary participation, informed consent, confidentiality, anonymity, and avoidance of harm. Given the non-invasive and participatory nature of the study, the applicable institutional procedures in place at the time of the research did not require a formal approval from a Research Ethics Committee; the ethical safeguards described above were implemented as a matter of research integrity.

4.2.6 Data Analysis

The qualitative data analysis followed a systematic, multi-cycle coding strategy that combined deductive and inductive logics, consistent with the principles of rigorous inductive research outlined by Gioia et al. (2013). The analytic approach was designed to ensure methodological transparency, conceptual depth, and a clear evidentiary chain from raw interview material to higher-order theoretical insights.

In the first cycle of analysis the interview material was organised according to Merchant and Van der Stede's (2017) Object of Control framework. This step served as an initial structuring device, enabling the data to be grouped by the broad type of control discussed in each narrative segment, namely Result Controls, Action Controls, Personnel Controls and Cultural Controls. Within each control category, coding remained inductive, allowing emergent themes to surface from informants' description rather than imposing predefined subcategories.

In parallel, the same excerpts were examined for manifestations of control problems and related organisational vulnerabilities, drawing on the mechanism-based insights developed in Chapters 2 and 3 and on prior research on management control and operational risk. Concepts such as structural problems, rigid-rule problems, incentive problems, and cultural problems were used as prompts rather than fixed coding bins. This enabled a more granular identification of weaknesses, misalignments, and behavioural vulnerabilities embedded in the Bank's control system and described by interviewees.

In the next step, the two coding layers were combined to form 1st-order codes that captured how a specific type of control (e.g., Action Control) was associated with a specific emergent control problem (e.g., structure-related issues). These 1st-order mechanism–problem combinations retained informant-centric meaning and formed systematic analytic units that allowed subsequent conceptual aggregation, consistent with the Gioia methodology.

Following Gioia et al. (2013), this stage emphasized faithfulness to participant terminology, transparency in coding logic, and the development of 1st-order terms before aggregating them into higher-order categories.

After collecting a stable set of 1st-order codes, a second cycle of inductive coding identified patterns, similarities, and conceptual clusters across the data. Through iterative comparison, discussion, and refinement, the analysis generated distinct 2nd-order themes that captured broader pathways linking the types of controls to the recurring types of control problems and operational vulnerabilities. This stage aligns with what Gioia et al. (2013) describe as "stepping up to a higher level of abstraction" while preserving clear links between data and interpretation.

The final step of the analysis involved clustering the 2nd-order themes into two overarching aggregate dimensions, representing the dominant pathways through which control system weaknesses manifested in the Bank: Design-Driven Control Problems, and Human-Capability & Behavioral Control Problems. These aggregate dimensions provided the structural framework for presenting the findings and formed the basis for linking RQ1 (control problems) with RQ2 (operational risk categories).

Consistent with the Gioia methodology, the entire analysis produced a data structure illustrating the progression from raw interview excerpts to aggregate dimensions (illustrated in Figure 8). This hierarchical representation satisfies the core criterion emphasized by Gioia et al. (2013, p. 21) "No data structure; know nothing", highlighting the transparency of the coding process and ensuring that interpretations remain grounded in the empirical evidence.

4.2.7 Thematic Analysis

The qualitative analysis resulted in a structured set of themes that capture the patterned ways in which the Bank's management control system generates control problems in practice. While the coding procedures and analytical steps are described in the Methodology chapter, this section outlines the thematic structure that emerged from the empirical material and provides the conceptual foundation for the findings that follow.

Across the interviews, two overarching aggregate dimensions were identified, each reflecting a distinct pathway through which weaknesses in controls influenced organisational behaviour and operational risk. The first, Design-Driven Control Problems, encompasses themes arising from limitations in the design, configuration, or rigidity of the Bank's control

systems. The second, Human-Capability & Behavioural Control Problems, captures themes relating to employees' skills, behavioural responses, ethical judgment, and the cultural context within which controls operate.

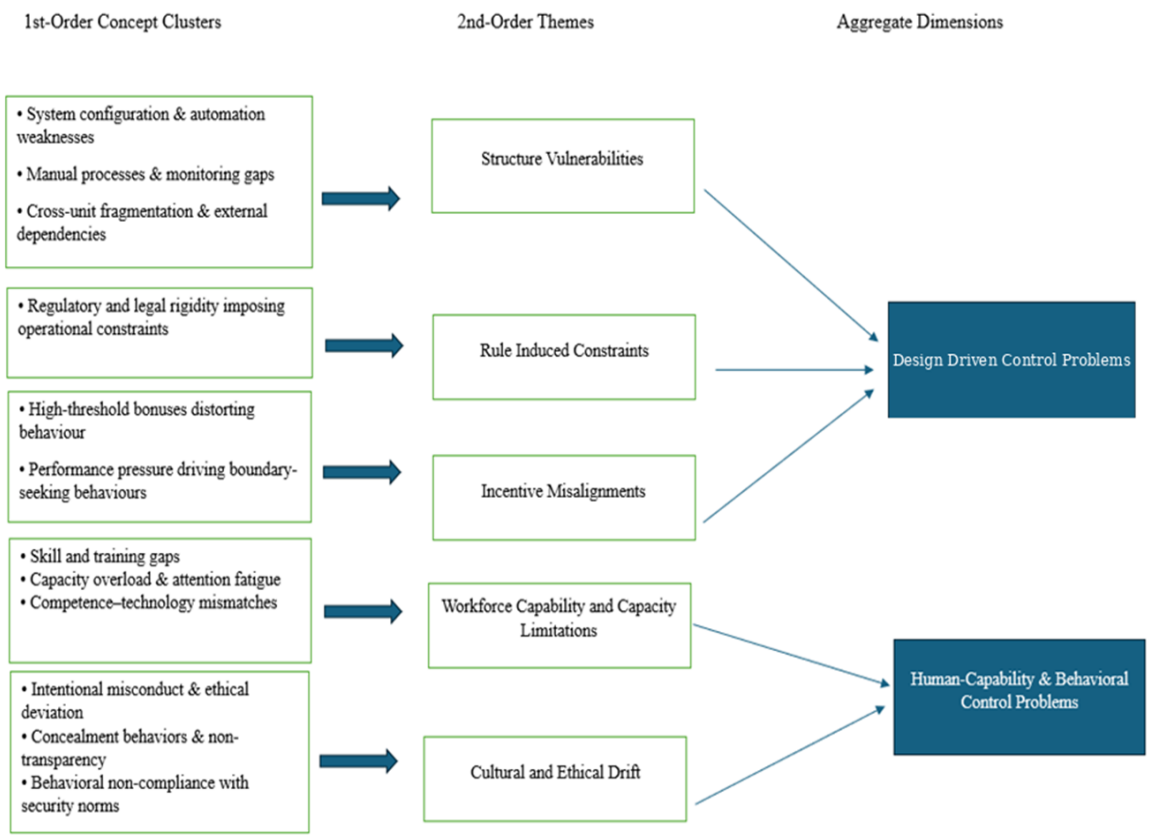
Five 2nd-order themes emerged from the analysis, which were then clustered into the two overarching dimensions:

- **Structural Vulnerabilities**
  Weaknesses emerging from system design, automation gaps, fragmented processes, and manual workarounds.
- **Rule-Induced Constraints**
  Issues arising from inflexible regulatory, legal, or procedural requirements that constrain operational adaptability.
- **Workforce Capability and Capacity Limitations**
  Skill gaps, workload pressures, migration-related staffing shortages, and resistance to digital transformation.
- **Incentive Misalignments**
  Pressures generated by the design of result controls, including high performance thresholds and target-linked rewards.
- **Cultural and Ethical Drift**
  Breakdowns in ethical norms, inconsistent risk awareness, and culturally driven deviations from expected procedures.

Together, these themes offer a comprehensive view of how different elements of the control system, including its design features, behavioural expectations, and organisational culture can generate recurring patterns of vulnerability within the Bank. They also provide the basis for answering the research questions: how control problems arise (RQ1) and how these problems translate into operational risk (RQ2**)**. The following sections introduce each of the themes developed through the iterative coding process. These thematic narratives synthesize the underlying mechanisms captured in the data and clarify how each theme reflects recurring patterns of control problems within the Bank's management control system.

Additionally, Figure 8 shows the three-tiered coding hierarchy, beginning with representative clusters of 1st-order concepts grounded in interview excerpts, followed by the 2nd-order themes derived through comparative categorization, and culminating in the two aggregate dimensions that organize the findings. This data structure provides a conceptual map for the empirical results reported in the following sections.

Figure 8: Data Structure form Concepts to Themes to Aggregate Dimensions



Source: Own work.

4.3 Findings

The purpose of this chapter is not to introduce new categories of control problems, but to empirically examine how the mechanisms identified in Chapters 2 and 3 become visible within the Bank's management control system. Chapter 2 conceptualised how different types of management control systems can generate dysfunction mechanisms. Chapter 3 showed how these mechanisms are associated with operational risk domains in the banking literature. Building on this foundation, Chapter 4 traces how these mechanisms appear in practice within the Bank and how they create pathways through which control problems translate into operational risk exposures. The aggregate dimensions and themes reported below do not represent a new categorisation of control problems. Rather, they organise the empirical material in a way that reflects the control types and dysfunction mechanisms identified in the previous chapters, while capturing how these mechanisms manifest in the Bank's organisational context.

4.3.1 Aggregate Dimension 1: Design-Driven Control Problems

Design-Driven Control Problems encompass weaknesses that originate from how MCS are designed, structured, or configured within the organization. These problems emerge when Action Controls, Result Controls, or structurally embedded Personnel Controls are misaligned with process realities, regulatory constraints, or technological infrastructures. They reflect vulnerabilities arising from the design rather than the enactment of the control system.

This dimension includes three themes:

- Structural Vulnerabilities
- Rule Induced Constraints
- Incentive Misalignment
- Each is presented below.

4.3.1.1 Structure Vulnerabilities

Structural vulnerabilities capture weaknesses embedded in the Bank's organizational architecture, the configuration and integration of its systems, and the operational structures within which Action Controls are implemented. These vulnerabilities arise when processes depend on fragmented systems, incomplete automation, insufficient IT development, or organizational growth that outpaces structural capacity. Structural weaknesses occur not because rules or procedures are absent, but because the underlying technological infrastructure, organizational, or cross-unit is not sufficiently robust to support the intended control environment.

Interviewees noted that a significant proportion of structural vulnerabilities stem from insufficiently configured systems, partial automation, and gaps between procedural design and system implementation. One interviewee reflected this clearly:

> *"In the last audit, we identified issues related to careless implementation of the bank's complete procedural controls, improper configuration of systems according to the bank's policy requirements, and non-automatic processes." (INT-03)*

This highlights a recurrent pattern, where even when procedures are defined, systems and processes are not consistently aligned with them, resulting in operational weaknesses that are structural rather than behavioural.

Structural constraints are also closely tied to the pace of technological development. Several interviewees described delays arising from IT dependencies and the need to rely on external vendors during system improvements:

"Delays typically arise, especially concerning IT aspects, where further development is often required on specific platforms to effectively manage risks. In such instances, we may engage external expertise to expedite solutions… Meanwhile, we also try to manage the situation with people, until we have a software–automatic solution" (INT- -05)

The Bank's organizational growth has further amplified these structural demands. As one interviewee emphasised that the institution's expanding operations require new investments:

"The bank is constantly growing, this growth is organic, and I think it needs additional staff and investments in specific systems for operational risk management, such as to develop an 'Early warning system' for operational risk, similar to KRI (Key Risk Indicators)"(INT-09)

This reflects a structural misalignment between expanding organizational activities and the technological and human resources required to support them.

Structural vulnerabilities also become visible when automated processes fail to execute fully, particularly in high-volume areas such as credit card processing:

"For instance, ten days ago, we had an incident with credit cards. Credit cards are used within one month, and then we have about 15 days to make the payment. If you've made 500 Euros of expenses within the month, the calculation is made, you owe 500 Euros but you also have about 15 days into the following month to pay off the credit card debt without interest. Sometimes, when processes fail within the bank, the calculation begins and is completed for 10,000 clients, however [in the last case] the process failed for about 2,000 clients who were left out. Now, it might coincide with a weekend, a holiday, or a Monday, and several days might pass, making it difficult to notice immediately, and the potential issue starts escalating slightly" (INT-10)

Here, a system-level failure created a large-scale risk exposure, demonstrating how partial or inconsistent process automation can generate operational disruptions that may remain undetected for days due to timing, workload, or holiday cycles.

Several interviewees noted that structural fragmentation continues to force reliance on manual processes where systems are not yet fully synchronized:

"There are still manual processes, for example, if a client goes to a branch and tells that their card is lost and they want it blocked, we don't have a synchronized system where once it's blocked there, it should also be blocked on our side through another channel. It's a kind of pain, it's tiring-block it here, block it there"(INT-10)

In such cases, weak system integration creates operational inefficiencies and increases the likelihood of errors or delays in implementing critical controls.

Structural vulnerabilities also emerge from cross-unit dependencies, particularly where cybersecurity risks intersect with operational responsibilities:

> *"The Legal Sector may face some legal risks arising from other professional units of the Bank… increasing cyber security efforts, including ransomware and phishing that have become more frequent… threat actors use security weaknesses in the IT infrastructure of companies to carry out cyber-attacks which damage clients but also the Bank." (INT-11)*

This example demonstrates how structural weaknesses in IT infrastructure and interdepartmental dependencies expose the organization to external threats that challenge operational continuity.

Based on the interviews structural weaknesses arise from misalignment between the Bank's procedural expectations and its technological, organizational, and infrastructural capacities. Whether through delayed IT development, insufficient system configuration, incomplete automation, reliance on manual workarounds, or fragmented cross-unit responsibilities, these vulnerabilities reflect systemic conditions that limit the effectiveness of Action Controls. Structural Problems therefore represent a foundational design weakness that shapes the conditions under which other control problems emerge.

4.3.1.2 Rule Induced Constraints

Rule-induced constraints arise when Action Controls are formulated as strict rules or procedures that are insufficiently adaptable to the operational banking environment. In banking, rule-based controls are essential, but when they become overly prescriptive, they generate bottlenecks, delays, or compliance tensions. This theme captures how legal mandates, regulatory strictness, and procedural rigidity constrain effective control execution. One manager clearly described this:

> *" The challenge is the legislation in force, court disputes, legal risk-The operational risk also occurred due to these cases. Improvements in the legal environment are very important. Also, the Central Bank of Kosovo should initiate any legislation regarding operational risk" (*INT-09)

Here, regulatory and legal requirements are experienced as rigid, slow, and constraining, inhibiting flexible resolution and embedding delay and cost into processes. The problem is not merely external regulation, but how internal Action Controls are designed to mirror, implement, or depend on these rigid frameworks.

4.3.1.3 Incentive Misalignments

Incentive misalignments emerge when Result Controls, in particular performance evaluation and bonus systems, encourage behaviour that conflicts with prudential risk management. Interviewees highlighted several ways in which incentives create behavioural pressures that interact with control effectiveness. A manager described how employees may feel compelled to compromise internal rules in order to achieve performance metrics tied to financial and job security outcomes:

> "*There is always a risk because people strive to reach targets and objectives, which are often linked to bonuses and, for some, job security. Targets are always challenging, and to achieve them, individuals may sometimes be tempted to violate regulations or internal procedures"* (INT-05)

Another manager expressed concern about the "Management by Objectives" framework, noting that the quality of target-setting itself can create risks:

> "*This is my personal opinion on the performance evaluation system 'Management by Objectives', here we have problems as an institution, because the objectives should always be evaluated according to the 'SMART' system (specific, measurable, achievable, realistic and in time), and in this aspect there is much room to be desired. The pressure to achieve the objectives creates opportunities to compromise with ethics even involuntarily, even though we try to be very rigorous in this aspect sometimes the great pressure to achieve the objectives exceeds this risk without our awareness"* (INT--07).

A manager highlighted the magnitude of bonus-related financial incentives, which significantly shape behaviors:

> "*The threshold level is very high because it is necessary to push the employees to work harder to achieve the objectives. 90 -100% you already get paid - you don't get bonus; 101% gets a bonus, and that bonus then varies. An average for all bank employees, excluding managerial positions, is up to two bonus salaries within the calendar year"* (INT-02)

Additionally, the manager described the governance processes around low performance scores, illustrating how subjective interpretation can shape outcomes:

> "*When the performance evaluation drops to 89%, we organize a meeting with the person who did the evaluation, with the evaluated employee, and one person in the hierarchy. In this meeting, we must see what happened, is there a subjectivism, are there any problems, are there any medical leave that impacted the performance, or are there any other issues. Only after all the circumstances are checked then the monitoring is set" (*INT-02)

These excerpts highlighted an incentive system characterized by high thresholds and pressure to achieve goals, and bonuses substantial enough to influence the behaviour. This tension shows a systemic vulnerability in the design of Result Controls, illustrating how incentives can unintentionally generate or intensify control problems.

4.3.2 Aggregate Dimension 2: Human Capability & Behavioural Control Problems

This dimension encompasses control problems rooted in human behaviour, competence, values, and informal norms. These problems emerge when Personnel Controls and Cultural Controls are insufficiently developed or inconsistently enacted. They reveal vulnerabilities that arise not from the design of controls, but from how people interpret, apply, or circumvent them.

The dimension includes two themes:

- Workforce Capability and Capacity Limitations
- Cultural and Ethical Drift

4.3.2.1 Workforce Capability and Capacity Limitations

Workforce capability and capacity limitations reflect weaknesses in employees' skills, training, experience, or cognitive capacity necessary for reliable work task execution. These issues arise when Personnel Controls, such as selection, training, and development, do not sufficiently equip employees to manage process complexity or detect errors. Capability gaps expose the organization to repeated human-error incidents, inadequate detection of anomalies, and vulnerabilities in frontline functions such as cash operations, and fraud detection. These problems become especially visible in environments where process complexity increases or where technological tools do not compensate for limited human skill.

Interviewees described recurring patterns of human error attributable to insufficient or outdated training. One manager explained how repeated mistakes were traced back to prolonged training gaps:

> *"During the analysis of the controls, we find that the cause is Human Error, and we see that the same person made the same mistake 5 times… we looked at the aspect of training and saw that the person in question has not attended training for 4 years."* (INT-03)

This example illustrates how capability deficits persist when training is neither continuous nor systematically aligned with operational demands. Additionally, this problem reflects not merely individual oversight but a structural weakness in how Personnel Controls ensure ongoing competence.

Repetition of routine operational errors was also reported at the branch level:

> "*Some of the most common errors are those related to the work of cashiers, errors such as differences in the cash register during the reconciliation process, errors in recording customer information, errors in transactions."* (INT-07)

These errors reflect both skill-based vulnerabilities (e.g., currency handling, reconciliation accuracy) and knowledge-based deficits (e.g., accurate customer information recording). Their frequency highlights the risk exposure of front-line processes when capability development does not keep pace with operational demands.

Capability issues were also evident in failure to detect fraudulent or suspicious items, particularly where technical tools were insufficient to compensate for human limitations:

> *"Recently, we had the case of fake €2 coins (metal coins), which for reasons of non-identification by the staff, non-sophisticated machines caused a loss, but the loss was not big, it was somewhat smaller than €5000."* (INT-09)

Through these excerpts we can see that limitations in workforce capability and capacity arise when employees lack the training, experience, or cognitive capacity required to execute controls reliably under varying conditions. These deficits weaken the effectiveness of Action Controls and amplify operational risk exposure across multiple processes

4.3.2.2 Cultural and Ethical Drift

Cultural and ethical drift captures the gradual weakening of shared norms, ethical expectations, and behavioural standards that are intended to guide employee conduct. These vulnerabilities arise when Cultural and Personnel Controls do not consistently reinforce integrity, transparency, and responsibility-taking across the organisation. In this context, drift becomes visible through behaviours such as intentional errors, concealment of misconduct, normalization of procedural violations, and cultural conditions that influence reporting behaviours and inconsistent adherence to ethical expectations. These vulnerabilities emerge when values, norms, and informal expectations within particular groups fail to reinforce compliant and ethical conduct.

Interviewees reported that intentional errors, although statistically infrequent, are particularly problematic because they are often planned, concealed, and difficult to detect through routine controls. As one compliance officer explained:

> *"Intentional errors are challenging to detect immediately because individuals who deliberately engage in misconduct have a plan in advance, consider their actions carefully, and often attempt to conceal them until they are eventually revealed."* **(**INT-05**)**

This illustrates that cultural weaknesses do not manifest only in routine oversight gaps but also in deliberate attempts to bypass controls. The challenge lies in the fact that intentional misconduct can occur despite the presence of formal Action Controls, highlighting the reliance on ethical norms and responsible behaviour to maintain control effectiveness.

Although intentional errors represent a small portion of incidents institutionally, their persistent presence reflects a deeper cultural pattern:

> *"Related to intentional errors in our bank, a statistic I can give you at the level of the institution is around 2%. In order not to make a mistake with statistics, I am calculating it now. And yes, as I said, on average since the period I have managed this sector, the reports consistently average at 2%."* **(**INT-05**)**

The consistency of this figure suggests a stable behavioural risk that is not easily mitigated through procedural reinforcement alone. Even at low frequency, intentional misconduct has disproportionate implications for risk culture, trust, and the credibility of internal controls.

Cultural or ethical deviations were also linked to violations of information security procedures, demonstrating how non-compliance can emerge in operational contexts even when rules are explicit and well-defined. One manager described how disciplinary procedures were triggered following such violations:

> *"We have had cases in the past when there may have been a violation of non-implementation of the information security procedures that are in the bank, and the case as foreseen by the procedure for the management of disciplinary acts, the commission was created, and they handled the case according to that procedure."* **(**INT-08**)**

This example reflects the formal disciplinary response when ethical norms or security protocols are breached, yet the need for disciplinary intervention indicates underlying challenges in achieving consistent cultural adherence.

Perhaps the most illustrative case involves a severe ethical lapse in frontline decision-making, where informal problem-solving practices directly conflicted with formal procedures and risk norms:

> *"There was a case in 2016… when the chief cashier in one of the branches, under pressure from a client, handed over physical cash for an exchange transaction… The chief cashier did not register the transaction in the system because he assumed the client would return the money as agreed. The client did not return the funds… The case was identified as a procedural violation, and the person involved, the branch's chief cashier, was dismissed."* **(**INT-12**)**

This incident demonstrates how social pressure, informal agreements, and deviations from prescribed procedures can lead to significant breaches of ethical standards and operational discipline. It also reveals a presence of a subculture within the branch, where prioritising customer accommodation and informal problem solving were given higher priority over the organisation wide risk and control norms. Although no financial loss was ultimately incurred, this past case reveals a cultural vulnerability. More precisely, this case shows a willingness within the particular branch to override formal controls based on interpersonal trust or perceived customer expectations, which stands in contrast to the stricter control orientation of head-office functions.

4.3.3 Empirical Findings (RQ1): Mechanisms Through Which MCS Generate Control Problems

The findings demonstrate that the Bank's control problems arise from weaknesses across all four types of management control systems identified by Merchant and Van der Stede (2017), namely action controls, result controls, personnel controls, and cultural controls. These weaknesses become visible through five recurring themes: Structural Problems, Rigid Rules Problems, Incentive Problems, Personnel Capability Problems, and Cultural/Ethical Control Problems. Together, these themes form two overarching aggregate dimensions that explain empirical pathways through which MCS generate vulnerabilities in practice.

The first aggregate dimension, Design-Driven Control Problems, captures systemic weaknesses arising from the design and configuration of action controls and result controls. Structural vulnerabilities originate primarily from weaknesses in the design and integration of action controls. The findings show that these problems emerge when systems are improperly configured relative to policy requirements; automated processes are incomplete or prone to failure (e.g., credit card processing outages affecting thousands of clients); operational workflows rely on manual workarounds due to lack of full system synchronization; IT development is delayed or dependent on external vendors; rapid organizational growth outpaces the capacity of existing systems; cybersecurity threats exploit structural vulnerabilities in the IT infrastructure. These issues reveal that Action Controls, while formally established, are structurally undermined by the technological and organizational environment necessary for their effective operation. Rule induced constraints also stem from action controls. When procedures are overly prescriptive or tightly bound to legal mandates, they restrict operational adaptability and can produce bottlenecks and compliance delays. In these cases, rigidity itself becomes a source of risk, producing inefficiencies and impeding timely action.

Incentive misalignments arise from weaknesses in Result Controls, particularly from the design of performance metrics, bonus systems, and evaluation frameworks. High-threshold bonus schemes, subjective evaluation practices, and pressure to meet demanding targets collectively distort behaviour, shifting employees' focus from compliance and accuracy to

target attainment. These misaligned incentives increase the likelihood of corner-cutting, ethical compromise, and underreporting of irregularities, demonstrating how Result Controls can unintentionally generate behavioural vulnerabilities.

The second aggregate dimension, Human-Capability & Behavioural Control Problems, reflects weaknesses in Personnel Controls and Cultural Controls, demonstrating how behavioural and competence-related factors produce additional vulnerabilities. Workforce capability and capacity limitations arise from weaknesses in Personnel Controls, such as selection and training, skill, or operational readiness required to reliably execute controls. Repeated human-error cases, prolonged gaps in training (e.g., employees not trained for four years), and inability to detect fraudulent items (e.g., counterfeit coins) reveal that capability development is uneven and insufficiently aligned with process complexity. Where automation fails or manual processes dominate, these gaps become especially consequential. Thus, weaknesses in Personnel Controls produce predictable patterns of error across frontline operations.

Cultural and ethical drift emerge from weakness in Culture Controls, such as, inconsistencies in shared norms, ethical standards, and informal expectations that shape behaviour. Instances of intentional errors (even if statistically small), violations of information security procedures, concealment of misconduct, client-pressure compliance, and informal rule-bending reflect areas where Cultural Controls do not sufficiently reinforce ethical and responsible behaviour. These patterns show that the informal cultural environment does not uniformly support compliance, integrity, or transparency, allowing behavioural deviations to surface despite formal control structures.

The findings show that the Bank's control problems arise from systemic misalignments between control design and the organizational conditions required for their effective functioning. Both technological and structural limitations, and human and behavioural dynamics contribute to the emergence of these vulnerabilities. In this way, the findings provide the empirical basis for examining how control problems generated within different management control systems translate into operational risk exposures. More specifically, the following sections will show how these problems materialize as operational risk exposures aligned with Basel II/III classifications.

4.3.4 Empirical Findings (RQ2): How these Mechanisms Map to Operational Risk Categories

This section addresses the subsequent research question:

RQ2: How do the identified control problems contribute to the emergence of operational risk within the bank?

Drawing on the five themes established under the two aggregate dimensions, the findings show that each category of control problem maps onto specific Basel II/III operational risk categories. Importantly, the themes do not operate in isolation; rather, their interaction creates systemic conditions in which operational risk events emerge. The analysis below integrates empirical evidence with Basel-driven risk typologies to demonstrate how control weaknesses translate into actual operational risk exposure

Structural Problems arising from system misconfigurations, incomplete automation, fragmented processes, and insufficient monitoring constitute a primary pathway through which the Bank becomes exposed to several Basel II/III operational risk categories. The interview data clearly shows that structural weaknesses undermine the reliability, completeness, and continuity of core banking processes, producing vulnerabilities that may materialize in Basel II/III categories: 1). Clients, Products and Business practices; 2). Execution, Delivery and Process management; 3). Employment practices and Workplace safety; 4). Internal Theft / Fraud; 5). External Theft/Fraud; 6). Systems; 7). Damage to Physical/Tangible assets.

The Interviewee reported various instances identified various instances where system configurations deviated from policy requirements, directly contributing to operational inefficiency and process failure.

> *"In the last audit, we identified issues related to careless implementation of the bank's complete procedural controls, improper configuration of systems according to the bank's policy requirements, and non-automatic processes." (IN-03)*

Improper system setup and the persistence of non-automated workflows place additional pressure on staff to manually execute or monitor processes, increasing the likelihood of human error, delayed processing, and inaccurate transaction handling. Within Basel II/III, these events fall under Execution, Delivery & Process Management risk, the category most associated with process design failures and control lapses.

Structural gaps also arise when the Bank is unable to implement automated controls due to system limitations or vendor constraints. As one manager explained:

> *"If I had put them on a percentage scale, I would say somewhere around 70% we have our setups, and 30% that mistakes can occur… the possibility of setting automatic control is almost impossible."* (INT-06)

This highlights structural constraints, whether technological, or stemming from vendor dependencies that limit the Bank's ability to embed robust automated safeguards. Such conditions increase reliance on manual oversight and expose the institution to Business Disruption and System Failures, especially when systemic errors propagate across high-volume products.

Structural weaknesses translate directly into significant process failures, particularly when system defects remain undetected for extended periods. One senior employee recalled:

> "*I do remember a situation that alarmed the entire bank. It was when it was discovered that for business credit cards, we weren't calculating interest, we weren't charging interest, that's what it was*." (INT-10)

Failure to calculate or charge interest is a textbook example of Clients, Products & Business Practices risk, capturing situations where system or procedural deficiencies result in incorrect client outcomes. These events can expose the Bank to client complaints, remedial obligations, regulatory sanctions, and reputational damage.

One of the most serious structural failures described in the interviews was the Bank's inability to differentiate transaction types required for VISA/MasterCard mandates. The consequences included a €160,000 loss:

> "*Company X (service provider) failed to provide a practical differentiation… and negligence in reading the instructions… the monetary loss was around €160,000."* (INT-11)

This incident illustrates how external vendor failures, internal negligence, and structural dependence on third-party systems can intersect to produce major operational losses. Within the Basel framework, this aligns with several risk categories: Execution, Delivery & Process Management (process design failure), External Fraud (clients receiving funds prematurely), Business Disruption (systemic inability to process transactions correctly). The case exemplifies how structural problems generate risk events whose magnitude far exceeds the scope of the originating control failure.

Taken together, these findings demonstrate that Structural Problems form a foundational layer of operational vulnerability. They weaken the reliability of core banking processes, increase dependence on manual workarounds, magnify human-error exposure, and reduce the Bank's resilience to system failures and vendor dependencies. The structural weaknesses identified in RQ1 thus provide the causal mechanisms that explain why the Bank experiences:

- Execution and process errors;
- External and internal fraud exposures;
- System and automation failures;
- Misreporting and compliance gaps; and
- Financial losses resulting from system design limitations.

These patterns illustrate that operational risk does not arise randomly, but emerges from persistent, structural vulenrabilities that impair the functioning of the Bank's management control systems.

Table 13 shows how the structural vulnerabilities identified in RQ1 translate into specific operational risk exposures under the Basel II/III classification framework.

Table 13: Structural Vulnerabilities and Associated Basel II/III Operational Risk Categories

Structural Vulnerability	**Basel II/III Operational Risk Category**	**Representative Evidence**
System misconfiguration & non-automated processes	Execution, Delivery & Process Management	"Improper configuration of systems… and non-automatic processes" (IN-03)
Incomplete automation; technological constraints	Business Disruption & System Failures	"70% we have our setups… 30% that mistakes can occur… setting automatic control is almost impossible" (INT-06)
Misapplication of calculation processes	Clients, Products & Business Practices	"We weren't calculating interest… we weren't charging interest" (INT-10)
Vendor dependence & processing breakdown (FastFund/MoneySend)	Execution, Delivery & Process Management; External Fraud	"ASSECO failed to provide a practical differentiation… loss was around €160,000" (INT-11)
Non-reporting of relevant events	Compliance Risk; Reporting Risk	"Such cases are not reported to Operational Risk" (INT-12)
Lack of continuous monitoring & cross-sector coordination	Execution, Delivery & Process Management	"Keeping people 'aware'… meetings with many people… ongoing process" (INT-13)

Source: Own work.

4.3.4.1 Rule Induced Constraints and the Emergence of Operational Risk

Rule induced constraints arise when formal rules, legal requirements, or regulatory frameworks impose constraints that reduce the Bank's operational flexibility and slow the resolution of risk-related issues. Unlike structural vulnerabilities, which stem from system design, rule-induced constratints originate from external regulatory mandates and legal

obligations that the Bank must follow, even when they create bottlenecks or expose the Bank to unintended forms of risk.

These problems map most directly onto the Basel II/III categories of Legal Risk, Compliance Risk, and Execution, Delivery & Process Management Risk, as well as broader elements of Business Practices Risk.

The interview evidence shows that the legal environment itself acts as a structural constraint that generates operational risk. As one manager explains:

"The challenge is the legislation in force, court disputes, legal risk. The operational risk also occurred due to these cases. Improvements in the legal environment are very important. Also, the Central Bank of Kosovo should initiate any legislation regarding operational risk. (INT-09)

This demonstrates that court processes, outdated legislation, and slow judicial procedures can directly create operational risk events. These include prolonged legal disputes, delayed contract enforcement, and inconsistencies between internal procedures and national regulatory requirements. Such exposures fall under Basel's Legal Risk, which is explicitly recognised as a component of operational risk.

The interview also shows that rigid or underdeveloped regulatory guidelines, especially in the area of operational risk creates uncertainty and increase the likelihood of compliance gaps. When the regulatory framework does not clearly define obligations or expectations, the Bank must implement internal interpretations that may later be challenged or corrected by supervisory authorities.

This contributes to:

- Compliance Risk, due to potential non-compliance with unclear regulations;
- Operational delays, as staff must navigate ambiguous or outdated regulatory expectations; and
- Process Management Risk, since rigid rules limit the Bank's ability to adapt procedures to practical realities

Rigid legal and regulatory rules reduce the Bank's ability to redesign processes, embed automated controls, or streamline operational workflows. When the Bank must follow strict legal steps even in cases where operational realities require flexibility this leads to: procedural backlogs, delayed incident resolution, increased resource allocation to manage exceptions errors arising from long, rigid process chains. These effects correspond to Basel's Execution, Delivery & Process Management Risk, which includes losses arising from failed internal processes, even when the root cause lies outside the organisation (e.g., imposed by the legal system).

Rule induced constraints reveal how the operational environment beyond the Bank's immediate control legislation, court procedures, and regulatory guidelines creates structural constraints that generate operational risk. Thus, rigid rules contribute to operational risk not through system design or human error, but through external institutional constraints that limit the Bank's ability to implement effective controls and timely remediation.

Table 14 shows how rule induced constraints identified in the findings translate into specific Basel II/III operational risk categories, supported by representative interview evidence.

Table 14: Rule Induced Constraints and Operational Risk Mapping

Rule Induced Constraint	**Basel II/III Operational Risk Category**	**Representative Evidence**
Legislative rigidity and slow legal processes	Legal Risk	"The challenge is the legislation in force, court disputes, legal risk… operational risk also occurred due to these cases." (INT-09)
Regulatory rules insufficient or rigid, requiring improvement	Compliance Risk	"Improvements in the legal environment are very important… CBK should initiate legislation regarding operational risk." (INT-09)
Rigid regulatory steps limiting operational flexibility	Execution, Delivery & Process Management Risk	"Court disputes and legislation in force created operational risk." (INT-09)

Source: Own work.

4.3.4.2 Incentive Misalignments and the Emergence of Operational Risk

Incentive misalignments arise when the design of Result Controls creates behavioral pressures that distort employee decision-making, weaken compliance, and increase exposure to operational risk. In the Bank, the performance evaluation and bonus system, particularly the high threshold for earning incentives, generates strong motivational dynamics that influence how employees navigate procedures, targets, and ethical boundaries. These pressures map primarily onto Execution, Delivery & Process Management Risk and Clients, Products & Business Practices Risk within the Basel II/III operational risk framework.

The Bank's bonus system awards incentives only when employees exceed 101% of their performance objectives. This encourages employees to push aggressively toward targets. As one manager explained:

> *"The threshold level is very high because it is necessary to push the employees to work harder to achieve the objectives… 90 to 100% you already get paid – you don't get bonus; 101% gets a bonus… up to two bonus salaries in the year."* (INT-02)

Such high-performance thresholds can generate pressure-induced behavioral risk, where employees prioritize target attainment over procedural integrity. In the Basel framework, this aligns most closely with Execution, Delivery & Process Management Risk, as pressure can lead to procedural shortcuts, incomplete documentation, or deviations from required processing steps.

Interviewees openly acknowledged that the pressure to meet targets combined with the bonus system and, for some, job security concerns create circumstances where employees may knowingly violate procedures:

> *"There is always a risk because people strive to reach targets and objectives… to achieve them, individuals may sometimes be tempted to violate regulations or internal procedures."* (INT-05)

This pattern aligns with Clients, Products & Business Practices Risk, as behavior motivated by performance pressure can lead to non-compliant handling of client transactions or failure to follow established standards. It also reinforces exposure to Execution, Delivery & Process Management Risk, as procedural deviations increase the likelihood of mistakes, inconsistent handling, and operational irregularities.

Thus, Incentive misalignments generate operational risk because they originate in the design of the incentive system itself. The design of Result Controls, such as high bonus thresholds, target-linked rewards, and performance evaluation criteria shapes employees' motivational environment in ways that can unintentionally produce dysfunctional behaviour. These design features create strong behavioural pressures, which in turn increase the likelihood that employees will engage in practices that compromise compliance, accuracy, or ethical standards. In this sense, the source of operational risk resides not merely in individual behavior, but in the design-driven incentives that systematically motivate boundary-seeking, corner-cutting, or non-compliant actions.

Table 15 shows how incentive misalignments arising from the design of Result Controls generate specific Basel II/III operational risk exposures, supported by representative interview evidence.

Table 15: Incentive Misalignments and Operational Risk Mapping

Incentive Misalignment	**Basel II/III Operational Risk Category**	**Representative Evidence**
High performance threshold (bonus only at 101%) creating pressure	Execution, Delivery & Process Management Risk	"90 to 100% you already get paid – you don't get bonus; 101% gets a bonus…" (INT-HR-02)
Target-driven behavioural pressure leading to boundary-seeking	Execution, Delivery & Process Management Risk	"People strive to reach targets… tempted to violate regulations or internal procedures." (INT-CO-05)
Target-linked job security increasing non-compliance likelihood	Clients, Products & Business Practices Risk	"To achieve them, individuals may sometimes be tempted to violate… procedures." (INT-CO-05)

Source: Own work.

4.3.4.3 Workforce Capability and Competence Limitations and the Emergence of Operational Risk

Workforce Capability and Cmpetence Limitations arise when employees lack the skills, training, adaptability, or capacity needed to reliably perform tasks and interact effectively with increasingly complex systems. These capability gaps create fertile conditions for human error, detection failures, and responsibility avoidance, all of which may be core pathways through which operational risk materializes. Within the Basel II/III framework, these issues most prominently map onto Execution, Delivery & Process Management Risk, Internal Fraud (negligent misconduct), and Business Disruption due to Human Factors.

The interviews consistently highlight that the "human factor" is perceived as the weakest link in the Bank's control chain, particularly in areas where automated or technical controls are insufficiently developed. As the manager emphasized:

"The human factor in security is considered the weakest link of this chain, because security must be layered, that is, it must be a combination of measures that must be taken, in addition to the technical measures that are established for the set-up of automated controls, to prevent a mistake, let's not call it misuse, but human mistakes, definitely a lot of work must be done in the direction that the human factor become aware, educated about the potential risks" (INT-08).

This recognition reflects a core Basel operational risk mechanism: Execution, Delivery & Process Management Risk, where human error leads to transaction mistakes, inaccurate data

handling, or failure to follow procedures. When employees lack the knowledge or awareness needed to identify risks, the Bank becomes more vulnerable to process breakdowns and security lapses, especially when layered controls rely on human vigilance rather than automated safeguards.

The Bank also faces capability challenges stemming from external labour market conditions, including increased migration and shortages of qualified staff. A senior interviewee described:

> *"What is one of the risks that we need to be careful about is the labour force, the qualified staff. From January of this year, we have significant migration, which has found the market unprepared. I mean, this is considered a risk for us, for qualified staff, since the opportunities for qualified staff are now also open in markets abroad" (INT-13)*

Loss of experienced personnel and difficulty replacing them with equally qualified staff creates operational fragility. Within the Basel framework, this aligns with Business Disruption & System Failures, specifically human resource disruption, and Execution, Delivery & Process Management Risk, since staffing shortages degrade process reliability and increase the likelihood of mistakes.

Another capability-related vulnerability concerns the alignment of older staff with modern systems. As a manager explained:

> *"[As risks], I would say, old staff and their alignment or adaptation to digital processes. Human errors are very present in all processes and in some cases have a great impact. Currently, our systems are not very advanced, and I have personally advocated for changes. The old staff do not want changes, and they are afraid of changes, this then decreases responsibility, and when the responsibility decreases, then the mistakes increase" (INT-09)*

This highlights a structural mismatch between employee capability and system complexity. Resistance to adopting new digital processes weakens both compliance and execution accuracy.

These consequences fall under Execution, Delivery & Process Management Risk, which captures operational losses arising from mistakes in process execution, and under Compliance Risk when resistance leads to avoidance or improper application of updated procedures.

Personnel Capability Problems generate operational risk through a competence–process mismatch: when employees lack the skills or willingness needed to operate within technologically evolving systems, the reliability of control execution deteriorates. Skill shortages, migration-driven capacity gaps, and resistance to digital change collectively

weaken the Bank's control environment, making human error more frequent and more consequential. These vulnerabilities align with the main Basel operational risk categories associated with: Execution, Delivery & Process Management (mistakes, process errors, miss- entries); Business Disruption due to Human Resource Instability (staff shortages, turnover); and Compliance Risk (responsibility avoidance, resistance to new processes).

Table 16 shows how workforce capability and capacity limitations link into specific Basel II/III operational risk categories, supported by representative interview evidence.

Table 16: Workcforce Capability and Competence Limitations and Operational Risk Mapping

Workforce Capability and Capacity Limitation	**Basel II/III Operational Risk Category**	**Representative Evidence**
Human factor as weakest link in layered security controls	Execution, Delivery & Process Management Risk	"The human factor in security is considered the weakest link… human factor becomes aware, educated about the potential risks." (INT-08)
Migration-driven staff shortages reducing operational capacity	Business Disruption & System Failures; Execution, Delivery & Process Management Risk	"We have significant migration… this is considered a risk for us, for qualified staff." (INT-13)
Legacy workforce resistance to digital systems leading to errors	Execution, Delivery & Process Management Risk; Compliance Risk	"Old staff… are afraid of changes… responsibility decreases, then the mistakes increase." (INT-09)

Source: Own work.

4.3.4.4 Cultural and Ethical Drift and the Emergence of Operational Risk

Cultural and ethical drift emerge when cultural control, shared norms, ethical expectations, and behavioural standards fail to guide employee decisions, especially in situations where controls depend on professional integrity and collective awareness. Weak cultural control, or insufficient ethical awareness can create conditions in which misconduct, concealment, or non-compliance occur. In the case bank, these weaknesses are not widespread but appeared within certain units. These weaknesses map to several Basel II/III risk categories, most notably Internal Fraud**,** Clients, Products & Business Practices Risk, and Execution, Delivery & Process Management Risk**.**

The interview evidence demonstrates that ethical failures can directly lead to fraudulent practices that bypass formal controls. A branch manager recalled a major case involving deliberate deception:

> "*The biggest damage that was done in this branch was in 2011, this case had to do with the creation of fictitious contracts by some employees in the bank, where these were contracts created for term deposit, and intentionally by persons involved, these contracts were not processed in the system, so these contracts were not registered in the system. As a result of this manipulation, the damage caused was around 100,000 Euros"* (INT-BM-07)

Here, employees intentionally created term deposit contracts but concealed them from the Bank's systems. This is a clear case of Internal Fraud**.** This incident shows not only individual ethics but also a local subculture weakness in that branch, in which such manipulation was possible and temporarily tolerated despite the formal control environment. This case, reveal how cultural weaknesses, such as tolerance for unethical practices or insufficient ethical oversight can produce major losses.

Another incident illustrates how ethical compliance can weaken under interpersonal or client pressure. A chief cashier, acting outside procedure, handed over cash based solely on verbal trust:

> *"There was a case in 2016 (on 30.12.2016) when the chief cashier in one of the branches, under pressure from a client, handed over physical cash for an exchange transaction. They had agreed that the cash would be returned within the same day. The chief cashier did not register the transaction in the system because he assumed the client would return the money as agreed. The client did not return the funds as promised, and by the end of the day, the cashier had to register the transaction in the system. The case was identified as a procedural violation, and the person involved, the branch's chief cashier, was dismissed. The client returned the funds the next day, on 31.12.2016, in euros, the same currency as received. In this case, the bank incurred no loss; the total loss was zero"* (INT-OR-12)

Although the bank ultimately incurred *no financial loss*, the case reveals a cultural vulnerability, specifically a willingness within one branch-level to override controls based on interpersonal trust or perceived customer expectations**.** This suggests the presence of a local subculture that placed higher value on client accommodation than on strict procedural adherence. Such behaviours fall under Clients, Products & Business Practices Risk, since staff actions breached proper treatment and handling of client funds; and also under Execution, Delivery & Process Management Risk, due to failure to record and execute the transaction appropriately. It also represents a breakdown in ethical discipline and responsibility**,** demonstrating how cultural norms "helping the client," trust-based reasoning, can override formal controls.

A further dimension of cultural vulnerability is the ongoing need to maintain ethical and risk-related awareness across the workforce. A board member mentioned:

> *"One of the main challenges here is keeping people 'aware' at all times about the risk"* (INT-BOM-13)

This illustrates the fragility of risk culture: staff may not consistently internalise or apply ethical and risk-related expectations unless continuous reinforcement is present. Such weaknesses fall within the Execution, Delivery & Process Management Risk, where failures of ethical vigilance contribute to late detection, poor monitoring, or procedural lapses.

Overall, these findings indicate that Cultural and Ethical Drift did not characterise the organisation as a whole but emerged within particular branches where locally shared norms diverged from the Bank's formal risk expectations, forming a subculture patterns. These subcultures create conditions through which operational risk can emerge. Therefore, when ethical norms fail, whether through intentional misconduct, pressure-driven deviations, or inconsistent risk awareness across different units, then formal controls become ineffective. These failures manifest as: Internal Fraud (intentional manipulation, concealment, creation of fictitious contracts**);** Clients, Products & Business Practices Risk (violations of ethical treatment and procedural obligations toward clients); and Execution**,** Delivery & Process Management Risk (recording failures, improper transaction handling, inconsistent risk vigilance). Thus, cultural weaknesses represent a critical behavioural pathway through which the Bank's management control system becomes vulnerable to operational failure.

Table 17 shows how Cultural and ethical drift link into specific Basel II/III operational risk categories, illustrated through representative interview evidence.

Table 17: Cultural/Ethical Control Problems and Operational Risk Mapping

Cultural/Ethical Control Problem	Basel II/III Operational Risk Category	Representative Evidence
Intentional manipulation and concealment of fictitious contracts	Internal Fraud	"Employees… created fictitious contracts… intentionally not processed in the system… damage around 100,000 Euros." (INT-07)
Procedural override due to client pressure and trust-based decisions	Clients, Products & Business Practices Risk; Execution, Delivery & Process Management Risk	"Under pressure from a client… handed over physical cash… did not register the transaction… procedural violation." (INT-12)
Weak ethical awareness and inconsistent risk vigilance	Execution, Delivery & Process Management Risk	"One of the main challenges… keeping people 'aware' at all times [about the risk]." (INT-13)

Source: Own work.

Table 18 shows the link between the control problems identified in RQ1 and the corresponding operational risk categories defined by the Basel II/III framework. It provides a consolidated overview of how each control-problem theme contributes to specific forms of operational risk, based on the empirical findings presented in this chapter.

Table 18: RQ1 Themes Mapped to RQ2 Operational Risk Categories

RQ1 – Control Problem Themes	RQ2 – Basel II/III Operational Risk Categories
Structural Vulnerabilities	• Execution, Delivery & Process Management Risk • Business Disruption & System Failures
Rule Induced Constraints	• Legal Risk • Compliance Risk • Process Management Risk
Incentive Misalignments	• Clients, Products & Business Practices Risk • Execution, Delivery & Process Management Risk

To be continued

Table 18: RQ1 Themes Mapped to RQ2 Operational Risk Categories (cont.)

RQ1 – Control Problem Themes	RQ2 – Basel II/III Operational Risk Categories
Workforce Capability and Capacity Limitations	• Execution, Delivery & Process Management Risk • Business Disruption (Human Resource Disruption) • Compliance Risk
Cultural and Ethical Drift	• Internal Fraud • Clients, Products & Business Practices Risk • Execution, Delivery & Process Management Risk

Source: Own work.

4.3.5 Triangulation through Documentary Evidence: Loss Event Report Analysis

To strengthen the credibility of the findings and ensure methodological triangulation, documentary evidence from the Bank's internal Loss Event Report (LER) was analyzed alongside the interview data. The Bank provided two structured summaries of operational loss events: (1) an aggregation by loss event type following Basel II/III categories (see table 19), and (2) an aggregation by root cause (People, Processes, Systems, External Factors), (see table 20). Monetary amounts were removed for confidentiality, but the number of events, their categorisation, and descriptive summaries were provided in full.

Together, these reports offer an independent empirical source that allows comparison between the Bank's actual recorded operational losses and the control problems identified in the qualitative interviews.

Table 19: Distrbution of Loss Events by Loss Event type

DESCRIPTION	No OF EVENTS	SHARE IN % (No. of events)
1. Clients, Products and Business practices	1	1%
2. Execution, Delivery and process management	99	73%
3. Employment practices and Workplace safety	0	0%
4. Internal Theft / Fraud	0	0%

To be continued

Table 19: Distribution of Loss Events by Loss Event type (cont.)

DESCRIPTION	No OF EVENTS	SHARE IN % (No. of events)
5. External Theft/Fraud	4	3%
6. Systems	31	23%
7. Damage to Physical/Tangible assets	0	0%
Total	**135**	**100%**

Source: Own work.

Note. Data adapted from the Bank's *Internal Loss Event Report* (2023). Unpublished internal document provided in anonymized form.

The Bank's loss-event distribution provides an overview of its operational risk profile. As summarized in Table 19, Execution, Delivery & Process Management accounts for the majority of recorded events, representing 73% of all incidents (99 out of 135). A further 23% relate to Systems failures (31 events). Losses associated with External Fraud appear infrequently (4 events), while no loss events were reported under Clients, Products & Business Practices, Employment Practices, Internal Fraud, and Physical Damage.

Table 20: Distribution of Loss Events by causes

DESCRIPTION	No OF EVENTS	SHARE IN % (No. of events)
1. People	96	71%
2. Processes	0	0%
3. Systems	33	24%
4. External factors	6	4%
Total	**135**	**100%**

Source: Own work.

Note. Data adapted from the Bank's *Internal Loss Event Report* (2023). Unpublished internal document provided in anonymized form.

As shown in Table 20, 71% of all incidents were attributed to People (96 events), followed by Systems, which accounted for 24% (33 events). External Factors represented 4% of incidents (6 events), while no Process-related events were recorded during the reporting period.

Detailed descriptions of the underlying causes (e.g., types of human errors, system failures, and technology-related issues) are provided in Appendix 8, where each event type is documented in detail as reported by the Bank.

This distribution pattern indicates that the Bank's operational risk exposure is dominated by errors in process execution, manual-processing failures, system weaknesses, and interface breakdowns between operational staff and the Bank's IT infrastructure. These patterns closely reflect the mechanisms identified in the interview analysis, particularly Structural Problems and Human Capability & Behavioural Control Problems.

4.4 Discussion

In this discussion, we examine how the empirical evidence obtained through the qualitative case study extends, refines, or challenges the conceptual model developed in Chapters 2 and 3. Chapter 2 identified the main control problems and dysfunction mechanisms associated with different types of management control systems, while Chapter 3 showed how these mechanisms become linked to operational risk within the banking context. Building on this foundation, Chapter 4 investigates how these mechanisms become visible in practice within the Bank.

The first pathway, design–use misalignment, captures vulnerabilities that arise when the intended design of controls diverges from how they are implemented, interpreted, or used in practice. Such misalignments may occur when systems are fragmented, processes are inconsistently executed, or gaps emerge between formal procedures and operational realities. These divergences weaken the effectiveness of controls and create conditions under which operational errors or unintended behaviours can occur.

The second pathway, behavioural–institutional coupling, highlights how behavioural norms, cultural expectations, incentives, and institutional routines interact with formal controls. These interactions may reinforce control effectiveness, but they may also undermine controls by normalising workarounds, shaping local risk perceptions, or generating pressures that contribute to non-compliant or error-prone behaviour.

Together, these two pathways provide the conceptual foundation against which the empirical findings are interpreted. The following subsections examine how the empirical evidence confirms, refines, or qualifies these pathways, beginning with the role of structural vulnerabilities in shaping design–use misalignment.

4.4.1 Discussion on Structural Vulnerabilities

The empirical findings both confirm and extend how structural problems are conceptualised in literature. As discussed in Chapter 3, prior research typically frames structural problems as organizational or governance-related weaknesses that shape how management control systems

(MCS) operate in practice. These include fragmentation and unclear boundaries between functions (e.g., Al-Amri & Davydov, 2016; Butler & Brooks, 2024; Cornwell et al., 2023; Lim et al., 2017; Soin & Collier, 2013), excessive centralisation of control responsibilities (Rad, 2016; Sabanova & Kudinska, 2022) and the decoupling of risk management activities from day-to-day operations (e.g Hartmann & Slapničar, 2007; Ringgaard et al., 2025). Structural deficiencies also arise when operational risk management (ORM) is insufficiently embedded into governance mechanisms, such as reporting lines, committee structures, and decision processes, resulting in weak feedback loops and unclear accountability (Cohn et al., 2014; Gurd & Helliar, 2017).

The empirical findings refine this view by demonstrating that, within the studied bank, structural problems manifest less as governance misalignments and more as socio-technical vulnerabilities embedded in the Bank's operational infrastructure. The theme of *Structural Vulnerabilities* captures weaknesses in system configuration, automation, and cross-process integration. These weaknesses arise when processes depend on fragmented systems, incomplete automation, insufficient IT development, or organisational growth that outpaces the Bank's structural capacity. Importantly, structural vulnerabilities emerge not because rules or procedures are poorly designed, but because the underlying technological and organisational infrastructure is not robust enough to support their reliable use. Examples include unsynchronised multi-channel card blocking, system errors affecting thousands of credit card accounts, IT vendor limitations that delay mandatory updates, and the absence of early-warning or KRI-type systems needed for real-time monitoring.

This shift represents a refinement of the structural perspective in the literature. While prior research emphasises structural fragmentation (Al-Amri & Davydov, 2016), hierarchical arrangements (Gurd & Helliar, 2017), and governance integration (Siaw Ofori et al., 2025), the empirical findings point to the importance of operational and infrastructural structure. Structural problems in practice are less about formal hierarchy and more about the alignment between processes, information systems, and automation capabilities. This does not contradict the literature; rather, it makes the abstract notion of "structural problems" more concrete by showing how structural weakness materialises inside an operational banking environment.

Accordingly, the empirical results refine the theoretical understanding of structural control problems by demonstrating that structural vulnerabilities can persist despite the presence of well-designed rules and procedures when the supporting infrastructure lacks the capacity or integration needed for reliable control execution. In this way, the findings contribute a more granular, operationally grounded understanding of structural control problems, enriching the theoretical model with a socio-technical dimension that is only implicitly acknowledged in the literature.

Therefore, while these insights clarify how structural vulnerabilities contribute to operational risk, the findings also show that design-related weaknesses are not confined to systems and

infrastructure, but extend to the configuration of incentive systems, which is discussed in the next subsection.

4.4.2 Discussion on Incentive Misalignments

The literature reviewed in Chapter 3 establishes a clear link between misaligned incentive structures and behavioural distortions that elevate operational risk. Prior research shows that poorly designed or inconsistently applied incentive systems, both monetary and non-monetary can generate moral hazard, short-termism, manipulation, and weakened ethical norms (Acrey et al., 2011; Cohn et al., 2014; Murphy, 2001). Studies emphasise that highly performance-sensitive compensation schemes encourage excessive risk-taking (Acrey et al., 2011; Huston & James, 1995) and that cultural reinforcement within banking environments amplifies these effects, contributing to "ethical blindness" and dishonest behaviour (Cohn et al., 2014; Faugère & Stul, 2021; Posch, 2020). The literature further highlights that subjective or difficult performance evaluation systems undermine fairness perceptions and can trigger opportunistic or non-compliant behaviours (Merchant & Van der Stede, 2017; Tran et al., 2021). Collectively, these studies conceptualise incentive problems as behavioural phenomena that may trigger control problems when employees experience tension between target achievement and procedural integrity.

The empirical findings from the case bank, however, refine and extend this view. In the qualitative data, incentive-related vulnerabilities arise not only from behavioural pressures but more fundamentally from the design and practical use of the Bank's performance evaluation system. Interviewees repeatedly emphasised the structural configuration of the incentive scheme, most notably the requirement to exceed 101% of objectives to qualify for any bonus, inconsistencies in the application of SMART criteria, and the heavy reliance on Management by Objectives as the primary source of risk-relevant distortion. These design features create conditions in which employees prioritise target attainment over procedural integrity, thereby generating operational risk through a misalignment between formal result controls and risk-management objectives. In this respect, the data suggest that incentives in the case bank function as design-driven misalignments that shape how employees interpret procedures, prioritise tasks, and navigate trade-offs between performance targets and compliance obligations.

This repositioning does not contradict the theoretical model; rather, it enriches it by showing that incentives operate at the boundary of the two mechanisms identified from the literature. Incentive Misalignments are, at their core, *design-driven* dimension. They originate in the structural configuration of result controls, but they also exert powerful behavioural effects (Faugère & Stul, 2021) that interact with cultural norms (Butler & Brooks, 2024), ethical judgements (Laguecir and Leca, 2022), and institutional routines (Moosa, 2017). The empirical evidence therefore extends the literature by highlighting the dual nature of incentive systems: they are simultaneously elements of the formal design of the control system and behavioural

forces that lead employees to risk-generating practices. Recognising this dual role enables a more nuanced understanding of how incentives contribute to operational risk and clarifies why, in the empirical data, they belong within the aggregate dimension of Design-Driven Control Problems, while still maintaining conceptual links to behavioural-institutional dynamics.

In addition to highlighting incentives as a hybrid design–behaviour mechanism, the findings underscore that the effectiveness of controls also depends on whether employees have the capability and capacity to operate within these systems. The next subsection discusses how personnel-related vulnerabilities refine this aspect of the theoretical model.

4.4.3 Discussion on Workforce Capability and Capacity Limitations

The empirical findings both confirm and deepen the theoretical expectations concerning personnel-related vulnerabilities in management control systems. At a high level, the case evidence confirms what the literature already implies: people's skills, training, and availability are central to the reliable functioning of controls (Merchant & Van der Stede, 2017), and weak personnel arrangements directly contribute to operational risk exposure (Cohn et al., 2014). In this sense, there is no contradiction between prior research and the empirical material; both recognise that personnel factors matter for the quality of control execution.

The empirical findings, however, refine the way the management control literature conceptually positions personnel issues. Personnel controls are largely embedded within structural arrangements, ensuring that organisational units are appropriately staffed, that control roles are properly assigned, and that governance structures support effective oversight (Merchant & Van der Stede, 2017; van der Kolk, 2019). The case data extend this perspective by pulling personnel-related vulnerabilities out of structural design and situating them within a broader mechanism of human capability and capacity. The interviews show that personnel-related problems are not simply about where individuals sit in the organisation, but about whether they possess the necessary skills, whether there are sufficient numbers of competent staff, and whether they can adapt to process and system changes. In practice, personnel issues behave less like a formal structural design problem and more like a human capability mechanism that interacts with behaviour, culture, and technological change.

The empirical findings also show that workforce capability is dynamic and context-sensitive, not static (e.g., Bieńkowska & Tworek, 2020). Employees' competencies shift with digitalisation, the introduction of new products, and evolving regulatory expectations. Older staff struggling with new systems, or those unable to detect counterfeit currency due to outdated training, illustrate how capability gaps emerge from the interaction between people and technological change. Second, capacity limitations, such as the migration of qualified staff, labour-market shortages, or increased workloads are structurally driven but behaviourally expressed. While the causes lie in external labour conditions or organisational staffing levels, the consequences materialise as reduced vigilance, higher error rates, and reduced monitoring

in daily work. Third, the findings demonstrate that personnel-related vulnerabilities belong conceptually with human capability and behaviour, not solely within formal organisational design. This supports and empirically justifies the aggregate dimension identified in the analysis: Human-Capability & Behavioural Control Problems**.** In doing so, it adds theoretical precision by framing people-related vulnerabilities as a mechanism that cuts across structural and behavioural aspects of control.

Taken together, the empirical evidence confirms the literature's assertion that personnel controls are essential for effective operational risk management, but it also refines and extends this understanding in three important ways. First, it reframes personnel-related weaknesses as dynamic constraints arising from changing capability and capacity conditions, rather than as a fixed structural deficiency. Second, it shows how workforce capability interacts with system complexity, organisational pressures, and changing process demands. Third, it demonstrates that personnel-related vulnerabilities operate behaviourally, justifying their inclusion in the aggregate dimension of *Human-Capability & Behavioural Control Problems*. This reconceptualization enriches the theoretical model by providing a more nuanced, practice-based understanding of how personnel factors contribute to operational risk in banking environments.

Beyond individual capability and staffing capacity, the empirical analysis shows that local norms, expectations, and shared meanings critically shape how controls are enacted. Accordingly, the following subsection turns to cultural and ethical drift as a further mechanism through which behavioural–institutional coupling contributes to operational risk.

4.4.4 Discussion on Cultural and Ethical Drift

The literature reviewed in Chapter 3 identifies cultural and behavioural factors as one of the deepest sources of management control problems affecting operational risk in banking. Organisational culture shapes how employees interpret and enact formal controls, with weak or misaligned cultures normalising deviance, eroding ethical standards, and undermining accountability (e.g., Cohn et al., 2014; Faugère & Stul, 2021; Kunz & Heitz, 2021; Lui, 2015; Mikes, 2009; Power, 2009). Prior studies show that leadership tone, banking identity and competitive norms, and fear- or compliance-driven environments jointly influence whether employees engage constructively with risk management or instead conceal errors, avoid reporting, and prioritise sales or performance pressures over prudential behaviour (Brauman et al., 2020; Carretta et al., 2024; Frese & Keith, 2015; Gurd & Helliar, 2017; Holland, 2019; Laguecir & Leca, 2022; Sabanova & Kudinska, 2023, 2024). Overall, cultural control problems emerge when organisational norms and social expectations counteract the intended effects of formal control systems, leading to misreporting, procedural drift, and increased exposure to operational risk.

The empirical findings broadly confirm the literature's proposition that cultural controls shape how employees interpret, enact, and sometimes circumvent formal management controls. Consistent with prior research summarised in Chapter 3, the case evidence shows that weak ethical norms, inconsistent risk awareness, and tolerance for procedural deviations increase the organisation's exposure to operational risk. However, the empirical results extend this understanding by demonstrating that cultural control problems materialise not simply as generalised "weak culture," but as *ethical drift* occurring differently across organisational sub-groups.

A key empirical insight is the presence of **s**ubcultures rather than a singular, uniform bank-wide culture. This aligns with prior organisational culture research, which shows that organizations may contain subcultures across departments, professional groups, or hierarchical levels (Hofstede, 1998). Additionally, such subcultures may reinforce, reinterpret, or even challenge the dominant organisational culture (Jermier et al., 1991). Evidence from the banking sector also supports this view. Although not focused on risk, the case study by Huang et al. (2002) shows how distinct subcultures shaped how different groups understood and responded to organisational initiatives. Consistent with this literature, the interview data illustrate that different departments operate under distinct normative expectations, behavioural routines, and informal assumptions about acceptable conduct. For example, the Internal Audit function reflects a culture of strict compliance and zero tolerance for deviations, emphasising procedural correctness and documentary evidence. In contrast, branch-level employees experience strong *client-facing pressure*, sometimes normalising small violations or relying on trust-based reasoning when interacting with customers. Staff in IT and e-banking describe a culture shaped by *procedural ambiguity*, where system constraints and technical exceptions create grey areas in which rules are interpreted flexibly. The Legal Department exhibits a more *formalistic orientation,* emphasising textual interpretation of procedures and regulatory mandates.

Importantly, these cultural control vulnerabilities were not uniform across the organisation. Only particular branches displayed notable cultural drift, indicating that problems emerged at the level of local subcultures**,** not at the level of a bank-wide culture. These subcultural patterns evolved through the daily routines, pressures, and priorities of each functional area. This observation represents a refinement of the existing literature: while Chapter 3 conceptualises culture as an organisational attribute shaped by leadership tone, professional identity, and behavioural norms, the empirical evidence here shows that cultural control problems often operate through department-specific or branch-level subcultures rather than through a uniform organisational culture.

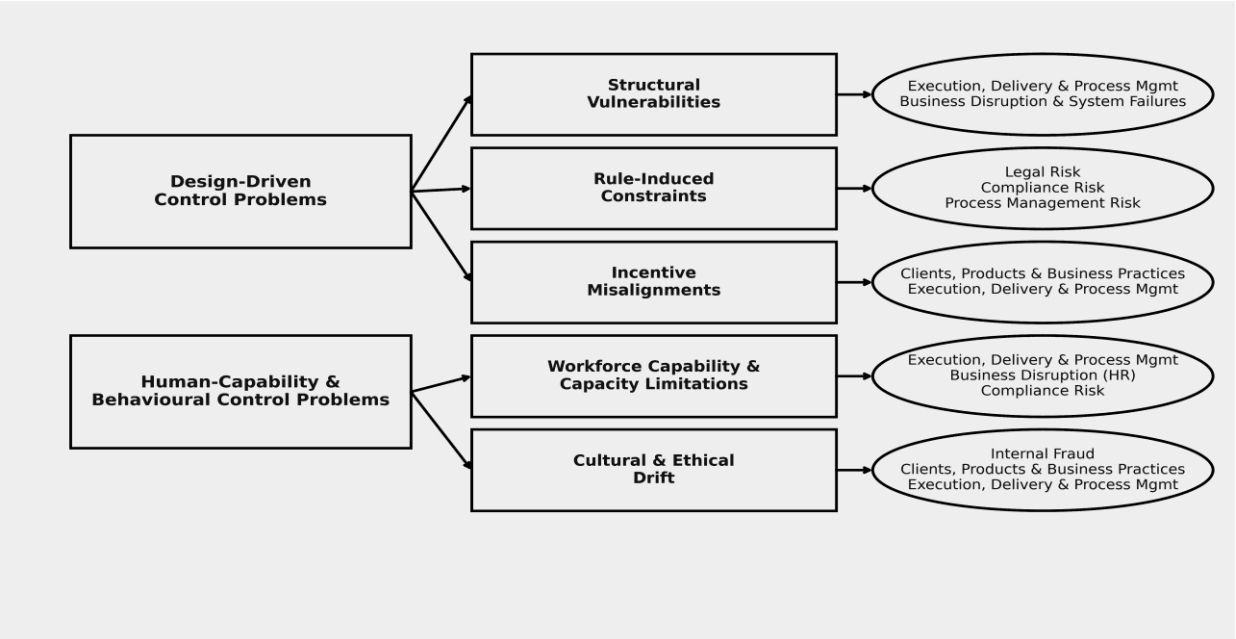
Moreover, while subcultures have been widely recognised in organisational research, the risk management literature has paid far less attention to how subcultural variation shapes operational risk behaviours. The findings of this study therefore underline the need for further research on how subcultures influence risk awareness, ethical judgement, and procedural adherence within banks.

Overall, the empirical analysis confirms the centrality of cultural mechanisms in shaping operational risk while refining theoretical understanding by showing that culture operates through differentiated subcultural patterns, ethical drift, and behavioural responses to local pressures. In doing so, the findings add conceptual depth and practical nuance to the theoretical model developed in the literature review. Therefore, the refinements across structural, incentive, capability, and cultural mechanisms provide the building blocks for an upgraded conceptual model. The next subsection integrates these insights by linking the five empirical mechanisms back to the dual theoretical mechanisms and to the Basel II/III operational risk categories.

4.4.5 Upgraded Conceptual Model: Integrating Theoretical Mechanisms and Empirical Pathways

The empirical findings refine and extend the dual-pathway model developed in Chapter 3 by showing how control-related vulnerabilities materialise through concrete organisational, behavioural, and socio-technical pathways within the case bank. While Chapter 3 conceptualised control failure through two broader integreative theoretical pathways: design–use misalignment and behavioural–institutional coupling, the qualitative evidence demonstrates that these pathways unfold through five more granular, empirically grounded pathways that link the design and operation of management control systems to the generation of operational risk.

Figure 9: Empirically Expanded Mechanisms Linking Control System Weaknesses to Operational Risk



Source: Own work.

The empirical data confirm the importance of design–use misalignment but reveal that this pathway consists of three distinct components in practice:

1. **Structural Vulnerabilities**: We identified weaknesses embedded in the Bank's operational infrastructure, including fragmented systems, incomplete automation, reliance on external IT vendors, and organisational growth that outpaces system or process capacity. These vulnerabilities show that misalignment arises not only from poor procedural design but from the inability of the underlying socio-technical infrastructure to reliably support control execution.
2. **Rule-Induced Constraints**: These occur when rules, procedures, or regulatory requirements become so rigid that they hinder operational adaptability, causing bottlenecks, delays, or reliance on informal workarounds. In contrast to the literature's depiction of procedural drift as a behavioural issue, the empirical study reveals that rigidity in rule design can itself constitute a structural source of misalignment.
3. **Incentive Misalignments**: The high threshold for bonuses, inconsistent SMART criteria, and heavy reliance on Management by Objectives, illustrate that incentives represent a design-driven source of control failure that also produces behavioural pressures. Incentive-related vulnerabilities emerge not only from behavioural responses to performance pressure, as emphasised in the literature, but from the design and inconsistent use of the Bank's result-control system.

Together, these three pathways form the aggregate dimension of Design-Driven Control Problems, offering a more granular interpretation of how design-related weaknesses create conditions for operational risk.

The empirical findings also corroborate the behavioural–institutional coupling pathway, while demonstrating that it is internally differentiated into two specific pathways:

4. **Workforce Capability and Capacity Limitations**: We identified skill gaps, training deficits, digital adaptation difficulties, migration-related staffing shortages, and workload-driven reductions in attentiveness. This mechanism shows that capability issues interact with institutional routines to produce recurring human-error exposures, thereby expanding theory by highlighting the dynamic and context-sensitive nature of personnel capabilities.
5. **Cultural and Ethical Drift**: Cultural weaknesses materialise not as a single organisational culture but through subcultures across departments, each shaping how rules are interpreted, risks are prioritised, and deviations are rationalised. This adds nuance to the literature by demonstrating that cultural control problems emerge through localised ethical drift rather than uniform cultural weakness.

These pathways combine into the aggregate dimension of Human-Capability & Behavioural Control Problems, illustrating that operational risk arises through the interplay between individual ability, behavioural norms, and departmental cultural pressures. Both aggregate

dimensions map directly onto the Basel II/III operational risk categories identified in RQ2. The data show clear linkages between the five mechanisms and the seven Basel II/III categories. This alignment demonstrates the pathways through which management control failures manifest as operational risk events.

The upgraded conceptual model advances the theoretical framework in three ways:

1. **It clarifies the internal structure of the two theoretical mechanisms**, showing that each consists of concrete empirical pathways that explain how misalignments and behavioural couplings occur in practice (Braumann, et al., 2024; Van der Kolk & Schokker, 2016).
2. **It repositions incentives as a hybrid mechanism**, operating simultaneously as a design-driven and behaviour-shaping force, thereby expanding the theoretical understanding of incentive-related control failures (Franco-Santos & Otley, 2018).
3. **It elevates personnel capability and departmental subcultures** as central mechanisms, extending prior theory by demonstrating that operational risk emerges from dynamic, localised capability and cultural conditions, not solely from organisational-level design choices (Di Antonio, 2017).

Overall, the revised conceptual model developed in Chapter 3 preserves the dual-pathway logic of the literature while incorporating five empirically grounded pathways that more accurately describe how management control systems contribute to operational risk within a real banking environment. It therefore provides a richer and more operationally relevant framework for understanding the behavioural, structural, and infrastructural origins of control failures.

To synthesise how the empirical findings relate back to the theoretical pathways developed in Chapter 3, Table 21 presents a structured comparison between the literature-based propositions and the evidence generated through the qualitative case study. The table distinguishes (1) what the empirical data confirm from the dual-pathway model: design–use misalignment and behavioural–institutional coupling; and (2) what elements of the empirical findings extend, refine, or nuance these theoretical expectations.

Table 21: Comparison of Theoretical Mechanisms and Empirical Evidence

Theoretical Mechanism (Literature Review Ch.2)	What the Empirical Data Confirm	What the Empirical Data Extend or Refine
Design–Use Misalignment	The empirical findings confirm that misalignment occurs when design diverges from operational use. Three patterns align with the mechanism: • Structural vulnerabilities (fragmented systems, incomplete automation). • Rule-induced constraints (rigid procedures causing delays and workarounds). • Incentive-related pressures influencing behaviour.	• Structural vulnerabilities are shown to be socio-technical (system integration, vendor limits), refining the literature's abstract structural framing. • Incentives operate as hybrid design–behaviour mechanisms, extending theoretical expectations. • Rule-induced constraints confirm theory but do not introduce new extensions or contradictions.
Behavioural–Institutional Coupling	Findings confirm that behavioural norms, capability, and cultural routines shape how controls operate: • Capability-based variation (skill gaps, attention loss). • Cultural drift and inconsistent risk awareness. • Localised behavioural norms affecting control execution.	• Workforce capability emerges as a dynamic mechanism influenced by digitalisation, workload, and labour-market pressures-extending the literature. • Culture is shown to operate through multiple micro-cultures rather than a single organisational culture-refining theory.

Source: Own work.

4.4.6 Practical implications

The empirical findings of this study provide several practical implications for strengthening the Bank's management control system and reducing operational risk exposure. By uncovering five empirically grounded pathways: Structural Vulnerabilities, Rule-Induced Constraints, Incentive Misalignments, Workforce Capability and Capacity Limitations, and Cultural and Ethical Drift, the study highlights where targeted interventions can meaningfully improve the reliability, adaptability, and behavioural integrity of control systems.

First, the findings emphasise the need for socio-technical strengthening of the control environment**.** Structural Vulnerabilities point to fragmented systems, incomplete automation, vendor dependencies, and organisational growth that outpaced system capacity. For practice, this implies that operational risk exposures depend not only on redesigning procedures but on upgrading system architecture, reducing manual workarounds, and improving cross-system integration. Investments in early-warning mechanisms, automated reconciliations, and real-time monitoring can mitigate the types of Execution, Delivery and Process Management risks observed in the case bank.

Second, the results highlight the importance of reviewing and refining the Bank's rule-based control architecture**.** Rule-Induced Constraints demonstrate that excessive procedural rigidity can unintentionally create operational bottlenecks, delay decision-making, and push employees toward informal workarounds. While regulatory compliance is non-negotiable, the findings show the value of designing rules that preserve interpretive flexibility where legally permissible. Clarifying ambiguous guidelines, reducing unnecessary procedural steps, and coordinating with supervisory authorities can help balance compliance obligations with operational efficiency.

Third, the analysis reveals that incentive systems must be redesigned to align more clearly with operational risk objectives. Incentive Misalignments show that performance evaluation structures, particularly the high bonus thresholds, inconsistent SMART criteria, and overreliance on Management by Objectives can drive behaviour that prioritises target achievement over procedural integrity. This suggests the need for redesigning result controls that integrate risk-management quality indicators, reduce excessive performance thresholds, and ensure consistency in objective-setting across units. The Bank may also consider integrating behavioural metrics or risk-culture indicators into appraisal systems.

Fourth, the findings highlight the significance of human capability for the reliable functioning of controls**.** Workforce Capability and Capacity Limitations demonstrate that skill shortages, digital adaptation difficulties, and workload-driven attentional fatigue are critical sources of operational risk. Practical implications include targeted training programmes, structured onboarding for new or rotating staff, periodic competence assessments, and measures to address staff shortages in key operational areas. Strengthening

human capability also supports the Bank's digitalisation agenda, ensuring that employees can effectively operate and monitor evolving technological processes.

Fifth, the findings show that risk culture must be addressed at the level of departmental micro-contexts rather than through generic bank-wide initiatives**.** Cultural and Ethical Drift reveals that different units operate within distinct micro-cultures shaped by local pressures, norms, and interpretive practices. This implies that interventions aimed at improving ethical discipline and procedural compliance need to be tailored to specific organisational sub-groups (e.g., branches, IT, Audit, Legal). Strengthening psychological safety, encouraging open reporting, and reinforcing accountability frameworks can help reduce concealment, trust-based deviations, and tolerance for small breaches that escalate into operational losses.

Overall, the practical implications of this study demonstrate that operational risk in banking is shaped by the interaction of system design, rule architecture, incentive structures, human capability, and cultural dynamics. The findings suggest that improving operational resilience requires a holistic approach to management control. Particularly, one that integrates socio-technical upgrades, regulatory and procedural flexibility, incentive redesign, targeted capability-building, and department-specific cultural interventions. Together, these measures can enhance the Bank's control reliability, reduce Basel II/III operational risk exposures, and support a more consistent alignment between formal control design and everyday operational practice.

4.4.7 Limitations

This study has several limitations that should be acknowledged. First, the analysis was guided primarily by a single theoretical lens, the Merchant and Van der Stede (2017) Objects of Control framework. While this framework provided analytical clarity and alignment with prior MCS research, relying on one dominant lens may have constrained the interpretation of certain organisational dynamics or the identification of alternative explanatory mechanisms.

Second, the empirical work is based on a single-case study conducted within one commercial bank operating in the Kosovo context. Although the bank is a major market player and the case provides rich insight into real-world control practices, the findings are context-dependent and should not be assumed to apply uniformly across the broader banking sector. This is particularly relevant in relation to investment banking, where business models, incentive structures, organisational tempo, and forms of risk-taking differ materially from those observed in commercial banking. As a result, some of the control problems identified in this study may take different forms in investment banking environments, especially where trading activity, deal execution, and market-based incentives play a more central role. At the same time, several findings are likely to be relevant beyond the studied bank, including those related to weak control alignment, monitoring quality, escalation, cross-functional coordination, and the behavioural consequences of poorly designed or inconsistently used

controls. By contrast, findings linked more directly to lending routines, customer-facing operations, payment processes, and service continuity are more closely tied to the commercial banking setting and should therefore be transferred to other banking contexts with appropriate contextual adaptation.

Third, the study relies primarily on interview data, and despite strong participation, some interviewees were understandably cautious in discussing sensitive topics such as people risk, internal errors, system weaknesses, or cultural tensions, which may reflect social desirability bias and limit the depth of insights. This limited openness may have constrained the depth of certain insights, particularly those related to behavioural or ethical issues. Efforts were made to mitigate this through triangulation with internal documentation, but unreported practices or informal norms may remain outside the scope of the analysis.

Fourth, documentary data such as the Loss Event Report, were partially anonymised due to confidentiality requirements. This limited access to detailed financial information and constrained opportunities for deeper quantitative integration with the qualitative insights.

Finally, the findings reflect organisational conditions at a single point in time**.** As digitalisation advances, regulatory expectations evolve, and internal structures change, the nature of control mechanisms and operational risk exposures may shift accordingly.

Despite these limitations, the study provides a valuable, empirically grounded contribution by revealing how management control systems generate or mitigate operational risk within a real banking environment, offering theoretical and practical insights that may also inform understanding in comparable commercial banking settings beyond the specific case.

4.4.8 Implications for Future Research

The findings of this study open several avenues for further investigation into the relationship between management control systems and operational risk in banking.

First, the study demonstrates that the Merchant and Van der Stede (2017) framework, while analytically powerful, only partially captures the socio-technical and micro-cultural mechanisms through which operational risk materialises. Future research could therefore extend or complement the Objects of Control framework by integrating perspectives from organisational sociology, behavioural ethics, or socio-technical systems theory. This would enable a more comprehensive theoretical account of how technological infrastructures, micro-cultures, and capability dynamics jointly shape control reliability.

Second, this study shows that “structural vulnerabilities,” “incentive misalignments,” and “cultural and ethical drift” are more granular and operational than the mechanisms conceptualised in existing literature. Future research could examine how are these empirically derived mechanisms manifested in other banking contexts, both in different

national settings and in banks with differing levels of digital maturity or organisational complexity. Comparative case studies or multi-site qualitative research would help determine which mechanisms are context-specific and which represent generalisable patterns in the banking sector.

Third, the findings suggest that workforce capability and capacity limitations are dynamic phenomena, shaped by digitalisation, labour market conditions, and process complexity. This highlights the need for future studies to investigate how capability evolves over time, particularly as banks undergo automation, centralisation, or technological transformation. Longitudinal qualitative studies or mixed-methods research could help clarify how human capability interacts with changing control architectures and whether certain interventions (e.g., training, job redesign, digital tools) mitigate capability-driven operational risk.

Third, the findings suggest that workforce capability and capacity limitations are dynamic phenomena, shaped by digitalisation, labour market conditions, and process complexity. This highlights the need for future studies to investigate how capability evolves over time, particularly as banks undergo automation, centralisation, or technological transformation. The growing integration of AI-enabled systems adds an additional layer of complexity. While AI tools may alleviate workload pressures, support accuracy, and reduce routine errors, they may also introduce new skill requirements, worsen capability gaps, or generate over-reliance on automated systems. Longitudinal qualitative studies or mixed-methods research could help clarify how human capability interacts with changing control architectures, specifically with AI-driven systems. It is important to understand whether interventions such as targeted training, job redesign, digital tools, or AI governance mechanisms can mitigate capability-driven operational risk.

Finally, this study shows that different departments operate with different micro-cultures, which shape how rules are interpreted and applied. Future research should therefore examine how these subcultures develop, how they influence employees' everyday decisions, and how cultural differences across units affect operational risk. Ethnographic methods, or real-time observational studies may reveal behavioural dynamics that interviews alone cannot fully capture.

4.5 Conclusion

The purpose of this chapter was to provide an in-depth qualitative examination of how management control systems function in practice within the case bank and how control-related vulnerabilities translate into operational risk. Drawing on insights from managers across key organisational units, the analysis identified the pathways through which the bank's management control system operates in practice and examined how these mechanisms map onto Basel II/III operational risk categories.

The findings show that weaknesses in the bank's management control system emerge through five recurrent pathways: structural vulnerabilities**,** rule-induced constraints**,** workforce capability and capacity limitations**,** incentive misalignments, and cultural and ethical drift**.** Together, these pathways describe how result, action, personnel, and cultural controls are translated into everyday practice and where, in that translation, vulnerabilities arise. Structural vulnerabilities capture weaknesses in the socio-technical infrastructure, including incomplete automation, system misconfigurations, fragmented processes, and reliance on manual workarounds. Rule-induced constraints reflect the way legal and regulatory requirements, together with highly prescriptive internal procedures, limit operational flexibility and create bottlenecks or compliance tensions. Workforce capability and capacity limitations arise from skill gaps, staffing shortages, resistance to digital transformation, and the persistence of human error in areas where automated controls are limited. Incentive misalignments originate in the design and use of result controls, particularly high bonus thresholds and target-driven pressures that shape how employees prioritise objectives and may encourage boundary-seeking behaviour. Cultural and ethical drift occurs when ethical discipline, shared norms, and risk awareness do not consistently guide behaviour, enabling misconduct, concealment, procedural bypassing, or trust-based deviations.

Therefore, these five pathways form the empirical pathways through which two broader dimensions of control problems manifest in the case bank**:** design-driven control problems (structural vulnerabilities, rule-induced constraints, incentive misalignments) and human-capability and behavioural control problems (workforce capability and capacity limitations, cultural and ethical drift). In this sense, the chapter addresses RQ1 by showing that operational vulnerabilities are not isolated or random incidents, but patterned mechanisms rooted in how controls are designed, interpreted, and enacted by employees.

The analysis further demonstrates that these pathways translate into specific and predictable operational risk exposures under the Basel II/III framework, thereby addressing RQ2. Structural vulnerabilities primarily generate execution, delivery and process management risk and system-related failures, especially where manual processes, vendor dependencies, or system instabilities undermine process reliability. Rule-induced constraints are associated with clients, products and business practices risk and compliance-related exposures, as rigid legal or procedural requirements create situations in which processes must be adapted or workarounds developed. Workforce capability and capacity limitations contribute mainly to execution, delivery and process management risk and employment practices and workplace safety, as capability gaps, migration of qualified staff, and resistance to digital processes which elevate error and reduce monitoring effectiveness. Incentive misalignments are linked to execution, delivery and process management risk and clients, products and business practices risk, where pressure to achieve targets shapes how employees handle procedures, clients, and documentation. Cultural and ethical drift generates internal fraud, clients, products and business practices risk, and execution, delivery and process management risk

when ethical vigilance, transparency, and procedural discipline break down, enabling misconduct, concealment, or trust-based violations of rules.

Overall, the chapter shows that operational risk in the case bank does not arise from isolated failures, but from identifiable design-driven and human-capability pathways embedded in the management control system. By addressing RQ1, the analysis explains where and how these pathways originate within the control architecture; by addressing RQ2, it demonstrates how these pathways materialise as operational risk exposures. The bank's operational risk profile is therefore shaped by the coherence and alignment of its control systems, the capabilities and capacity of staff to execute those controls reliably, the robustness of the underlying systems and processes, and the strength of its ethical culture in guiding day-to-day operations.

5 BEHAVIOURAL PATHWAYS LINKING MANAGEMENT CONTROL PROBLEMS TO OPERATIONAL RISK IN BANKING: THE EFFECT OF TIGHT CONTROLS ON RISKY BEHAVIOURS

5.1 Introduction

Operational risk in banks arises to a great extent from employee behaviour (Xu et al., 2017). Even small attentional errors or seemingly benign rule deviations can escalate into significant losses when they occur in tightly coupled financial systems (Faugère & Stul, 2021; Kuhn & Neu, 2003; Liang et al., 2024; Muermann & Oktem, 2002). In response, banks rely heavily on tight management control systems (de Waal & Coevert, 2007; Fakhri et al., 2010; Hussain, 2005; Middaugh, 1988; Rikhardsson et al., 2021; Van der Stede, 2001; Zéman et al., 2013), particularly tight results controls[2] such as performance targets that specify expected outcomes with limited tolerance for deviation, as well as rigid action controls, including rules, procedures, checklists, and standard operating processes designed to regulate how work must be conducted. These controls are implemented with the intention of reducing human-related operational risks by increasing behavioural predictability and compliance.

However, decades of behavioural and organisational research suggest that tight controls may function as double-edged swords (Goebel & Weißenberger, 2016; Van der Stede, 2000). While they are designed to prevent mistakes and ensure reliable performance, they can also create new behavioural vulnerabilities (Carroll & Marginson, 2021; Franco-Santos et al.,

[2] In Merchant and Van der Stede's (2012) framework, "tight results controls" specify desired performance outcomes with precise targets, frequent monitoring, and limited tolerance for deviation. "Tight action controls" consist of detailed rules, procedures, checklists, and standard operating processes that prescribe in advance how tasks must be completed and ensure close compliance.

2012; Hopwood, 1972; Ridgway, 1956). Tight results controls may heighten time pressure and cognitive load (Becker & Green, 1962; Linder et al., 2020; Staal, 2004), increasing the likelihood of slips and lapses, i.e. unintentional errors that occur when attentional resources are strained (Reason, 1990). Tight action controls, while aimed at eliminating rule-breaking, may reduce intrinsic motivation and encourage routine rule violations, as employees habitually circumvent procedures they perceive as inefficient (Reason et al., 1998). These same tight controls may also influence exceptional violations, which occur under situational pressure when rigid rules clash with the immediate demands of the task (Hale & Boris, 2013). In this sense, controls adopted to prevent operational failures may paradoxically trigger new forms of risky behaviour.

Understanding how tight controls shape these different behavioural outcomes requires attention to the broader organisational context. Risk culture, encapsulating the shared norms, expectations, and values surrounding risk awareness and responsible conduct (Power et al., 2021), plays a central role in how employees interpret and respond to tight controls. A strong risk culture may strengthen the intended effects of controls by reinforcing disciplined behaviour and signalling the importance of compliance. Conversely, when risk culture is weak, tight controls may be viewed as punitive or mechanical, reducing their behavioural impact or motivating resistance. Another important element in banking context concerns how risk management system (RMS) is used (Mikes, 2009). When used interactively, risk management can stimulate dialogue, learning, and shared sensemaking (Bisbe & Otley 2004; Marc et al., 2023). Interactive use can reinforce cultural expectations, making risk culture more likely to shape behaviour as intended. Yet tight management controls also affect employees' internal regulation mechanisms (Verburg, 2017). They may enhance self-control by clarifying expectations and heightening attentiveness (Johnson et al., 2018; Tyler & Blader 2005) or undermine it by shifting responsibility from the individual to the formal rule system (Adler & Borys, 1996; Christ et al., 2012).

Despite the centrality of tight controls in banking and the widespread assumption that they reduce human-related risk, little is known about their unintended behavioural consequences, particularly across different types of operational risk behaviours. Recent reviews of operational risk highlight that existing research remains heavily concentrated on modelling loss distributions and regulatory capital requirements (Chavez-Demoulin et al., 2015; Moosa, 2007; Power, 2005), while the behavioural and people-related origins of operational risk are still insufficiently understood (Xu et al., 2017). Xu et al., (2017) note that although operational risk events in financial services often arise from human actions embedded within organisational processes, the literature has paid comparatively little attention to the behavioural drivers of risk, calling for new research that explicitly incorporates human-factor perspectives. Pakhchanyan (2016) identifies a similar gap, noting that among 279 reviewed studies, very few address internal, staff-related sources of operational risk, despite clear evidence that factors such as competence, workload, and procedural adherence play a central role in generating loss events. More recently, Mabwe et al. (2022) provide qualitative evidence from UK banks demonstrating that "people risk" remains unevenly conceptualised

and insufficiently integrated into operational risk management practice, with practitioners acknowledging that employee behaviour plays a critical yet under-addressed role in risk generation. Taken together, these studies highlight a persistent need for research that moves beyond capital modelling and examines operational risk through a behavioural, people-centred lens. This provides a strong foundation for the present study, which investigates how management control problems shape people-risk behaviours that contribute to operational risk in banking.

The quantitative model developed in this chapter is intentionally narrower than the broader framework examined in the preceding chapters. Two modelling choices require explicit justification: the focus on Results Controls and Action Controls to the exclusion of Personnel and Cultural Controls, and the concentration on tight configurations of these controls. The focus on Results Controls and Action Controls reflects the findings from Chapters 2 and 3, that these two control types are most directly associated with the emergence of control problems and behavioural distortions in day-to-day operations. Results Controls guide behaviour through performance targets and expected outcomes, while Action Controls prescribe behaviour through rules, procedures, and standardised processes. This focus reflects an analytical simplification rather than a rejection of Personnel Controls. Personnel Controls and Cultural Controls, although conceptually important, operate through mechanisms that are more distal from ongoing task execution. Personnel Controls shape behaviour primarily through employee selection, training, and internalisation of values, while Cultural Controls operate through shared norms, informal expectations, and organisational socialisation processes. Both influence behaviour over longer time horizons and through channels that are less amenable to the variance-based modelling approach adopted here. This is not to suggest that either is irrelevant to operational risk outcomes, but rather that their effects are more indirect and operate through mechanisms that are analytically distinct from those examined in this chapter.

The focus on "tight" controls configurations is similarly motivated. Tight controls are more likely to intensify performance pressure, increase behavioural rigidity, and trigger the kinds of unintended responses that are central to the research question. Concentrating on this end of the control spectrum also creates a more demanding analytical test: if control problems and operational risk exposures are detectable under tight controls (where compliance and standardisation are strongest) this provides a more conservative and theoretically meaningful assessment of the relationship between control design and operational risk outcomes.

Our guiding research question in this chapter is therefore: "*How do management control problems affect the frequency of people-risk behaviours that contribute to operational risk?"* We address this question by examining how tight results controls and tight action controls influence three distinct categories of risky behaviour which lead to operational risk events: slips and lapses (unintentional mistakes), routine violations (habitual intentional shortcuts), and exceptional violations (situational intentional deviations). We develop and test a model in which tight controls are associated with these behaviours directly, but also indirectly

through employees' self-control. We also examine the paths through which risk culture is associated with these behaviours and test if interactive use of risk management affects them. Using established measurement instrument for the constructs in the model, we collected survey data from 150 employees of one bank and tested the model with the PLS-SEM approach.

By studying tight controls as potential double-edged swords, we contribute to a more nuanced understanding of operational risk in banks originating from human behaviour (i.e., people risk). Our findings explain why controls designed to enhance reliability can, in some cases generate new forms of operational vulnerabilities. They also identify the organisational conditions under which tight controls mitigate or unintentionally amplify employee-induced operational risk.

The remainder of this chapter is organised as follows. The next section develops the theoretical framework underpinning the study and derives the hypotheses that link tight results controls, tight action controls, self-control, risk culture, and interactive use of risk management to three categories of people-risk behaviours. This is followed by a section describing the research design, sampling strategy, measurement instruments, and analytical approach, including the use of PLS-SEM. The subsequent section presents the empirical results, beginning with an evaluation of the measurement model and followed by the structural model and hypothesis testing. The following section discusses the implications of the findings in light of prior research on management control systems and operational risk. The chapter concludes with a final section outlining the theoretical and practical contributions, limitations, and directions for future research.

5.2 Theoretical Framework and Hypotheses Development

In this section we develop our conceptual model and develop the hypotheses about relationships between the constructs. The model is summarized in Figure 10. Our main constructs of interest are the two types of management control systems – results controls (RC) and action control (AC), as well as the role of risk culture.

5.2.1 Management Controls

Banks rely heavily on tight management control systems to mitigate operational risk and ensure compliant, predictable employee behaviour (Rad, 2016). Two forms of tight control are central in this context: tight results controls (RC) and tight action controls (AC) (Merchant & Van der Stede, 2017). Tight results controls specify clear, demanding performance expectations and hold employees accountable for deviations from expected outcomes. Tight action controls prescribe in detail how tasks must be carried out, typically through standard operating procedures, rules, checklists, and process documentation. Both

forms of control are widely used in highly regulated sectors such as banking, where the reliability and accuracy of task execution are crucial.

Management control theory traditionally assumes that tighter controls lead to improved reliability, reduced errors, and fewer rule violations (Anthony & Govindarajan 2007; Malmi & Brown, 2008; Simons, 1995). Yet, empirical research also highlights the potential side-effects of tight controls, such as employee stress, rigidity, and behavioural displacement (Adler & Borys, 1996; Van der Kolk, 2019). These effects raise the possibility that controls designed to prevent operational failures may paradoxically contribute to them, positioning tight controls as double-edged swords.

To clarify the behavioural outcomes examined in this study, it is useful to draw on the human error and safety literature. A foundational distinction in this literature is between slips and lapses, which are unintentional execution and memory failures, mistakes, which arise from faulty judgments or plans, and violations, which involve deliberate departures from prescribed rules or procedures (Reason, 1990, 2000). This literature further suggests that such behaviours do not arise randomly but are shaped by the conditions under which people work, including time pressure, attentional overload, fatigue, inadequate resources, and unworkable procedures (Reason, 2000). With regard to rule violations, review evidence shows that formal procedures are often necessary in complex systems, yet violations may become routine where rules are experienced as impractical, excessive, contradictory, or misaligned with operational realities (Hale & Borys, 2013).

Building on this behavioural perspective, the present study focuses on three categories of risky behaviour that are especially relevant to tight controls: slips and lapses, routine rule violations, and exceptional rule violations. Tight results controls can increase performance pressure and attentional demands, which may elevate the risk of slips and lapses by straining employees' cognitive resources (Reason, 1990, 2000). Tight action controls, by contrast, are intended to reduce non-compliance by prescribing how tasks should be performed, but they may also restrict discretion to the point where procedures are experienced as overly rigid or impractical (Hale & Borys, 2013). Under such conditions, employees may adopt routine violations, that is, habitual workarounds that deviate from formal rules but facilitate task completion (Hale & Borys, 2013). A different class of intentional deviations, known as exceptional violations, may arise in unusual or high-pressure situations where strict adherence to rules becomes incompatible with task demands (Reason, 1990). This literature suggests that tight controls may both suppress and provoke risky behaviours, depending on employees' psychological responses and the broader organisational environment. We therefore examine how tight controls are associated with three behavioural outcomes: slips and lapses (unintentional errors), routine rule violations (habitual shortcuts), and exceptional rule violations (situational deviations under pressure).

Tight results controls specify clear and demanding performance expectations. In principle, such clarity should reduce errors, because employees know what is required of them.

However, tight targets also increase time pressure, cognitive load, and attentional demands. Under these conditions, unintentional mistakes such as slips and lapses, may become more likely. Results controls therefore carry a paradoxical quality: they are implemented to improve reliability but may inadvertently increase the likelihood of minor errors by straining individual attentional resources. Nonetheless, because RC are intended to enhance performance accuracy, we hypothesise an intended negative relationship:

H1a: Tight results controls are negatively associated with slips and lapses.

Action controls prescribe detailed procedures for task execution. By reducing discretion, AC aim to limit rule violations and create consistent, predictable behaviour (Merchant & Van der Stede, 2017). However, very tight procedures may be experienced as restrictive, reduce intrinsic motivation, and encourage employees to circumvent rules that are perceived as inefficient or impractical (Adler & Borys, 1996; Christ et al., 2012). This duality is central to operational risk: procedures are implemented to prevent non-compliance, yet rigid procedures can motivate workarounds which may result in more operational risk. Nevertheless, because their intended purpose is to prevent rule-breaking, we hypothesise negative direct effects:

H1b: Tight action controls are negatively associated with routine rule violations.

H1c: Tight action controls are negatively associated with exceptional rule violations.

Self-control reflects the individual's ability to regulate impulses, sustain attention, and adhere to behavioural standards (Kirsch and Cummings, 1996; Tangney et al., 2018). It plays a central role in reliable performance. In operational settings, high self-control reduces slips and lapses, because individuals maintain attention and avoid inadvertent mistakes (Tangney et al., 2018). It also reduces rule violations, both routine and exceptional, because disciplined employees are more likely to resist shortcuts and comply with rules even when efficiency pressures or situational demands encourage deviation. Self-control is shaped by both cultural and structural factors (Hofmann, 2024). Cultural expectations of responsibility promote internalised self-regulation, while tight controls may either strengthen or weaken self-control depending on whether they promote attentiveness (results controls) or diminish intrinsic responsibility (action controls). Thus, self-control serves as a central psychological mechanism linking control systems and organisational culture to employee behaviour (Duckworth et al., 2018; Johnson et al., 2018).

Tight results controls may enhance self-control by increasing accountability, clarifying expectations, and creating focus. Employees subject to demanding performance standards may become more vigilant and attentive, strengthening their internal regulation.

H2a: Tight results controls increase self-control

In contrast, tight action controls may reduce self-control. When rules and procedures become excessively prescriptive, employees may develop a compliance mentality that shifts responsibility from the individual ("I must remain attentive") to the system ("the rules tell me what to do"). This can undermine internal motivation and weaken the development of controlled behaviour.

H2b: Tight action controls decrease self-control.

5.2.2 Risk Culture

Risk culture refers to shared norms and expectations concerning responsible conduct, risk awareness, and behavioural accountability (Power et al., 2021). In banking, risk culture is considered a foundational element of effective risk management, shaping how employees interpret controls and make decisions under uncertainty (Carretta et al., 2017; Kunz & Heitz, 2021). A strong risk culture emphasises accountability, attention to detail, and adherence to organisational standards. As such it encourages employees to recognise risks, follow rules, and behave attentively, thereby reducing the frequency of slips and lapses. We hypothesize the following:

H3a,b,c: Risk culture is negatively associated with slips and lapses (a), routine violations (b), and exceptional violations (c).

Additionally, risk culture fosters self-control, which refers to employee's ability to regulate their behaviour, maintain focus, and resist counterproductive actions (Johnson et al., 2018), because employees internalise the importance of behaving cautiously and responsibly. When risk awareness is embedded in the organisational environment, employees are more likely to regulate their own conduct leading employees to maintain attention, resist shortcuts, and behave responsibly without external enforcement. High self-control reduces unintentional errors by supporting careful and attentive task execution (De Ridder et al., 2012). It also reduces intentional deviations because self-regulated employees are more likely to adhere to rules, even when shortcuts appear tempting or situational pressures arise (Baumeister et al., 2007; Wang et al., 2021). We therefore expect self-control to reduce all three forms of behavioural risk.

This internalisation effect positions risk culture as a central construct relating to all forms of risky behaviour also indirectly through self-control:

H4: Risk culture is positively associated with employees' self-control.

H5a,b,c: Self-control is negatively associated with slips and lapses (a), routine rule violations (b), and exceptional rule violations (c).

Risk culture not only influences behaviour directly but also shapes employees' reactions to formal controls (Kunz & Heitz, 2021). The behavioural effects of tight controls depend

critically on the risk culture in which they are embedded. Risk culture comprises shared norms and values that emphasise responsible conduct, attentiveness, and rule adherence (IRM, 2012). When risk culture is strong, employees are more likely to interpret tight controls as valid, meaningful, and aligned with organisational purpose. Under such conditions, tight controls reinforce rather than undermine disciplined behaviour. Conversely, when risk culture is weak, tight controls may be perceived as coercive or overly bureaucratic, reducing their effectiveness or even provoking resistance in the form of rule violations (Liu et al., 2015). Therefore, we propose the following hypotheses:

H6: Risk culture strengthens the effect of tight controls on self-control.

As such, risk culture serves both as a direct and indirect behavioural influence, as well as a contextual moderator that conditions the effects of formal controls.

5.2.3 Interactive Use of Risk Management

Within Simons' (1995) levers of control framework, interactive use refers to the use of performance measures in frequent, face-to-face discussions aimed at learning, communication, and the identification of emerging issues. Prior research shows that interactive use of risk management importantly enhances employee understanding of priorities and reinforces risk management (Marc et al., 2023; Mikes, 2009). Interactive use keeps key risks at the centre of organisational attention and supports shared sensemaking (Frigo & Anderson, 2014; Gurd & Helliar, 2017; Hall et al., 2015). In the context of operational risk, interactive use may amplify the influence of risk culture, because dialogue and shared interpretation strengthen collective awareness of appropriate behaviour and the importance of risk management. Although interactive use is not typically associated with reducing errors directly, it shapes how cultural signals are transmitted and understood, therefore interactive use is likely to amplify the effects of risk culture on behavioural outcomes – the frequency of risky behaviour (slips and lapses, routine violations, exceptional violations) and the self-control. We therefore hypothesize:

H7: Interactive use amplifies the positive effects of risk culture on self-control.

H8 a,b,c: Interactive use amplifies the positive effects of risk culture on slips and lapses (a), routine violations (b) , and exceptional violations(c).

5.2.4 The conceptual model

Banks operate in environments where seemingly minor human errors or procedural deviations can scale into material operational losses (Sobanova & Kudinska, 2023). To address these risks, institutions rely on tight RC and tight AC, which are designed to structure employee behaviour by limiting discretion and increasing predictability. Yet, as the preceding literature suggests, (e.g., Carroll & Marginson, 2021; Christ et al., 2012; Franco-

Santos et al., 2012; Goebel & Weißenberger, 2016), these controls may function as double-edged swords: while intended to prevent mistakes and ensure reliable performance, they may simultaneously create new behavioural vulnerabilities. Our conceptual model, illustrated in figure 10, integrates these tensions with the broader organisational context defined by risk culture, interactive use of risk management system, and employees' self-control to explain three distinct forms of risky behaviour: slips and lapses, routine rule violations, and exceptional rule violations.

We will separately test the model (Figure 10) for three categories of risky behaviour that differ in their causes and organisational antecedents:

1. Slips and lapses — cognitive and attentional failures.
2. Routine violations — intentional, habitual deviations from rules to improve efficiency.
3. Exceptional violations — intentional deviations that occur under situational pressure.

Tight results controls primarily affect attentional processes and are therefore expected to shape slips and lapses. Tight action controls aim to prevent rule-breaking but may unintentionally contribute to both routine and exceptional violations. Risk culture and self-control are expected to play roles in all three models, though through different pathways, reflecting the distinct origins of each behaviour.

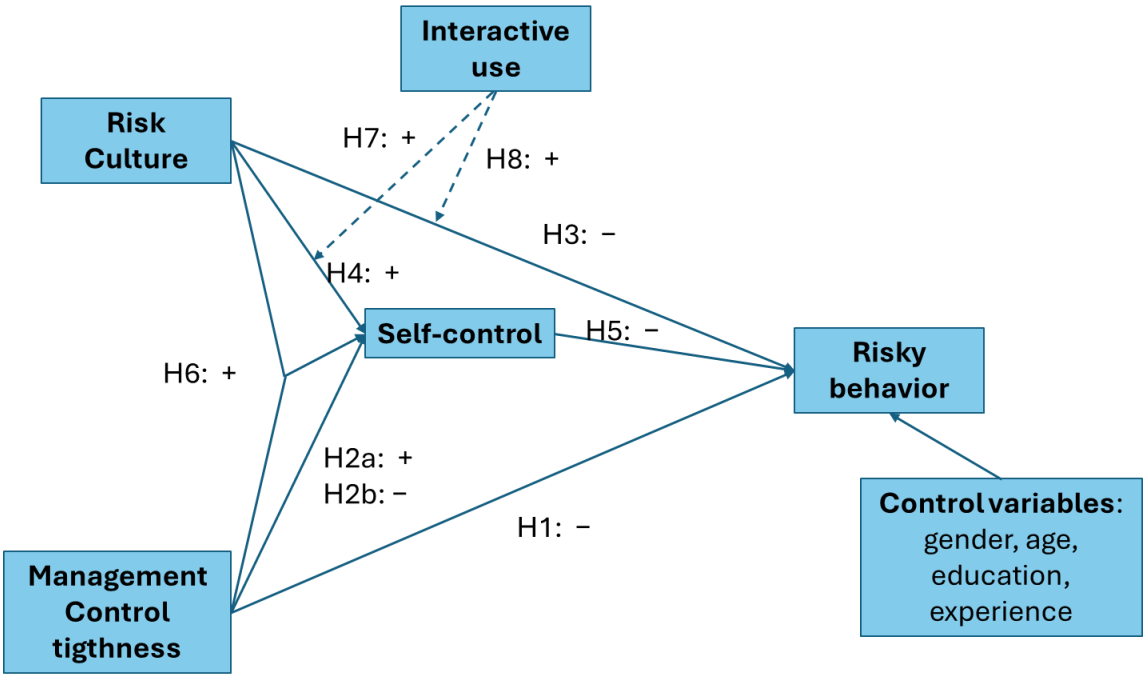
Across all three behavioural outcomes, self-control serves as a central psychological mechanism through which controls and culture influence behaviour (Figure 10). Self-control reflects an individual's capacity to sustain attention, regulate impulses, and adhere to behavioural standards. High self-control lowers the likelihood of slips and lapses, because such errors typically arise from lapses in attention. It also reduces routine and exceptional violations, because self-controlled employees are more capable of resisting habitual shortcuts and situational temptations to deviate from rules.

Tight controls influence self-control in different ways. Tight results controls may enhance discipline by clarifying expectations and increasing vigilance. Tight action controls, however, may diminish discipline by shifting responsibility from the individual ("I must behave carefully") to the system ("the rules tell me what to do"), thereby weakening intrinsic motivation. Risk culture supports self-control by encouraging employees to internalise norms of responsible conduct. Interactive use further strengthens these cultural signals. Thus, self-control forms the linking mechanism that explains how the combination of controls, cultural context, and control style affects different types of risk-related behaviour.

In our model, interactive use is conceptualised as reinforcing the influence of risk culture on employees' internal regulation (Figure 10). When performance measures are used interactively, cultural expectations are more visible and meaningful, thereby strengthening the relationship between risk culture and self-control

Taken together, our model and hypotheses argue that tight controls are designed to prevent operational risks but may also introduce new behavioural vulnerabilities. Their effects depend on risk culture, interactive control style, and the extent to which they enhance or undermine employees' self-control. Different behavioural outcomes emerge through different pathways, highlighting the complex interplay between formal controls, cultural context, and individual psychological regulation.

Figure 10: Conceptual Model and Hypothesised Relationships



Source: Own Work

5.3 Methods

The following sections provide a detailed description of the research design, sampling approach, measures, analytical procedures, and ethical considerations underlying this quantitative study.

5.3.1 Research Design

Given the presence of indirect and interaction effects, the presence of multiple endogenous variables, we employ partial least squares structural equation modelling (PLS-SEM). PLS-SEM is appropriate for studies with complex models, latent constructs measured by multiple indicators, and a mixture of formative and reflective variables (Hair et al., 2022). It is particularly suitable when the research objective is theory development in organisational settings and when the goal is to maximise explained variance in the endogenous constructs

(Hair et al., 2011). The alternative, CB-SEM, is not suitable because the study does not aim to confirm a well-established covariance model.

According to developed hypotheses, we estimate three variations of the conceptual model (Figure 10), each focusing on a specific management control mechanism and a corresponding risk behaviour. One variant examines Results Control tightness in relation to slips and lapses (Model A), while the other two assess Action Control tightness in relation to routine violations (Model B) and exceptional violations (Model C). This design enables a focused assessment of how distinct control practices shape different forms of risky behaviour, while maintaining a consistent analytical framework across all estimations.

5.3.2 Sample and Data Collection

Data were collected from employees working in the selected medium-sized Bank operating in Kosovo. The target population included employees of the selected Bank working in its largest branch units, which collectively represent the organisation's most operationally important environments. Although the Bank operates with 35 branches nationwide, five of these branches account for a disproportionately large share of total customer volume, transactional workload, and operational-risk exposure. These branches were therefore purposively selected as the sampling frame, consistent with the study's focus on people-risk behaviours that are most likely to arise in busiest settings. Within each of the selected branches, all employees were invited to participate in the survey, resulting in a target population of frontline and operational personnel (N = 216). Branch directors were excluded because they had participated in the qualitative phase of the research, and their roles do not expose them to the same task-level operational demands as branch staff. This sampling logic ensured alignment with the research objective, as employees in these roles routinely handle customer transactions, documentation, verification, and system-based procedures and are therefore more likely to encounter conditions associated with slips, lapses, and rule violations. Organisational access was granted first by the Bank's Board and subsequently by senior management, with participation remaining entirely voluntary and anonymous. The online survey was administered via the 1KA platform between 18 September 2025 and 30 October 2025. After filtering out failed survey attempts, 150 responses were retained (69.4% response rate). Not all respondents answered every item; therefore, pairwise deletion was applied to retain the maximum amount of information for each analysis. This approach is suitable for PLS-SEM, which is robust to item-level missingness and does not require listwise deletion. The minimum number of valid cases among all retained items was 111, which is above recommended thresholds for PLS-SEM estimation and statistical power.

Respondents were invited to complete an online survey that assessed their perceptions of management control systems' tightness (results control, action control), risk culture, self-control, interactive use of risk management, and the frequency of selected risky behaviours (i.e., slips and lapses, routine violations, exceptional violations). Participation was voluntary

and anonymous. To minimise the common-method bias concerns, respondents were assured that there were no right or wrong answers and that their responses would be used solely for academic purposes; additionally, different response formats were used across sections of the questionnaire.

Survey-based research in which the same respondent provides data on both predictor and outcome variables is susceptible to common method bias (CMB), whereby observed covariation between constructs is partly attributable to the measurement method rather than to genuine construct relationships (Podsakoff et al., 2003). Several procedural controls were implemented at the design stage to reduce this risk. First, respondents were explicitly informed that there are no right or wrong answers and that their responses would be used solely for academic research purposes, reducing evaluation apprehension, which is one of the primary psychological mechanisms through which CMB inflates self-reported associations (Podsakoff et al., 2003). Second, the questionnaire was carefully worded to avoid judgemental or leading phrasing, particularly for items capturing behaviourally sensitive content such as rule violations and attentional errors. Third, response formats were deliberately varied across construct blocks: predictor constructs were measured on agreement-based Likert scales, while outcome constructs were measured on a separate frequency scale, reducing the likelihood that a uniform response tendency would artificially align predictors with outcomes. These procedural measures follow established recommendations for minimising CMB in organisational survey research (Podsakoff et al., 2003; Podsakoff et al., 2012).

Regarding non-response bias, the achieved response rate of 69.4% is relatively high for organisational survey research and reduces concerns about systematic non-participation. In addition, respondents were drawn from operational units with direct exposure to the studied phenomena, increasing the likelihood that the sample adequately reflects the relevant population. Non-response bias was assessed by comparing early and late respondents on all key constructs using independent samples *t*-tests and Mann-Whitney tests. No statistically significant differences were found across any construct (all $p > 0.05$). The combination of a high response rate, broad sampling coverage, the applied data collection procedures, and statistical evidence suggests that non-response bias is unlikely to materially affect the results.

Respondents represented a wide range of functional areas, hierarchical levels, and job roles, ensuring adequate variability in perceptions of controls and behavioural outcomes. Table 22 presents the sample structure by demographic variables (age, gender, education, and work experience) which were included as control variables in the structural model to account for individual-level differences known to influence work behaviour.

Table 22: Sample Structure by Demographic Variables

Demographic characteristic		Frequency	Percent
Gender	Male	50	43.86 %
	Female	64	56.14 %
	Other		0 %
		114	
Age	20 – 30	11	9.48 %
	31 – 40	29	25.00 %
	41 – 50	47	40.52 %
	51 – 60	24	20.69 %
	Over 61	5	4.31 %
		116	
Education	High school	18	15.52 %
	Bachelor degree	58	50.00 %
	Master degree	38	32.76 %
	Doctoral degree	2	1.72 %
		116	
Work experience	Less than 1 year	4	3.45 %
	1 – 2 years	5	4.31 %
	3 – 5 years	11	9.48 %
	6 – 10 years	12	10.34 %
	More than 10 years	84	72.41 %
		116	

Source: Own work.

The sample of respondents is approximately balanced by gender, with women slightly overrepresented (55%). The age distribution reflects a mature workforce, with the majority of respondents (41 – 50 years; 40%) in mid-career, followed by the 31 – 40 and 51 – 60 years groups. The distribution appears typical for banking environment, where many positions require experience, professional judgement, and knowledge of regulatory frameworks. Educational attainment is high, as expected for knowledge-intensive industry. Half of respondents (50%) holds a bachelor degree, and an additional 33% holds a master degree. Work experience is concentrated at the upper end: almost three quarters of respondents (72%) have more than 10 years of professional experience. This indicates that the sample consists largely of experienced employees, who have had substantial exposure to organisational controls, risk management practices, and operational processes. In this context, their perceptions of control systems and risk culture are likely to be informed by long-term observations, which increases the credibility and interpretative value of their responses.

5.3.3 Measures

Before describing the operationalisation of the study constructs, the questionnaire was pilot tested to assess the clarity, wording, and overall length of the instrument. The pilot study

involved five participants (four colleagues from a financial department and one bank employee) and was administered in paper form to facilitate direct feedback on item clarity and structure. Feedback from the pilot indicated that the questionnaire items were clearly worded, the overall length was appropriate, and no major ambiguities or practical issues were identified. Therefore, no changes were made prior to the final distribution of the questionnaire. Data collected during the pilot study were not included in the final analysis.

Construct operationalisation followed a combination of theoretical reasoning and empirical assessment. Prior to estimating the PLS-SEM models, an exploratory factor analysis (EFA) was conducted to examine the dimensionality of all multi-item scales. Principal factor extraction was used with both orthogonal (varimax) and oblique (promax) rotations. Two constructs (*Interactive Use* and *Risk Culture*) were operationalized as composite variables using mean scores because both represent aggregated organisational practices and norms rather than single latent traits; moreover, EFA results supported this choice.

By contrast, the behavioural outcome constructs (*Slips/Lapses*, *Routine Violations*, and *Exceptional Violations*) as well as the control constructs (*Results Control*, *Action Control*), and *Self-Control* were retained as reflective latent variables. Although EFA supported unidimensionality for these scales, item loadings exhibited greater heterogeneity, indicating that items contributed unequally to the underlying constructs. In such cases, latent variable modelling is preferable, as it allows the PLS algorithm to estimate indicator weights based on their empirical contribution rather than assuming equal weighting.

For the three behavioural outcome constructs, item selection was further guided by indicator reliability thresholds. Items with loadings below 0.40 were removed, while items loading between 0.40 and 0.70 were retained when theoretically important and supported by acceptable levels of construct reliability. This ensured both content validity and measurement quality, consistent with recommended PLS-SEM practices.

The complete set of measures is included in the Appendix 11. All constructs were measured using established multi-item scales from the literature, adapted to the banking context. Unless noted otherwise, respondents indicated their agreement on five-point Likert scales (1 = strongly disagree; 5 = strongly agree).

5.3.4 Main outcome variables – Frequency of risky behaviours

Participants were asked about the frequency of several types of slips, lapses, mistakes, and violations (not grouped into constructs in the actual questionnaire) on a scale of 1 to 5 , where 1 is never (“This has not happened at all.”) and 5 is very often (“This is a frequent and consistent part of my work experience occurring several times a week.”). We performed EFA to verify the validity of scales and based on results, we selected the most psychometrically sound construct specifications. Three forms of risky behaviour were used as outcome variables:

- ***Slips and Lapses (SLIPSLAPS):*** 6 items measuring unintentional, attention-based errors, adapted from Shakerian et al. (2019). EFA yielded a dominant first factor (eigenvalue = 2.50), while all remaining eigenvalues were close to zero or negative, indicating that a single construct underlies the indicators. All items loaded positively and meaningfully on the primary factor (0.49–0.72), with acceptable communalities. Although orthogonal and oblique rotations produced two artefactual factors, these were highly correlated and lacked theoretical interpretability, consistent with a strong general factor. The LR test ($\chi^2(15) = 246.14$, $p < 0.001$) further confirmed substantial common variance. On this basis, *Slips/Lapses* were treated as a unidimensional reflective latent construct in the structural models.
- ***Routine Violations of rules (RV):*** 3 items assessing habitual, intentional shortcuts or deviations from procedures done for efficiency, adapted from Shakerian et al. (2019). EFA was initially conducted on the four *RV* indicators and revealed a strong single factor (eigenvalue = 2.18) with three items loading highly (0.73–0.84), while item *RV4* showed a substantially weaker loading (0.50) and high uniqueness (0.75), indicating limited contribution to the underlying construct. Based on these results, item *RV4* was removed, and the final *RV* construct was specified using the remaining three indicators, all of which showed strong reliability and convergent validity in the PLS-SEM analysis.
- ***Exceptional Violations of rules (EV):*** 3 items capturing intentional deviations that occur in unusual or high-pressure situations, adapted from Shakerian et al. (2019). EFA confirmed a clear single-factor solution (eigenvalue = 1.80), with all items loading strongly on the latent dimension (0.72–0.82). Uniqueness values ranged between 0.33 and 0.48, indicating adequate shared variance. Since the items formed a coherent, unidimensional construct, all three were retained as unidimensional reflective latent construct for PLS-SEM analysis,

The behavioural-risk section of the questionnaire included additional items intended to capture Mistakes (MIS1-MIS3) and Situational Violations (SV1-SV3). These dimensions were not part of the theoretical model and exploratory analyses suggested weak psychometric structure and low conceptual coherence. For this reason, they were not included in the PLS-SEM models. The full item list is provided in the Appendix 11 for completeness and transparency.

5.3.5 Explanatory variables

Two types of management control systems' tightness were used as the main variables of interest. Because the items are manifestations of an underlying degree of tightness rather than formative components of it, both were modelled reflectively:

- **Results Controls (*RC*)**: measured using 5 items adapted from Agarwal and Ramaswami, (1993) capturing the tightness, specificity, and strictness of performance targets, accountability mechanisms, and performance monitoring. Items reflect the extent to

which performance outcomes are clearly defined and deviations are not tolerated. EFA suggested a clear one-factor structure, with a dominant factor (eigenvalue = 2.28) and all remaining eigenvalues well below zero. All items loaded acceptably on the single factor (0.54–0.81), and no cross-loadings or secondary factors emerged. The LR test ($\chi^2(10) = 236.60$, $p < 0.001$) confirmed substantial shared variance across indicators. Given this strong unidimensional structure, *RC* was treated as a reflective latent construct in the PLS-SEM models, with all five items retained.

- **Action Controls (*AC*):** measured using 5 items adapted from Agarwal and Ramaswami, (1993), reflecting the presence of detailed procedures, checklists, and behavioural prescriptions. The scale captures the restrictiveness and rigidity of rules governing task execution. EFA indicated a clear one-factor solution, with a dominant first factor (eigenvalue = 2.95) and all remaining eigenvalues close to zero or negative. All items loaded strongly on the single latent factor (0.74–0.81), and communalities were satisfactory. Rotated solutions did not reveal any interpretable secondary factors. The LR test ($\chi^2(10) = 367.96$, $p < 0.001$) confirmed significant shared variance among indicators. Given the unidimensional structure, *Action Control* was modelled as a reflective latent construct in the PLS-SEM analysis.

Alongside the two control constructs, the analysis includes supporting organisational and individual factors that shape how employees interpret and react to control systems:

- ***Risk Culture* (*R Culture*)**: measured using 14 items adapted from Dürst and Kunz (2025), capturing shared norms, expectations, and values regarding risk awareness, carefulness, and responsible conduct. The scale is multidimensional and reflects employees' perceptions of whether the organisation encourages risk-conscious behaviour. This conceptual structure already implies that *Risk Culture* represents a broad organizational property rather than a single reflective latent trait. EFA confirmed a multidimensional structure, with several secondary factors and cross-loadings. This pattern is consistent with the conceptualization of *Risk Culture* as a broad, higher-order factor rather than a single latent behavioural dimension. For this reason, we operationalised *Risk Culture* as a composite variable using the mean scores across its items.
- ***Interactive Use* (*INT*)**: assessed using 3 items adapted from Abernethy and Brownell (1999), capturing the extent to which managers use risk management tools for dialogue, learning, and shared attention to emerging issues. EFA pointed to a clear single-factor solution (eigenvalue of 1.80), with all items loading strongly on the same factor (0.7676; 0771; 0782), indicating unidimensionality, therefore we operationalized *INT* as an aggregate composite using the mean score of its items.
- ***Self-Control* (*SC*)**: measured using 11 items adapted from Tangney et al. (2018), capturing employees' capacity for self-regulation, attentional control, and adherence to behavioural standards (e.g., sustained focus, resisting shortcuts, maintaining accuracy). EFA was used to confirm that all items load to one factor (loadings from 0.46 to 0.82), which explains 88% of the common variance (eigenvalue of 5.36). Given the clear

dominance of the first factor and the strong, consistent loadings, *Self-Control* was treated as a reflective latent construct in the PLS-SEM models.

Table 23: Summary of Exploratory Factor Anlaysis for multi-item constructs

Construct	Items retained (assesed)	Eigenvalue (1st factor)	% Common variance explained*	Loading range (retained items)	Notes
Results Controls (RC)	5 (5)	2.28	46%	0.54–0.81	Single-factor structure; all items retained.
Action Controls (AC)	5 (5)	2.95	59%	0.74–0.81	Strong dominant factor; all items retained.
Risk Culture (RCulture)	14 (14)	7.99	— (multidim.)	Many > 0.70 but with cross-loadings	Multidimensional; operationalised as composite (mean score).
Self-Control (SC)	11 (11)	5.36	88%	0.46–0.82	Single-factor structure; all items retained.
Interactive Use (INT)	3 (3)	1.80	60%	0.77–0.78	Strong unidimensional factor; treated as composite (mean score).
Slips/Lapses (SLIPSLAPS)	6 (6)	2.50	42%	0.49–0.72	One dominant factor; all items retained.
Routine Violations (RV)	3 (4)	2.18	54%	0.73–0.84	One item (RV4) removed due to low loading (0.50) and high uniqueness (~0.75). Final construct uses 3 items.
Exceptional Violations (EV)	3 (3)	1.80	60%	0.72–0.82	Single-factor structure; all items retained.

Note: *% common variance refers to the variance accounted for by the first factor in principal factor analysis; values approximate due to PFA properties.*

Source: Own Work

5.3.6 Control variables

We used the following demographic variables as control variables:

- *Gender*: participants were asked about their gender – 0 if male, 1 if female, 2 if other.
- *Age*: participants were asked in which age category they are – 1 if 20-30, 2 if 31-40, 3 if 41-50, 4 if 51-60, 5 if over 61.

- *Education*: participants were asked about their education – 1 is high school degree, 2 is bachelor degree, 3 is master degree, and 4 is doctoral degree.

– *Experience*: participants were asked about their work experience – 1 is less than 1 year, 2 is 1-2 years, 3 is 3-5 years; 4 is 6-10 years, and 5 is more than 10 years.

5.3.7 Measurement Model Assessment

We assessed the reliability and validity of all reflective constructs following standard PLS-SEM guidelines.

- Internal consistency reliability was evaluated using Cronbach's alpha and composite reliability (CR), with thresholds of 0.70 considered acceptable (Hair et al., 2022; Nunnally & Bernstein, 1994).
- Convergent validity was assessed using average variance extracted (AVE), with values above 0.50 indicating adequate convergence (Fornell & Larcker, 1981).
- Indicator reliability was assessed by examining outer loadings; items below 0.40 were removed, and items between 0.40–0.70 were evaluated for theoretical importance and model fit.
- Discriminant validity assesses whether constructs in the model are empirically distinct from each other—meaning each construct captures a unique phenomenon. Discriminant validity was assessed using the Fornell–Larcker criterion and the heterotrait–monotrait ratio (HTMT), with HTMT values below conservative cut-off of 0.85 indicating satisfactory discriminant validity (Henseler et al., 2015).

Composite variables (*RCulture, INT*) are not assessed using AVE or CR, as these criteria apply only to reflective constructs.

Because all three structural models rely on the same reflective measurement model, indicator loadings and reliability assessments are very similar across Models A, B, and C, but not identical as in PLS-SEM the measurement and structural models are estimated jointly. All constructs met or exceeded recommended thresholds. Cross-loadings confirmed that items loaded more highly on their intended constructs than on any other constructs. All three models (A–C) demonstrated satisfactory convergent validity (all AVE values > 0.50) and internal consistency reliability (CR > 0.70). Discriminant validity was also supported in each model, based on both the Fornell–Larcker criterion and HTMT values below 0.85. The complete and detailed measurement model statistics for each model are provided in Appendices 12 – 14.

Given that all constructs were measured using a single survey instrument, the potential for common method bias was considered. Several procedural remedies were implemented at the design stage to reduce this risk. Participation was voluntary and anonymous, respondents were assured that there were no right or wrong answers, and different response formats were

used across sections of the questionnaire. In addition, the items were worded carefully to reduce ambiguity and evaluation apprehension, particularly for questions relating to behavioural deviations. Taken together, these design features reduce the likelihood that the observed relationships are primarily attributable to common method bias.

5.3.8 Structural Model Assessment

The structural models were assessed following Hair et al. (2022):

- Multicollinearity was examined using VIF values; all VIFs were below the recommended threshold of 5.
- Path coefficients were estimated using bootstrapping with 5,000 resamples to assess significance levels (bias-corrected and accelerated (BCa) confidence intervals).
- Coefficient of determination (R^2) values were inspected to evaluate explanatory power and evaluated according to thresholds recommended by Hair et al. (2022). We obtained moderate R^2 values for all behavioural outcomes, consistent with complex behavioural models.
- Effect sizes (f^2) were calculated to assess the substantive impact of individual predictors and were evaluated using Cohen's (1988) guidelines.
- Predictive relevance was assessed using the PLSpredict procedure in SmartPLS 4, with Q^2_predict values and prediction metrics (RMSE, MAE) were compared to the naïve benchmark (Indicator Average) following Shmueli et al. (2016).

Two statistical checks were conducted to assess common method bias. First, Harman's single-factor test on all construct indicators (N = 98) yielded a single factor accounting for 36.69% of total variance, well below the 50% threshold (Podsakoff et al., 2003). Second, a full collinearity VIF assessment (Kock, 2015) produced values ranging from 1.00 to 3.36 across all three models, with only one Self-Control indicator marginally exceeding the 3.3 threshold due to its central mediating role rather than method contamination. Both tests consistently suggest that common method bias is unlikely to be a major threat to the validity of the reported findings.

5.3.9 Ethical Considerations

The study adhered to standard ethical guidelines for research involving human participants. All respondents were informed about the purpose of the study, participation was voluntary, and confidentiality was guaranteed. No identifying information was collected.

5.4 Results

We interpret the results for each specification (model) in turn.

5.4.1 Model A

Model A examines how tight results control and risk culture shape employees' behavioural discipline, which in turn reduces the frequency of slips and lapses. The structural model includes *Results Control* (*RC*)*, Risk Culture (RCulture), Self-Control (SC),* and *Interactive Use (INT)*, with demographic variables entered as controls. *Results Control* reflects the degree of performance tightness (i.e., targets, expectations), while *Risk Culture* captures shared values and norms regarding risk awareness and responsible behaviour.

The measurement model for Model A was evaluated in accordance with recommended PLS-SEM criteria (summarized in Table 24, details in Appendix 12). All latent constructs demonstrated satisfactory internal consistency reliability, with Cronbach's α and composite reliability (CR) values exceeding the recommended threshold of 0.70 for all multi-item constructs, including *Results Control* (α = 0.805; CR = 0.860), *Self-Control* (α = 0.907; CR = 0.922), and *Slips/Lapses* (α = 0.810; CR = 0.861)

Convergent validity was confirmed for all multi-item constructs. Average variance extracted (AVE) values exceeded the 0.50 criterion for *Results Control* (0.555), *Self-Control* (0.524), and *Slips/Lapses* (0.512). Outer loadings for all retained indicators were above 0.50 and statistically significant. Items with moderate loadings (0.50–0.70) were retained based on theoretical justification and acceptable composite reliability, while no indicator fell below the 0.40 threshold.

Discriminant validity was assessed using the Fornell–Larcker criterion and the heterotrait–monotrait ratio (HTMT). According to the Fornell–Larcker criterion, the square root of the average variance extracted (AVE) for each construct must exceed its correlations with other constructs. This condition was satisfied for all constructs, indicating that each latent variable shares more variance with its own indicators than with any other construct. The HTMT statistic was also examined, as it provides a more robust assessment of discriminant validity. All HTMT values were well below 0.85 for all construct pairs, including the theoretically related constructs (e.g., *SC–SLIPSLAPS* = 0.340; *RC–SLIPSLAPS* = 0.318), providing evidence of adequate discriminant validity across the model. Taken together, the results support the discriminant validity of the measurement model. Overall, the measurement model met all reliability and validity requirements.

Table 24: Summary of Measurement Model A

Construct	Cronbach's α	CR	AVE	*INT*	*RC*	*RCulture*	*SC*	*SLIPS LAPS*
INT	1.000	1.000	1.000	**(1.00)**	0.440	0.361	0.109	0.016
RC	0.805	0.860	0.555	0.663	**(0.745)**	0.300	0.108	0.074
RCulture	1.000	1.000	1.000	0.601	0.548	**(1.00)**	0.291	0.018
SC	0.907	0.922	0.524	0.330	0.328	0.539	**(0.724)**	0.091
SLIPS LAPS	0.810	0.861	0.512	–0.125	–0.272	–0.133	–0.302	**(0.716)**

Notes: Values above the diagonal are squared Pearson correlations, values on the diagonal are square roots of AVE (Fornell–Larcker criterion). Values below the diagonal are Pearson correlations.

Source: Own Work

The results of model A structural estimation are presented in Table 25. Standardized path coefficients (β) are reported and interpreted. Figure 11 illustrates for which hypotheses we find support. Prior to evaluating structural relationships, the model was assessed for multicollinearity. All inner and outer VIF values were below the recommended threshold of 5, indicating that multicollinearity was not a concern. Inner VIF values for key predictors of *Slips/Lapses* (e.g., *RC*, *SC*, *INT*, *RCulture*) ranged from 1.546 to 2.357, confirming acceptable collinearity levels.

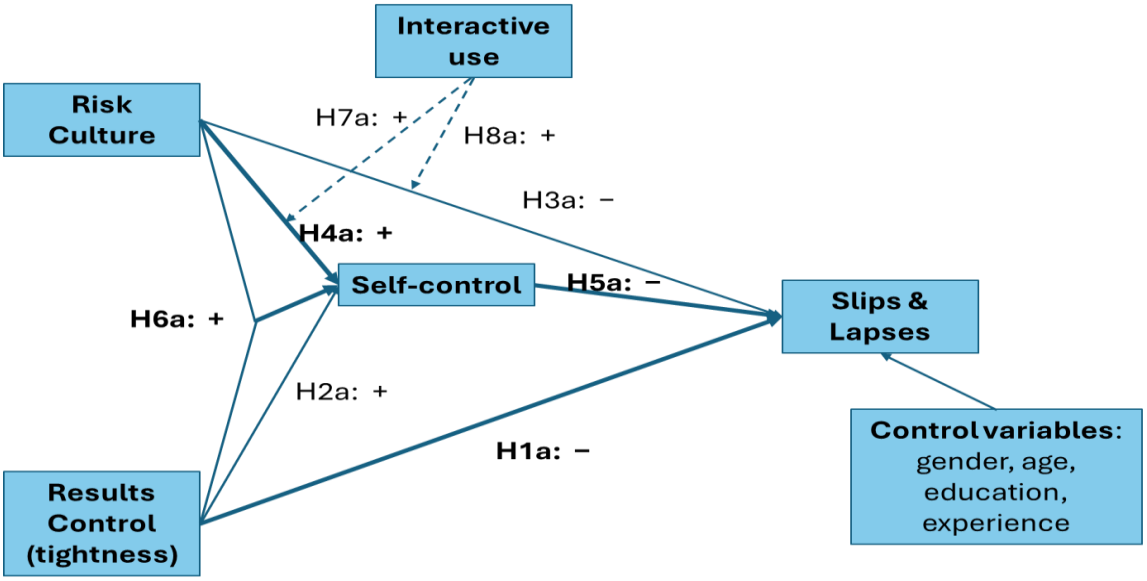
Table 25: Structural Model A - Summary of Standardized direct, indirect, and total effects

H	Relation between constructs	Direct β	Indirect β	Total β
1a	*RC → SLIPSLAPS*	-0.353 *	-0.006	-0.359 *
2a	*RC → SC*	0.019		0.019
3a	*RCulture → SLIPSLAPS*	0.185	-0.166 *	0.019
4a	*RCulture → SC*	0.567 ***		0.567 ***
5a	*SC → SLIPSLAPS*	-0.293 *		-0.293 *
6a	*RC×RCulture → SC*	0.183 *		0.183 *
	RC×RCulture → SLIPSLAPS	-0.059	-0.054	-0.113
	INT → SC	-0.004		-0.004
7a	*INT×RCulture → SC*	-0.049		-0.049
	INT → SLIPSLAPS	0.092	0.001	0.093
8a	*INT×RCulture → SLIPSLAPS*	0.014	0.014	0.028
	Model statistics:			
	SC: R^2 = 0.328 (adj. 0.304); Q^2predict = 0.193; RMSE 0.929; MAE 0.760			
	SLIPSLAPS: R^2 = 0.230 (adj. 0.175); Q^2predict = 0.034; RMSE 1.027; MAE 0.687			

Notes: ***, **, * significant at p<0.001, p<0.01, and p<0.05, respectively.

Source: Own Work

Figure 11: Model A - Empirically Supported Hypothesis



Notes: Hypothesized paths for which we find empirical support are shown in bold.

Source: Own Work

The structural paths demonstrate several meaningful effects. As hypothesised, tight *Results Controls* are directly associated with *Slips/Lapses*, with a significant negative effect (*RC* → *SLIPSLAPS*: β = –0.353, p = 0.032). However, we do not find support for the indirect effect on *Slips/Lapses* via *Self-Control* (p = 0.897). Although the direct effect of *Self-Control* on *Slips/Lapses* is expectedly significant and negative (*SC* → *SLIPSLAPS*: β = –0.293, p = 0.019), highlighting the role of internal behavioural regulation in preventing unintentional errors, we do not find that tight *Results Controls* are positively associated with *Self-Control* (*RC* → *SC*: p = 0.885).

In contrast, *Risk Culture* significantly increases *Self-Control* (*RCulture* → *SC*: β = 0.567, p < 0.001), but does not directly influence *Slips/Lapses* (p = 0.263). A key feature of the model involves the interaction effect between *Risk Culture* and *Results Control.* This joint effect on *Self-control* is positive and significant (*RCulture* × *RC* → *SC*: β = 0.183, p = 0.041), indicating that the impact of tight results controls on self-control becomes stronger when employees perceive a stronger risk culture. However, the interaction term is not significant for *Slips/Lapses* (p = 0.609).

Interactive use does not show significant direct effects on *Self-Control* or *Slips/Lapses*. The hypothesised amplifying role of *Interactive use* (*INT* × *RCulture*) is not supported for either *Self-Control* or *Slips/Lapses* (all p > 0.50). Indirect effects involving *Results Control*, *Interactive use*, and the two interaction terms are not significant.

Among controls, only *Gender* displays a significant effect on *Slips/Lapses* ($\beta = -0.454$, $p = 0.008$), indicating that women on average make less frequently slips and lapses, while *Age*, *Education*, and *Experience* remain insignificant.

The model explains 32.8% of the variance in *Self-Control* (R^2 of 0.328, adjusted 0.304), which represents a moderate explanatory power for an internal regulatory construct in behavioural settings. The model explains 23% of the variance in *Slips/Lapses* (R^2 of 0.230, adjusted 0.175), indicating weak but acceptable explanatory power, consistent with typical effect sizes observed in models predicting unintentional human error. Effect sizes (f^2) indicate that:

- *Risk Culture* has a substantial effect on *Self-Control* ($f^2 = 0.274$);
- *Results Control* has a small but relevant effects on *Slips/Lapses* ($f^2 = 0.078$);
- *Self-Control* has a small but relevant effect on *Slips/Lapses* ($f^2 = 0.072$);
- All other effects are negligible.

Predictive relevance was evaluated using the PLSpredict procedure implemented in SmartPLS 4. Both endogenous constructs exhibited positive Q^2_predict values (*SC* = 0.193; *Slips/Lapses* = 0.034), indicating that the model possesses out-of-sample predictive capability. Following Hair et al. (2022), the Q^2_predict value for *Self-Control* reflects medium predictive relevance, whereas the smaller Q^2_predict value for *Slips/Lapses* indicates low but acceptable predictive relevance for behavioural outcomes of this type. Taken together, the results confirm that Model A provides meaningful predictive performance at the latent variable level.

Model A reveals that tight results controls and self-control both contribute to reducing slips and lapses. Risk culture does not directly reduce these unintentional errors but exerts an important indirect effect through self-control. Moderation results show that risk culture strengthens the effect of results controls on self-control but does not enhance their direct effect on slips. Interactive use plays no meaningful role in this behavioural context.

5.4.2 Model B

The model examines how organisational control practices and cultural conditions shape employees' engagement in **routine violations**, i.e. intentional deviations from prescribed procedures carried out to improve efficiency or convenience. The structural model includes *Action Control* (*AC*)*, Risk Culture (RCulture), Self-Control (SC),* and *Interactive Use (INT)*, with demographic variables entered as controls. *Action Control* reflects the degree of procedural tightness (i.e., rules, standard operating procedures, checklists), while *Risk Culture* captures shared values and norms regarding risk awareness and responsible behaviour.

The measurement model for Model B showed strong psychometric properties (Table 26, details in Appendix 13). Internal consistency reliability was satisfactory for all reflective multi-item constructs. Cronbach's α values exceeded the recommended 0.70 threshold for *Action Control* (α = 0.882), *Self-Control* (α = 0.907), and *Routine Violations* (α = 0.859). Composite reliability (CR) values were also high, ranging from 0.913 for *AC* and *RV* to 0.923 for *SC*, indicating reliable internal consistency among indicators.

Convergent validity was confirmed via AVE, with all multi-item constructs demonstrating AVE above the 0.50 threshold: *Action Control* (0.676), *Self-Control* (0.524), and *Routine Violations* (0.778). All indicators loaded significantly on their respective constructs. No item fell below the 0.40 minimum loading criterion, and items between 0.50 and 0.70 were retained based on theoretical relevance and adequate CR values.

Discriminant validity was established using both the Fornell–Larcker criterion and HTMT. For each construct, the square root of the average variance extracted (AVE) exceeded all inter-construct correlations, indicating that the constructs share more variance with their own indicators than with other latent variables (Fornell & Larcker, 1981). HTMT values across all construct pairs were well below the 0.85 benchmark (e.g., *SC–RV* = 0.303; *AC–RV* = 0.160; *RCulture–INT* = 0.601), indicating satisfactory distinction among latent constructs. Overall, the measurement model satisfies all requirements for internal consistency, convergent validity, and discriminant validity.

Table 26: Summary of Measurement Model B

Construct	**Cronbach's α**	**CR**	**AVE**	***AC***	***INT***	***RCulture***	***SC***	***RV***
AC	0.882	0.913	0.676	**(0.822)**	0.504	0.373	0.104	0.018
INT	1.000	1.000	1.000	0.710	**(1.00)**	0.361	0.109	0.008
RCulture	1.000	1.000	1.000	0.611	0.601	**(1.00)**	0.291	0.004
SC	0.907	0.923	0.524	0.323	0.330	0.539	**(0.724)**	0.070
RV	0.859	0.913	0.778	–0.136	–0.087	–0.063	–0.265	**(0.882)**

Notes: Values above the diagonal are squared Pearson correlations, values on the diagonal are square roots of AVE (Fornell–Larcker criterion). Values below the diagonal are Pearson correlations.

Source: Own Work

The results of model B structural estimation are presented in Table 27. Standardized path coefficents (β) are reported and interpreted. Figure 12 illustrates for which hypotheses we

find support. Before examining path coefficients, multicollinearity was assessed. All inner VIF values were below 5, indicating no problematic multicollinearity levels among predictors: VIF values for predictors of *Routine Violations* ranged from 1.057 to 2.540, and for *Self-Control* from 1.772 to 2.372

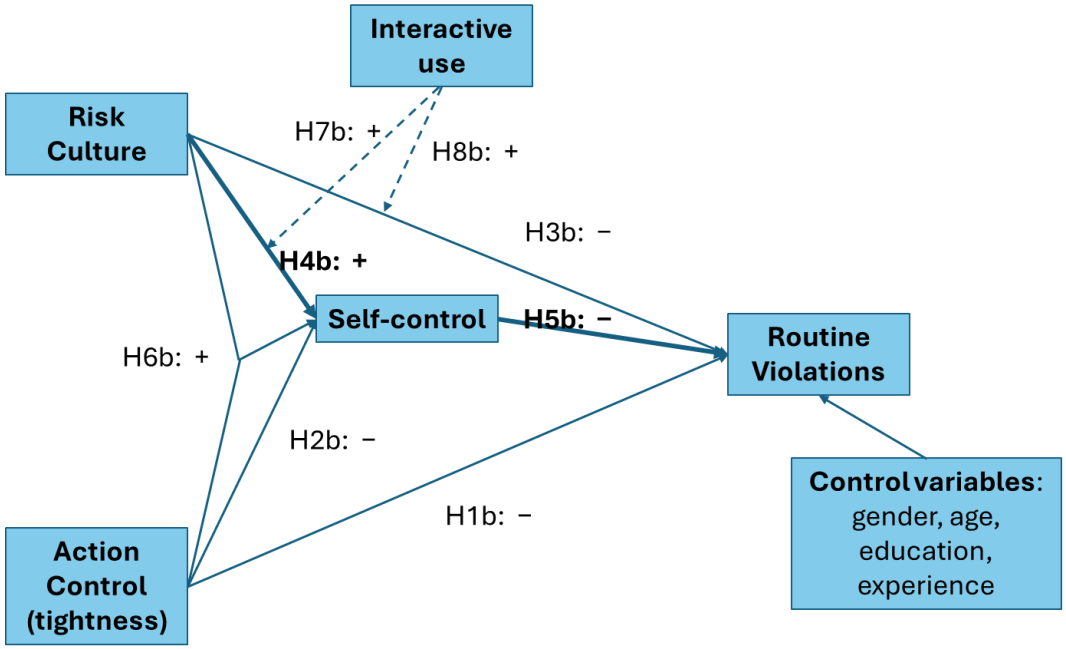
Table 27: Structural Model B - Summary of standardized, direct, indirect, and total effects

H	Relation between constructs	Direct β	Indirect β	Total β
1b	*AC → RV*	-0.263	0.008	-0.254
2b	*AC → SC*	-0.026		-0.026
3b	*RCulture → RV*	0.259	-0.176 *	0.083
4b	*RCulture → SC*	0.556 ***		0.556 ***
5b	*SC → RV*	-0.317 **		-0.317 **
6b	*AC×RCulture → SC*	0.171		0.171
	AC×RCulture →RV		-0.054	-0.054
	INT → SC	0.037		0.037
7b	*INT×RCulture → SC*	-0.066		-0.066
	INT → RV	0.037	-0.012	0.026
8b	*INT×RCulture → RV*	-0.102	0.021	-0.081
	Model statistics:			
	SC: R^2 = 0.314 (adj. 0.290); Q^2predict = 0.176; RMSE 0.936; MAE 0.763			
	RV: R^2 = 0.137 (adj. 0.082); Q^2predict = 0.187; RMSE 0.957; MAE 0.573			

Notes: ***, **, * significant at p<0.001, p<0.01, and p<0.05, respectively.

Source: Own Work

Figure 12: Model B - Empirically Supported Hypothesis



Source: Own Work

Contrary to expectations, tight *Action Control* does not directly reduce *Routine Violations* (β = –0.263, p = 0.230) and has no significant effect on *Self-Control* (β = –0.026, p = 0.846), indicating that tighter rules, procedures, and checklists do not appear to influence individual discipline, nor do they discourage employees from engaging in habitual, intentional shortcuts.

Consistent with theoretical expectations, *Self-Control* is strongly negatively associated with *Routine Violations* (*SC* → *RV*: β = –0.317, p = 0.004), indicating that internally regulated behaviour plays a central role in preventing habitual shortcuts.

Risk Culture exhibits a strong positive effect on *Self-Control* (*RCulture* → *SC*: β = 0.556, p < 0.001), suggesting that shared norms around carefulness and responsibility foster more disciplined individual behaviour. Although its direct effect on *Routine Violations* is not significant (*RCulture* → *RV*: β = 0.259, p = 0.216), the indirect effect of *Risk Culture* on *Routine Violations* through *Self-Control* is statistically significant and negative (-0.176, p = 0.025). This indicates that cultural norms reduce habitual violations only when they strengthen internal behavioural regulation. We do not find support for the hypothesised amplification of cultural and control effects on *Self-Control* or *Routine Violations*, as the interaction effect between *Risk Culture* and *Action Control* is not significant (*SC*: β = 0.171, p = 0.090; *RV*: p = 0.165).

All other indirect effects, including those involving *Action Control*, *Interactive use*, and interaction terms, are non-significant. *Interactive use* shows neither significant direct effects, nor significant interaction effects with *Risk Culture* on *Self-Control* (p = 0.612) or *Routine Violations* (p = 0.185). These findings indicate that discussion-oriented, learning-focused use of controls is largely unrelated to routine rule-breaking behaviour.

Demographic control variables do not play a major role. *Gender* shows a marginal negative effect (β = –0.311, p = 0.067) suggesting that women may violate rules less, but the effect does not reach conventional significance level.

The model demonstrates a modest explanatory power. *Routine Violations* show an R^2 of 0.137 (adjusted 0.082), and *Self-Control* an R^2 of 0.314 (adjusted 0.290), values typical for behavioural research involving complex models and multiple indirect pathways. Effect sizes (f^2) highlight that:

- *Risk Culture* has a substantial impact on *Self-Control* (f^2 = 0.254),
- *Self-Control* has a small effect on *Routine Violations* (f^2 = 0.079);
- All other predictors exhibit negligible f^2 values.

The model's out-of-sample predictive performance was evaluated using PLS predict and the cross-validated predictive ability test (CVPAT). Both endogenous constructs demonstrated meaningful predictive relevance, with Q^2_predict values well above zero (*SC* = 0.176; *RV* = 0.187). These values indicate moderate predictive power. Prediction error statistics (RMSE

and MAE) also support adequate predictive accuracy, with *Routine Violations* showing lower average prediction error than *Self-Control*. The CVPAT results further confirm the model's predictive capability: for both constructs, PLS-SEM exhibited significantly lower prediction loss than the Indicator Average (IA) benchmark (all $p < 0.001$). Collectively, these findings indicate that Model B demonstrates solid and statistically meaningful predictive accuracy, particularly for predicting intentional routine rule violations.

Model B indicates that tight action controls do not meaningfully reduce routine rule violations, nor do they influence employees' self-control. Instead, routine violations are primarily shaped by internal regulation: employees with higher self-control are significantly less likely to engage in habitual rule-breaking. Risk culture does not directly reduce routine violations but indirectly lowers them by strengthening self-control. Moderation effects of interactive use and cultural interactions with action controls are not supported. Overall, routine violations appear resistant to formal controls and more strongly influenced by internalised behavioural norms.

5.4.3 Model C

The model examines how organisational control practices and cultural conditions shape employees' engagement in **exceptional violations**, i.e. contextual and pressure-driven violations of rules and procedures. The structural model includes the same constructs as Model B, i.e. *Action Control* (*AC*)*, Risk Culture (RCulture), Self-Control (SC),* and *Interactive Use (INT)*, with demographic variables as controls.

The measurement model for Model C demonstrates similar psychometric quality as Model B (Table 28, details in Appendix 14). All multi-item reflective constructs achieved high internal consistency reliability, with Cronbach's α values well above the 0.70 threshold for *Action Control* ($\alpha = 0.882$), *Self-Control* ($\alpha = 0.907$), and *Exceptional Violations* ($\alpha = 0.844$). Composite reliability (CR) values also indicated strong consistency (*AC*: 0.913; *SC*: 0.923; *EV*: 0.906), satisfying recommended cut-offs.

Convergent validity was supported across constructs, with AVE values exceeding 0.50 for *AC* (0.677), *SC* (0.524), and *EV* (0.762). All outer loadings for reflective items were significant and above 0.50; no indicator fell below the 0.40 threshold. Items with moderate loadings (0.50–0.70) were retained due to theoretical relevance and satisfactory construct reliability.

Discriminant validity was confirmed using both the Fornell–Larcker criterion and HTMT ratios. All HTMT values remained below the 0.85 benchmark (e.g., *AC–EV* = 0.361; *SC–EV* = 0.421; *RCulture–INT* = 0.601), demonstrating that constructs are empirically distinct and appropriately measured. Overall, the measurement model satisfies all requirements for internal consistency, convergent validity, and discriminant validity.

Table 28: Summary of Measurement Model C

Construct	Cronbach's α	CR	AVE	*AC*	*INT*	*RCulture*	*SC*	*EV*
AC	0.882	0.913	0.677	**(0.823)**	0.503	0.373	0.103	0.110
INT	1.000	1.000	1.000	0.709	**(1.00)**	0.361	0.108	0.045
RCulture	1.000	1.000	1.000	0.611	0.601	**(1.00)**	0.288	0.030
SC	0.907	0.923	0.524	0.321	0.329	0.537	**(0.724)**	0.133
EV	0.844	0.906	0.762	–0.331	–0.213	–0.173	–0.365	**(0.873)**

Notes: Values above the diagonal are squared Pearson correlations, values on the diagonal are square roots of AVE (Fornell–Larcker criterion). Values below the diagonal are Pearson correlations.

Source: Own Work

The results of model C structural estimation are presented in Table 29. Standardized path coefficents (β) are reported and interpreted. Figure 13 illustrates for which hypotheses we find support. Before examining path coefficients, multicollinearity was assessed. All inner VIF values were below 5, indicating acceptable multicollinearity levels among predictors (e.g., VIF for *AC* → *EV* = 2.539; *RCulture* → *SC* = 1.775; *INT* → *EV* = 2.265)

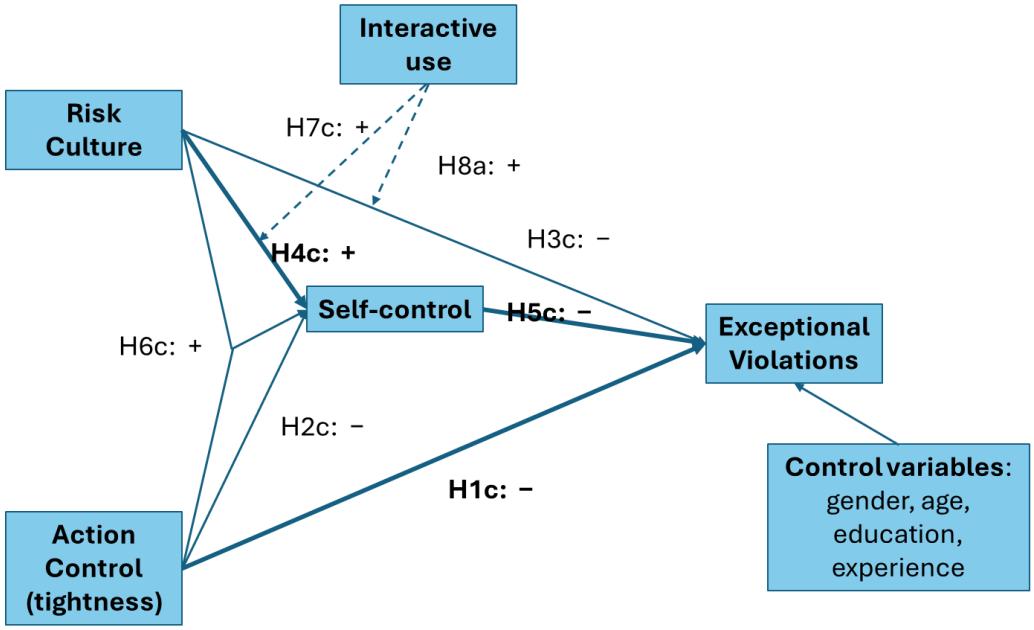
Table 29: Structural Model C: Summary of standardized direct, indirect, and total effects

H	Relation between constructs	Direct β	Indirect β	Total β
1c	*AC* → *EV*	-0.457 **	0.011	-0.446 **
2c	*AC* → *SC*	-0.029		-0.029
3c	*RCulture* → *EV*	0.306	-0.214 **	0.092
4c	*RCulture* → *SC*	0.556 ***		0.556 ***
5c	*SC* → *EV*	-0.385 ***		-0.385 ***
6c	*AC*×*RCulture* → *SC*	0.177		0.177
	AC×*RCulture* →*EV*		-0.068	-0.068
	INT → *SC*	0.039		0.039
7c	*INT*×*RCulture* → *SC*	-0.069		-0.069
	INT → *EV*	0.048	-0.015	0.033
8c	*INT*×*RCulture* → *EV*	-0.039	0.027	-0.012
	Model statistics: *SC*: R^2 = 0.313 (adj. 0.290); Q^2predict = 0.174; RMSE 0.937; MAE 0.763 *EV*: R^2 = 0.248 (adj. 0.199); Q^2predict = 0.198; RMSE 0.927; MAE 0.590			

Notes: ***, **, * significant at p<0.001, p<0.01, and p<0.05, respectively.

Source: Own Work

Figure 13: Model C - Empirically Supported Hypothesis



Source: Own Work

The model reveals several notable findings. First, tight *Action Control* is significantly negatively associated with *Exceptional Violations* (*AC* → *EV*: β = –0.457, p = 0.005), showing a strong intended effect of procedural strictness on situational rule-breaking. This effect is the strongest direct control effect across all three models. In contrast, *Action Control* is not significantly negatively associated with *Self-Control* (*AC* → *SC*: β = –0.029, p = 0.823) as hypothesized. Although this does not support our hypothesis, consistent to model B, also this model indicates that procedures do not build discipline. Exceptional violations occur when rules cannot be followed due to context. Therefore, adding rules (*AC*) does *not* prevent violations that occur when rules cannot be applied.

Second, when *Exceptional Violations* are the dependent variable, the effect of *Self-Control* is also significant (*SC* → *EV*: β = –0.385; p = 0.000), confirming that employees with higher internal self-regulation are less likely to deviate from procedures under exceptional circumstances**.** This supports the hypothesized relationship that exceptional violations require immediate judgment, and disciplined workers resist "doing the wrong thing under pressure." The negative effect of *Self-Control* on *Exceptional violations* is stronger than its effect on routine violations (model B). Routine violations are intentional shortcuts, habitual and socially normalised, and not shaped by self-control. Exceptional violations are situational, effort-dependent, and thus self-control matters more.

The direct effect of *Risk Culture* on *Exceptional Violations* is not significant (p = 0.079). Cultural norms do not directly prevent exceptional violations, but they strengthen self-control, which is the key behavioural mechanism in these situations. The effect of *Risk Culture* on *SC* remains positive and significant (*RCulture* → *SC*: β = 0.556, p < 0.001), which

indicates that risk culture builds self-control which in turn reduces exceptional violations. Thus, *Risk Culture* has a significant negative indirect effect on *Exceptional Violations* via *Self-Control* (*RCulture* → *SC* → *EV*: β = –0.214, p = 0.009), but not a direct one. Discipline matters when violations are situational, not habitual. This mirrors the pattern observed in Models A and B: cultural strength reduces risk behaviour primarily through supporting internalised self-regulation.

The indirect effects involving *Action Control*, *Interactive use*, and interaction terms are not significant. *Interactive use* has no significant direct effect on *Self-Control* or *Exceptional Violations*; control variables (*Gender*, *Age*, *Education*, *Experience*) are all statistically non-significant. Also, interaction effects *Risk Culture* × *AC* do not significantly influence *Self-Control* (β = 0.177, p = 0.072) or *Exceptional Violations* (p = 0.119). Similarly, we do not find evidence for the hypothesised amplifying effect of *Interactive use* (*INT* × *RCulture* not significant for either *SC* or *EV;* all p > 0.53).

The model exhibits moderate explanatory power: *Self-Control* is explained at $R^2 = 0.313$ (adjusted 0.290), and *Exceptional Violations* at $R^2 = 0.248$ (adjusted 0.199). Effect sizes (f^2) highlight that:

- *RCulture* has a large effect on *Self-Control* ($f^2 = 0.253$).
- *Self-Control* has a medium effect on *Exceptional Violations* ($f^2 = 0.135$).
- *Action Control* has a small-to-medium effect on *Exceptional Violations* ($f^2 = 0.110$).
- All remaining predictors have negligible effect sizes.

The predictive performance of Model C was assessed using PLSpredict and the cross-validated predictive ability test (CVPAT). Both endogenous constructs demonstrated positive Q^2_predict values (*SC* = 0.174; *EV* = 0.198), indicating meaningful out-of-sample predictive relevance. These values suggest moderate predictive ability, with stronger predictive accuracy for exceptional rule violations than for self-control. Prediction error statistics (RMSE and MAE) further support adequate predictive accuracy, with *EV* showing notably lower average error. The CVPAT results confirm the model's predictive superiority: for both endogenous constructs, prediction loss in the PLS model was significantly lower than in the Indicator Average benchmark (all p < 0.001). This demonstrates that Model C provides statistically superior and practically meaningful predictive performance**.**

Model C implies that tight action controls have a clear, significant, and negative effect on exceptional rule violations. Exceptional violations appear to be the domain where prescriptive rules "work as designed" by reducing situational rule-breaking. Self-control further contributes to preventing exceptional violations, and risk culture influences these behaviours indirectly by strengthening employees' internal self-regulation. No moderation effects are supported, and interactive use plays no meaningful role. Compared to the other models, Model C displays the strongest direct effect of a control mechanism on risk behaviour.

5.5 Discussion

In sum, our theoretical framework integrates tight controls, cultural context, control styles, and self-regulatory mechanisms to explain why controls designed to reduce operational risks sometimes succeed, sometimes fail, and sometimes generate new forms of risk behaviour.

Tight results controls impose demanding performance standards and link accountability directly to outcomes (Merchant & Van der Stede, 2017). Their intended function is to minimise errors by improving behavioural focus, clarifying expectations, and motivating careful task execution. At the same time, such controls can create time pressure (Linder et al., 2020), increase cognitive load (Becker & Green, 1962; Staal, 2004), and narrow attentional capacity, under which slips and lapses become more likely (Reason, 1990). This duality makes results controls inherently ambivalent: they can heighten vigilance, but they can also induce the very attentional failures they aim to prevent.

Empirical results for Model A confirm that self-control acts as the central behavioural mechanism linking organisational context to behavioural reliability. Risk culture exerts a strong positive influence on self-control, and self-control in turn significantly reduces the occurrence of slips. This mediation indicates that risk culture does not directly lower mistake rates; instead, it shapes how employees regulate their own behaviour. Employees in a strong risk-culture setting appear more capable of maintaining attentiveness, adhering to rules, and avoiding unintentional errors. In other words, behavioural reliability emerges through the development of individual discipline rather than through direct cultural pressure.

While results control does not directly influence self-control, the interaction effect shows that results control becomes effective only when embedded within a strong risk culture. In high-risk-culture environments, employees interpret performance goals and results metrics as part of a coherent system that reinforces careful, reliable work. Under weak risk culture, the same results control system would have no meaningful behavioural effect. This moderation demonstrates that the effectiveness of formal controls depends on cultural alignment. Results control alone is insufficient to enhance disciplined behaviour; it needs the interpretive frame provided by risk culture. This fits recent developments in management control research emphasising that formal mechanisms gain meaning and legitimacy through cultural and social processes (Malmi & Brown, 2008; Merchant & Van der Stede, 2017; Sandelin, 2008).

Interactive use of risk management does not significantly predict self-control or slips in this model, nor is it shaped strongly by risk culture. This suggests that interactive use operates independently from the mechanisms driving behavioural reliability here. Its role may be more relevant for learning, adaptability, or strategic responsiveness rather than routine operational reliability. In this behavioural-safety context, the primary levers appear to be cultural alignment and result-oriented monitoring rather than dialogue-based control.

Taken together, the model highlights a culturally enabled control system, in which:

1. Risk culture provides the normative foundation that encourages disciplined behaviour.
2. Self-control is the behavioural conduit through which this organisational environment shapes operational reliability.
3. Results control contributes to disciplined behaviour only when supported by an underlying cultural risk context.
4. Interactive use does not participate in this mechanism.

This supports a behavioural-control perspective in which reliable performance is enabled when formal controls and cultural norms reinforce one another, and where self-control plays the central mediating role.

Tight action controls regulate *how* work should be carried out by specifying procedures, standardising task execution, and constraining behavioural discretion (Merchant & Van der Stede, 2017). In principle, such controls should reduce rule violations by limiting opportunities for deviation. At the same time, highly prescriptive procedures can lower intrinsic motivation and create pressure to circumvent rules (Christ et al., 2012), especially when they are perceived as coercive, inefficient or misaligned with local conditions (Adler & Borys, 1996). Our three models show that these tensions play out differently for routine versus exceptional violations, and that action controls interact in systematic ways with risk culture and self-control.

In Model B (routine violations), tight action controls do not significantly reduce habitual rule-breaking, nor do they build self-control. Routine violations (i.e., shortcuts that are socially normalised and often justified as pragmatic responses to workload) appear largely insensitive to procedural tightening. Employees seem willing to bypass rules they perceive as rigid or inefficient, regardless of how detailed the procedures are. Instead, routine violations are primarily shaped by internal regulation and cultural context: self-control is negatively associated with routine violations, and risk culture reduces such behaviour indirectly by strengthening self-control. Thus, in the domain of routine, normalised violations, formal action controls are weak levers, whereas an internalised sense of responsibility, supported by a strong risk culture, matters more.

In Model C (exceptional violations), the pattern is different. Here, tight action controls have a clear and substantial negative effect on exceptional violations, while still failing to build self-control. Exceptional violations are situational decisions taken under pressure or in unusual circumstances, where employees weigh adherence to rules against perceived demands of the context. In this setting, prescriptive procedures "work as designed": they constrain improvisation and reduce the likelihood that employees abandon rules when facing exceptional situations. At the same time, self-control again plays an important role as employees with higher self-control are less inclined to violate rules even when circumstances

are exceptional. Risk culture does not directly reduce exceptional violations but exerts a consistent indirect effect by fostering self-control, which in turn lowers the likelihood of contextual rule-breaking.

Taken together with Model A (slips and lapses), the three models reveal a coherent behavioural taxonomy:

- Slips and lapses are cognitive errors, primarily shaped by self-control, which is itself strongly supported by risk culture. Tight results controls reduce slips directly, but their effect is amplified only when embedded in a strong risk culture, and they do not build discipline on their own.
- Routine violations are socially normalised shortcuts, relatively resistant to both results and action controls. They respond mainly to the pathway from risk culture to self-control: when risk culture strengthens internal regulation, routine violations decrease, but tightening procedures alone has little impact.
- Exceptional violations are situational decisions under pressure, where both self-control and action controls matter. Tight procedures directly suppress exceptional rule-breaking, while risk culture works indirectly by supporting disciplined judgement in unusual circumstances.

This combined evidence shows that different types of unsafe behaviour have different organisational antecedents. Slips and exceptional violations are shaped strongly by individual self-control, supported by risk culture, whereas routine violations are driven more by shared norms and the internalisation of those norms than by formal tightening of controls. Action controls are therefore not universally effective; they are powerful in the domain of exceptional violations, largely irrelevant for routine violations, and secondary to self-control for slips.

5.5.1 Implications for operational risk management in banks

The findings across the three models have several important implications for how banks design and implement operational risk controls. First, operational people-risk is often treated as a uniform behavioural category, yet the results reveal three distinct types of risk behaviour (slips, routine violations, and exceptional violations) each shaped by different antecedents. Slips and exceptional violations are primarily influenced by self-control, whereas routine violations respond mainly to cultural norms. Action and results controls therefore do not have uniform effects across behavioural categories. Effective operational people-risk management requires matching specific control mechanisms to the behavioural domain rather than relying on generic “tightening” of controls.

Second, the models show that simply adding rules, increasing procedural detail, or tightening performance targets does not automatically reduce behavioural risk. Tight action controls meaningfully reduce only exceptional violations, while routine violations remain unaffected.

Similarly, tight results controls reduce slips but do not shape self-control or intentional violations. These findings caution against the widespread practice of responding to incidents by increasing procedural intensity. Control accumulation, without behavioural fit, may create inefficiencies without lowering risk. Many authors argue that interactive use can counteract the tightness and rigidity of control systems (e.g., Davila et al., 2024; Ford et al., 2008; Kuminis & Dudau, 2012; Lewis et al., 2024; Mundy, 2010; Pilonato & Monfardini, 2020; Widener, 2007). Although interactive use of controls can foster learning and organisational adaptability, our models show that it plays no significant role in reducing slips or violations. Its benefits may lie in strategic or developmental domains rather than in frontline operational reliability. This suggests that banks should avoid relying on interactive control use as a mechanism for preventing everyday operational risk events but may reserve such use of risk management tools for addressing strategic risks.

Third, risk culture consistently strengthens self-control and self-control in turn reduces all three examined behavioural risk outcomes. This highlights risk culture as the deep structural antecedent of operational reliability. Banks aiming to reduce behavioural risk should therefore focus on strengthening local norms, shared expectations, and leadership signals that cultivate responsible conduct. Culture does not directly reduce mistakes or violations, but it builds the self-regulatory capacity that does. Moreover, the interaction patterns indicate that formal controls are most effective when supported by strong risk culture. Results controls reduce slips only when embedded in a strong cultural context, and cultural alignment amplifies the effect of formal mechanisms on self-control. Misaligned controls, by contrast, show little or no behavioural effect. Banks should therefore prioritise the alignment of formal controls and cultural norms over the intensification of control systems. Control design that is not culturally supported is unlikely to shape behaviour meaningfully.

Fourth, across the models, self-control is the only predictor that significantly reduces all three examined behavioural risk types. This identifies internal behavioural regulation, not merely compliance, as a key asset in operational risk management. Banks rarely monitor or develop self-control explicitly, but it can be supported indirectly when employees have clear expectations and sufficient autonomy to manage routine tasks independently. Such conditions enable individuals to regulate their own behaviour within the boundaries of established procedures. Integrating indicators of behavioural discipline into risk monitoring frameworks could strengthen early detection of emerging risk.

Together, the three models provide more precise behavioural insights into operational risk management:

- Cognitive reliability is best supported by cultural alignment and appropriate results controls.
- Routine rule adherence is primarily shaped by cultural norms and internalised discipline, not by added rules.

- Rule-following under pressure is improved through tight action controls combined with disciplined judgement.

These insights can guide banks in shaping a more effective, behaviourally informed approach to risk management systems that target the specific drivers of different forms of operational risk.

5.5.2 Limitations and future research

Several methodological limitations inherent to the survey-based design of this study should be acknowledged. First, despite the procedural controls implemented to reduce CMB (including response format variation, anonymity guarantees, and the reduction of evaluation apprehension), the single-source, single-time-point design means that CMB cannot be fully ruled out (Podsakoff et al., 2003). All predictor and outcome variables were collected from the same respondents in a single survey wave, which introduces the risk that some of the observed covariation between constructs reflects shared measurement context rather than genuine construct relationships. Although the statistical checks conducted did not indicate a severe CMB problem, this limitation should be considered when interpreting the magnitude of the reported associations. Second, the self-reported nature of the outcome variables introduces the possibility of social desirability bias. Items capturing the frequency of slips, lapses, and rule violations are behaviourally sensitive, and despite guaranteed anonymity, some respondents may have underreported the frequency of such behaviours. If present, this form of bias would attenuate the observed relationships, making the reported effect sizes conservative lower-bound estimates rather than inflated ones. Third, the outcome variables exhibit positively skewed distributions, reflecting the low base rate of operational errors and violations in a regulated banking environment. This pattern is theoretically expected and does not compromise the validity of PLS-SEM estimation, which is robust to non-normal distributions (Hair et al., 2022), but it does suggest that the frequency estimates represent a restricted range of the construct space, and that replication in higher-risk or less-regulated environments could yield stronger and more differentiated effects.

Although established and statistically validated measurement scales were used, the instruments may still fall short of fully capturing the underlying behavioural constructs, as all scales were originally developed and validated in contexts outside of banking. Future work could further refine or extend these measures to better represent the nuances of frontline risk behaviour.

Although the sample size is not unusually low for studies in highly specialised organisational settings, replication with larger datasets would strengthen the robustness of the structural relationships identified here.

The structural model necessarily simplifies the behavioural landscape of operational risk. Other potentially influential factors (e.g., specific cultural dimensions, ethical climates, or

leadership behaviours) were not included. Their omission means the estimates may be conservative, and future research could integrate these constructs to enhance explanatory power.

Finally, the cross-sectional design limits the conclusions to associative relationships. Causal inferences should therefore be made cautiously. Longitudinal or experimental designs would allow researchers to assess how behavioural mechanisms and control use evolve over time and whether observed associations reflect stable causal processes.

Building on these limitations, several promising avenues for further research emerge. Longitudinal analyses could explain the dynamic development of risk behaviour, control use, and reliability outcomes. Future models may incorporate additional constructs, such as organisational culture, ethical orientations, or leadership styles to deepen our understanding of behavioural antecedents. Another fruitful direction is to examine risk culture as an outcome variable in its own right, enabling a more integrated view of how behavioural controls shape broader organisational norms. Finally, more fine-grained investigation of action controls, rule violations, and the situational factors that influence them would address an underexplored area in operational risk research.

5.6 Conclusion

This chapter examined how management control problems shape the frequency of people-risk behaviours that contribute to operational risk in banking. Established measurement instruments were employed for all constructs, and the analysis focused on the relationships between tight results controls, tight action controls, risk culture, interactive use of risk management, self-control, and three categories of risky behaviour: slips and lapses, routine violations, and exceptional violations. Based on survey data from 150 employees of one bank and analysed with PLS-SEM, the chapter provided a quantitative test of the proposed model.

The results show that people-risk behaviours are not homogeneous but follow a coherent behavioural pattern. Slips and lapses emerge primarily as cognitive and attentional failures that are strongly shaped by self-control and indirectly by risk culture, which strengthens employees' internal discipline. Tight results controls reduce slips directly, but their effect is contingent on the presence of a strong risk culture, and they do not, on their own, build self-control. Routine violations appear largely insensitive to additional tightening of results or action controls; instead, they are mainly shaped by the pathway from risk culture to self-control, such that stronger risk culture and higher self-control are associated with fewer habitual shortcuts. Exceptional violations are most strongly influenced by tight action controls and self-control: detailed procedures effectively constrain rule-breaking in unusual or high-pressure situations, while risk culture again operates indirectly through its positive association with self-control.

Overall, the chapter confirms that tight controls can function as double-edged swords. Results and action controls do contribute to reducing specific types of risky behaviour, but their effects depend on the surrounding risk culture and on employees' ability to maintain self-control. Risk culture consistently strengthens self-control, and self-control in turn reduces all three forms of people-risk behaviour. Interactive use of risk management, by contrast, does not play a significant role in explaining slips-lapses, routine violations, or exceptional violations in this setting. These findings explain the conditions under which tight controls operate as intended and the circumstances under which their behavioural effects are limited.

The analysis further advances understanding by differentiating the behavioural mechanisms through which people-risk emerges. Slips–lapses, routine violations, and exceptional violations arise through distinct organisational pathways, and these differences help explain why a single control strategy cannot address all forms of behavioural risk. The results show that operational reliability depends not only on the design of tight controls but also on the cultural environment that supports employees' self-control. Therefore, the chapter offers a clearer empirical basis for interpreting how control design, cultural norms, and individual self-control jointly influence the behavioural origins of operational risk in banking.

6 DISCUSSION

6.1 Restating the research problem

Management control systems (MCS) have traditionally been conceptualised as instruments for aligning behaviour with organisational objectives, supporting strategy implementation, and ensuring accountability (Anthony, 1965; Malmi & Brown, 2008; Simons, 1995). At the same time, a substantial body of research shows that these systems may also generate unintended and dysfunctional consequences (e.g., Cugueró-Escofet & Rosanas, 2017; Goebel & Weißenberger, 2016; Speklé & Verbeeten, 2014; Van der Stede, 2000). Building on Merchant and Van der Stede (2017), we understand control problems as behavioural manifestations that arise when individuals experience lack of direction, motivational problems, or personal limitations in the face of control demands. In such situations, responses such as budgetary slack, gaming practices, symbolic compliance, and ethical erosion may emerge (e.g., Langfield-Smith & Smith, 2003; Rosanas & Velilla, 2005; Schweitzer et al., 2002; Van der Stede, 2000), and undermine the integrity and effectiveness of control systems. The theoretical and practical challenge, therefore, is not whether control problems exist, but under what conditions particular controls generate detrimental effects and through which mechanisms these outcomes take shape. Although prior research documents dysfunctional consequences (e.g., Fiolleau et al., 2018; Malmi et al., 2022), it often does so without consistently tracing the underlying behavioural mechanisms or clarifying how different control types can produce distinct patterns of dysfunction.

Importantly, management control systems are not only sources of potential dysfunction, but also essential organisational mechanisms for coordination, accountability, and performance. When appropriately designed and used, MCS help organisations translate objectives into action, structure expectations, support decision-making, and maintain operational discipline. The contribution of this dissertation therefore does not lie in questioning the value or necessity of MCS as such. Rather, it lies in examining a more specific but theoretically and practically important issue: the conditions under which systems intended to generate these benefits may also give rise to control problems and unintended behavioural responses. In the banking context, this issue becomes especially significant because such responses may contribute to operational vulnerabilities that affect not only organisational reliability but also the stability of the broader financial system, given the systemic externalities that banking failures can generate.

For this reason, the discussion focuses on interpreting what the dissertation's findings imply for understanding how management control problems emerge and how these problems shape operational risk in banking. This linkage is especially salient in banks because operational risk is not only a regulatory category but also an organisational outcome that is produced through controlled work processes, compliance routines, and employees' behavioural adaptations to control demands. Therefore, this discussion interprets the findings in relation to the three research questions and reflects on their implications for management control theory and operational risk management in banking.

In this context, operational risk has become one of the most prominent risk categories in banking, particularly following the Basel II and Basel III frameworks, which formalised it as a distinct regulatory construct and emphasised systematic identification, assessment, and mitigation of risks arising from failures in processes, systems, people, or external events (Basel Committee, 2003, 2006, 2011). Much of the early and mainstream work on operational risk focused on measurement, modelling, and capital allocation (Chapelle et al., 2004), often treating operational risk as a technical category linked to indicators, loss data, and regulatory monitoring. More recent contributions argue that operational risk emerges through organisational and behavioural processes shaped by how individuals interpret, enact, or circumvent organisational controls in practice (Faugère & Stul, 2021; Liang et al., 2024; Xu et al., 2017). This shift is central for interpreting the dissertation's research questions because it positions operational risk not only as a regulatory classification, but also as an outcome that is behaviourally produced and therefore plausibly connected to management control problems.

Despite these developments, the links between management control systems and operational risk exposures remain only partially explored, and the two fields remain insufficiently integrated. Research in management accounting has primarily examined dysfunctional consequences of targets, incentives, rules, and cultural interventions, including gaming, slack, symbolic compliance, and ethical erosion (Bromwich & Scapens, 2016; Fiolleau et al., 2018; Franco-Santos et al., 2012; Li & Evans, 2022; Müller et al., 2025; Van Camp &

Braet, 2016). In contrast, the operational risk and regulatory literature focus mainly on loss events, governance arrangements, and regulatory frameworks, emphasising measurement, capital allocation, and compliance structures (Cornalba & Giudici, 2004; Cruz et al., 1998; Fontnouvelle et al., 2005; Moosa, 2007; Power, 2005). Although both streams increasingly acknowledge behavioural and organisational dimensions of risk, they have largely evolved in parallel, with limited conceptual or empirical integration between management control and operational risk research (Collier et al., 2007; Miller et al., 2008; Soin & Scheytt, 2010). As a result, the interpretation of how specific types of controls generate particular control problems, how these problems materialise in banking practice, has remained unexplored.

In this dissertation, we address this integration gap. Specifically, we focus on explaining how management control problems emerge and how these problems influence operational risk in banking. Our goal is not simply to demonstrate that MCS may generate adverse outcomes, but to specify how particular types of controls relate to distinct behavioural mechanisms and how these mechanisms translate into observable organisational vulnerabilities that are relevant for operational risk in banking. In doing so, the dissertation connects management control systems and operational risk as interdependent layers of control and highlights how behavioural responses to formal controls constitute a key pathway through which operational risk exposures develop.

The dissertation is organised into four main chapters, each addressing a specific part of the overall research aim. The first chapter provides a systematic literature review that establishes the theoretical grounding for understanding management control systems and control problems. The second chapter extends this review into the context of operational risk in banking, examining how management control literature discussed operational risk-related issues and regulatory frameworks. The third chapter presents a qualitative analysis of management control systems within an organisational banking setting and empirically explores how management control problems translate to operational risk. The fourth chapter builds on this by presenting a quantitative examination of the behavioural components relevant to management control systems and operational risk.

Overall, this dissertation study:

− identifies how different types of management control systems (result, action, personnel and cultural controls) give rise to specific categories of management control problems;

− synthesises existing research into a structured framework that clarifies the behavioural, psychological, and ethical manifestations of control problems and the mechanisms through which they emerge;

− examines empirically how these control problems materialise in banking practice, based on qualitative evidence from organisational actors responsible for risk, compliance, operations, and employee oversight;

− links identified control problems to operational risk exposures by situating them within regulatory classifications and organisational risk processes;

− demonstrates the behavioural consequences of control problems by analysing how variations in control tightness, risk culture, and self-regulation relate to people-risk behaviours in operational settings;

− provides evidence on how management controls influence behaviours that precede operational failures, thereby clarifying the behavioural pathways through which operational risk develops in banking.

6.2 Summarising key findings

Our findings reveal how management control systems constitute both a regulating and risk-generating organisational infrastructure in banking. Rather than functioning solely as instruments for alignment and accountability (Merchant & Van der Stede, 2017; Simons, 1995), our analysis demonstrates that controls also become sources of behavioural, psychological, and ethical vulnerabilities when design and use features are misaligned with organisational context. By systematically classifying unintended consequences of result, action, personnel, and cultural controls, we conceptualise how the darker side of control emerges through identifiable mechanisms rather than random behavioural deviations. In doing so, we extend prior work on unintended consequences of performance measurement systems, incentive schemes, behavioural controls, and ethical infrastructures (e.g., Fiolleau et al., 2018; Franco-Santos et al., 2012; Linder et al., 2020; Müller et al., 2025) and provide an analytically structured explanation of problematic control dynamics.

In Chapter 2, we conducted a systematic literature review to clarify how different types of management controls give rise to distinct categories of control problems. The review showed that result controls commonly produce dysfunctional consequences such as gaming, slack creation, tunnel vision, and data manipulation; action controls often lead to rule-bending, habitual compliance, or procedural avoidance; personnel controls produce mistrust, capability misalignment, or motivation misfit; while cultural controls are linked to symbolic ethics, norm confusion, or value rejection. These behavioural, psychological, and ethical manifestations were not treated as isolated findings but were traced to six foundational mechanisms: overly rigid or coercive design, misfit with values or context, crowding out of intrinsic motivation, lack of participation and autonomy, symbolic or inconsistent use of controls, and design–use misalignment. This systematic classification moves beyond descriptive reporting of unintended consequences and contributes a mechanism-based explanation of how and why control problems emerge.

Building on this foundation, Chapter 3 examined how management control problems relate to operational risk in the banking sector. Reviewing literature on operational risk regulation (Basel Committee, 2003, 2006, 2011), behavioural responses to risk systems (e.g., Mikes,

2009; Power, 2007), and internal governance failures (e.g., Gontarek, 2016; Siaw Ofori et al. 2025), we demonstrate that control problems precede operational exposures in systematic ways. In particular, structure-related weaknesses, rigid procedural enforcement, incentive contradictions, capability asymmetries and cultural inconsistencies were shown to align with established loss categories such as processing errors, internal fraud, mis-selling behaviour, inadequate supervision, and ethical breaches. This confirms that operational risk is not only a process or system-related phenomenon, but also behavioural and control-generated in nature.

In Chapter 4, we deepen this understanding through qualitative evidence from a case-study banking environment. Interview insights reveal that structural pressures, rigid documentation requirements, conflicting directives, role ambiguity, and insufficient training act as activating conditions through which control mechanisms translate into exposures. Interviews with risk, compliance, operational managers and branch-level actors showed how multiple control systems interact and intensify friction points. For example, tight action controls increased workload pressure and encouraged procedural shortcuts; incentive-related controls created conditions for selective reporting; capability gaps contributed to error repetition; and inconsistencies in behavioural expectations reduced ethical coherence. These dynamics further confirmed that control problems do not exist only as abstract constructs, but materialise in operational routines, supervision practices, documentation procedures, and customer interactions (Burns et al., 2000; Dechow & Mouritsen, 2005; Feldman & Pentland,2003).

Chapter 5 extends this contribution quantitatively by examining the behavioural consequences of management control problems. Using survey evidence from operational employees, we demonstrate that variations in tightness of controls, self-regulation capacity, and risk culture predict the frequency of three categories of people-risk behaviour: slips/lapses, routine violations, and exceptional violations. These behaviours represent indicators of operational risk emergence and align with behaviourally grounded perspectives in risk research. Our model confirms that risk culture supports self-control (e.g., Grieser and Pedell, 2022; Jia et al., 2015), and that self-control reduces behavioural precursors of operational loss (Pang et al., 2015), thus providing statistically grounded evidence for pathways identified in earlier chapters.

Taken together, this dissertation provides an integrated explanation of how management controls shape operational reliability. Result controls, action controls, personnel controls, and cultural controls, individually and in combination can create context-dependent vulnerabilities that influence people-risk behaviour and therefore operational risk. By identifying mechanisms, validating them in organisational practice, and subjecting them to quantitative testing, the dissertation responds to gaps identified in prior literature, clarifying how control systems operate not only as behavioural regulators but also as behavioural risk generators.

6.3 Interpretation of the results

The aim of this dissertation is to deepen the theoretical understanding of how management control systems generate management control problems and how these problems relate to operational risk in banking. Our focus unfolds across three layers: first, we concentrate on management control systems (MCS) and the specific types of control problems they create; second, we examine how these control problems are linked to operational risk in banking; and third, we analyse how organisational mechanisms and behavioural pathways connect management control problems to people-risk behaviours that precede operational failures.

In relation to the first research question, the discussion interprets how different types of management control systems: result, action, personnel, and cultural controls, generate distinct management control problems through identifiable behavioural, psychological, and ethical mechanisms.

In the first layer, we develop a comprehensive overview of how different types of MCS – result controls, action controls, personnel controls, and cultural controls can be linked to recurring patterns of dysfunctional behaviour, depending on how these controls are designed, implemented and enacted in practice. Using Merchant and Van der Stede's (2017) Object of Control framework as a behavioural lens, we classify manifested control problems into behavioural, psychological, and ethical categories and interpret them through six recurrent mechanisms: overly rigid or coercive design, misfit with values or context, crowding out of intrinsic motivation, lack of participation and autonomy, symbolic or inconsistent use of controls, and design–use misalignment.

This mapping clarifies that the "darker side" of controls does not arise randomly, but through identifiable mechanisms triggered by how controls are designed and used and moderated by contextual factors. For example, overly rigid or coercive control design aligns with concerns in the literature showing that tight controls and coercive procedures can generate stress, alienation, and resistance among employees (Adler & Borys, 1996; Linder et al., 2020). Similarly, misfit with values or context reflects well-established evidence that controls which are poorly aligned with local culture or task characteristics are more likely to be ignored or to provoke workarounds (Jaworski, 1988).Crowding out of intrinsic motivation resonates with research showing how strong extrinsic incentives and formalisation can undermine intrinsic commitment and ethical norms (Sorauren, 2000), and lack of participation and autonomy reinforces findings on budgeting, performance evaluation and resistance, where limited voice and perceived unfairness foster slack, gaming, and withdrawal (Elmassri & Harris, 2011; Merchant & Van der Stede, 2017; Onsi, 1973). Symbolic or inconsistent use of controls connects to studies of symbolic ethics and decoupling, where codes of conduct and cultural programs become ceremonial, producing cynicism and moral disengagement rather than genuine alignment (Kaptein, 2011; Weaver et al., 1999). Finally, design–use misalignment captures situations in which controls that are reasonable in principle become

dysfunctional due to how managers enact them in practice, for example when diagnostic use dominates where interactive use is needed (Henri, 2006).

Our synthesis also indicates that each control type tends to be associated with a characteristic risk profile. Result controls are frequently linked to gaming, data manipulation, tunnel vision, slack creation, and stress (e.g., Goebel & Weißenberger, 2016; Grizzle, 2002; Merchant, 1990; Speklé & Verbeeten, 2014); action controls tend to be associated with employee alienation, routine rule violations, micromanagement, and role conflicts (e.g., Christ et al., 2012; Jurkiewicz & Giacalone, 2014; Lagios et al., 2023) personnel controls, when problematic, are associated with mistrust, deviance, and motivation misfit (e.g., Campbell, 2012; MacKenzie et al., 2011; MacLane & Walmsley, 2010), and cultural control failures are associated with norm confusion, symbolic ethics, ethical drift, and rejection of controls (Malmi et al., 2022; Van Fleet and Griffin, 2006; Weaver et al., 1999). By bringing these recurrent patterns together, we offer a structured behavioural map that helps researchers and practitioners anticipate which kinds of control problems are most likely to arise under different control regimes and combinations.

At the same time, the results show that these mechanisms and manifestations are shaped by contextual conditions. The reviewed literature highlights the moderating roles of task uncertainty and complexity, cultural and professional norms, leadership style and ethical tone, organisational structure, and external pressures. Contexts characterised by high uncertainty or complex tasks make rigid, simplified controls more prone to failure (Brownell & Hirst, 1986), while cultural and professional norms determine whether controls are perceived as legitimate or intrusive. Leadership style and ethical tone influence whether controls are interpreted as supportive or punitive, aligning with evidence on ethical infrastructure and tone at the top (Kaptein, 2011; Weaver et al., 1999). Organisational structure, including siloed arrangements and fragmented governance, shapes how control packages interact (Bedford, 2020; Ferreira & Otley, 2009; Malmi & Brown, 2008), and external pressures – regulatory, market, or crisis-driven – intensify result-based pressures that can trigger gaming and unethical behaviour (Cheng & Coyte, 2014; Cravens et al., 2004; Franco-Santos et al., 2012; Linder et al., 2020).

In relation to the second research question, the discussion interprets how these management control problems relate to operational risk in banking, by showing how control-related vulnerabilities translate into Basel II/III operational risk exposures.

The second layer of the dissertation interprets these insights within the specific domain of operational risk in banking. Here, we use a targeted literature review to examine how management control problems underlie operational risk events as defined in Basel II/III. Building on contributions that view operational risk not only as a technical loss category but as an outcome of organisational and behavioural processes (Cendrowski & Mair, 2015; Mikes, 2009; Power, 2007), we show that weaknesses in result, action, personnel, and cultural controls translate into operational exposures through concrete mechanisms.

Rules and procedures that are excessively formalised, fragmented, or inconsistently enforced create fertile ground for process failures, workarounds, and compliance gaps (e.g., Lim et al., 2017; Moosa, 2017; Ringgaard et al., 2025). Structural arrangements (e.g., siloed units, unclear responsibilities, unintegrated systems) weaken feedback loops and complicate coordination, making it difficult to identify and manage emerging risks (e.g., Cornwell et al., 2023; Mabwe et al., 2022; Soin & Collier, 2013). Incentive systems that prioritise sales, volume, or short-term metrics over risk-conscious behaviour encourage mis-selling, procedural shortcuts, and data manipulation, thereby increasing the likelihood of internal fraud or misreporting (e.g., Butler & Brooks, 2024; Caretta et al, 2024; Faugère & Stul, 2021). Cultural dynamics, finally, is central: when commercial culture dominates risk culture, when speaking up is discouraged, or when risk messages remain symbolic rather than enacted, operational risks accumulate and remain under-reported (e.g., Brauman et al., 2020; Kunz & Heitz, 2021; Laguecir & Leca 2022). Across these categories, operational risk emerges as a phenomenon that is tightly coupled to how control systems are designed and enacted, rather than as a purely external shock or system failure.

In this way, the literature-based analysis develops two overarching theoretical mechanisms, design–use misalignment and behavioural–institutional coupling, that provide the conceptual bridge between management control problems and operational risk. Design–use misalignment captures vulnerabilities that occur when the intended design of controls diverges from their use in practice, for example when checklists become ritualistic, indicators are monitored without corrective action, or risk tools are applied primarily for compliance rather than learning. Behavioural–institutional coupling captures how local norms, informal practices, incentives, and cultural expectations interact with formal controls, sometimes reinforcing them but often normalising workarounds, selective compliance, and tolerance for deviance. Together, these mechanisms explain how supposedly robust control systems can become sources of operational risk.

The third layer of the dissertation interprets how these theoretical mechanisms materialise within a specific banking organisation. The qualitative case study shows that design–use misalignment and behavioural–institutional coupling takes on concrete forms through a set of organisational mechanisms that we group into two aggregate dimensions: Design-Driven Control Problems and Human-Capability & Behavioural Control Problems.

Design-Driven Control Problems encompass structural vulnerabilities, rule-induced constraints, and incentive misalignments. Structural vulnerabilities refer to weaknesses in system configuration, automation, and cross-process integration: fragmented systems, incomplete automation, system errors with wide impact, IT vendor limitations, and infrastructural growth that lags organisational complexity. These vulnerabilities appear even where formal rules and procedures are well designed, demonstrating that structural problems are socio-technical rather than purely organisational and that controls depend on adequate infrastructure to function as intended. Rule-induced constraints capture the burdens of rigid procedural design, standardised routines, and extensive documentation demands, which

increase workload, slow responses, and can generate pressures for informal shortcuts. Incentive misalignments arise from the configuration and use of performance evaluation systems, such as demanding thresholds for bonus eligibility, inconsistent application of SMART criteria, and strong reliance on Management by Objectives. These design features encourage employees to prioritise target attainment over procedural integrity, aligning with prior evidence that performance-sensitive compensation can foster moral hazard and ethical blindness (Acrey et al., 2011; Cohn et al., 2014; Merchant & Van der Stede, 2017; Posch, 2020; Tran et al., 2021).

Human-Capability & Behavioural Control Problems encompass workforce capability and capacity limitations, as well as cultural and ethical drift. Workforce capability and capacity limitations refer to skill gaps, inconsistent past training, heavy workloads, and turnover driven by migration. These conditions constrain human capital and increase vulnerability to human error, particularly in manual and fraud-sensitive tasks. Cultural and ethical drift captures discrepancies between formal ethical and risk norms and their enactment in practice. Behaviours based on trust, convenience, or informal rules, such as bypassing system confirmations or relying on personal familiarity, illustrate how cultural controls can be unevenly internalised. In such cases, this uneven internalisation leads to norm confusion, under-enforcement, and ethical drift. These mechanisms correspond closely to Basel II/III risk categories such as Execution, Delivery & Process Management, Internal Fraud, and Business Practices, while the Bank's Loss Event Report corroborates the centrality of internal control design and use in shaping loss patterns.

The qualitative evidence refines and extends the theoretical model by showing that design-driven and human-capability mechanisms are intertwined in practice. Structural vulnerabilities and rule-induced constraints shape how employees experience controls, while capability limitations and cultural drift influence how they respond to these demands. Behavioural–institutional coupling is visible in the ways employees normalise workarounds, rely on informal coordination, or prioritise commercial objectives, thereby altering how controls operate in reality. The findings therefore support the view that operational risk emerges from the interaction between formal control architectures and lived organisational practices, rather than from isolated failures in one domain.

In relation to the third research question, the quantitative analysis examines how management control problems influence people-risk behaviours such as slips and lapses, routine violations, and exceptional violations that act as behavioural precursors to operational loss.

The quantitative study deepens this interpretation by examining how management control problems are reflected in people-risk behaviours. Focusing on tight results controls, tight action controls, risk culture, interactive use of risk management, and self-control, the analysis differentiates three categories of people-risk behaviour: slips and lapses, routine violations, and exceptional violations. Across the tested models, self-control consistently

appears as the only predictor that reduces all three categories of risky behaviour, while risk culture operates primarily by strengthening self-control rather than directly lowering risk behaviours. Tight results controls reduce slips and lapses, but do not strengthen self-control, and their effectiveness depends on a strong risk culture. Tight action controls reduce exceptional violations, but they do not reduce routine violations nor build internal discipline in that domain. Interactive use of risk management does not exhibit the expected amplifying effects.

These results suggest that people-risk is not a homogeneous construct, but comprises distinct behavioural categories shaped by different organisational mechanisms. Slips and lapses are influenced by how performance demands and internal discipline interact; routine violations are particularly resistant to formal tightening and are influenced mainly through self-control supported by risk culture; exceptional violations respond to detailed procedures that constrain situational deviations. The findings reinforce the idea that tight controls function as double-edged mechanisms: they can reduce certain forms of behavioural risk, but their effectiveness is contingent on the surrounding risk culture and on employees' behavioural capacities.

Overall, the interpretation of results across all four core chapters shows that management control problems and operational risk in banking are co-produced by control design, control use, organisational structures, and behavioural responses. The dissertation indicates that simply tightening controls by adding rules, raising performance demands, or layering additional systems does not automatically reduce operational risk. Instead, operational reliability depends on how management control systems are configured, how they interact with each other, how they are embedded in organisational infrastructure, and how they shape and are shaped by risk culture and self-control. By integrating conceptual synthesis, qualitative analysis, and quantitative evidence, the dissertation provides a multi-layered interpretation of how management control systems generate management control problems and how these problems relate to operational risk in banking.

6.4 Limitations and future research avenues

The limitations of the dissertation were discussed in depth throughout individual chapters. Below, we elaborate on those most relevant for interpreting the overall contribution of the dissertation and highlight future research opportunities emerging from them.

The primary limitation relates to the structure and timing of the research phases. The design of the quantitative instrument was completed before the full qualitative analysis was finalised. Although the survey was theoretically grounded and based on validated constructs from the relevant literature, several mechanisms identified later based on interviews were not fully incorporated. In particular, these included factors related to capability constraints, contextual misfit, and role pressures. Future research could thus investigate their role also quantitatively.

Another limitation concerns the single-organisational setting of the empirical work. The qualitative analysis was conducted in a single banking institution, which enabled an in-depth examination of how management control problems materialise in everyday organisational practice. However, the mechanisms identified, such as rigid procedural enforcement, incentive contradictions, capability gaps and cultural inconsistencies, may manifest differently in banks with different ownership structures, strategic orientations, or regulatory pressures. Future research should examine multiple banking organisations to compare whether structural mechanisms and behavioural manifestations differ under alternative institutional settings, as also encouraged by prior research that highlights organisational differences in risk implementation and governance (Mikes, 2009; Power, 2007).

A further limitation concerns the cross-sectional design of the quantitative study, which restricts the ability to infer causality between management controls and people-risk behaviours. The quantitative study relies on cross-sectional, self-reported data, which constrains causal claims and may be affected by response biases; procedural and statistical checks for common method bias are reported in Chapter 5. Although behavioural outcomes were statistically associated with variations in tight controls, self-regulation and risk culture, cross-sectional data cannot establish temporal ordering. Longitudinal designs that track changes in control systems alongside behavioural indicators and internal loss data would deepen our understanding of how behavioural risk precursors evolve and how risk outcomes materialise over time. Such designs would further contribute to expanding the understanding of dynamic control environments (Merchant & Van der Stede, 2017).

The dissertation focuses on a selected set of operationalized constructs, tight results and action controls, risk culture, interactive use of risk management and self-control. While other factors empirically surfaced, they were not statistically modelled. Issues such as ethical climate, leadership behaviour, procedural fairness and perceived organisational support emerged in interview data yet could not be incorporated into the tested model due to scope and time constraints. As these findings resonate with prior work recognising leadership tone, ethical reinforcement, and communication quality as influential in shaping control compliance and deviance (Kaptein, 2011; Weaver et al., 1999), future research should expand the tested behavioural model by integrating these organisational variables and examine their interactions with control systems.

The dissertation is situated within a specific banking and regulatory context. Risk behaviour is influenced by national institutional expectations, cultural norms regarding supervision and compliance, and local interpretations of regulatory obligations. While Basel II/III frameworks provide conceptual comparability across countries, implementation practices differ. Future research would benefit from cross-country studies examining whether structural vulnerabilities, rigidity of procedural practices or incentive tensions differ under varying regulatory regimes or cultural environments.

Finally, a limitation relates to the temporal and technological context of the study. The case bank represents a mature institutional setting with established operational processes and formalised control structures. However, the organisational context in which management control systems operate is evolving rapidly due to digitalisation, centralisation, and the increasing use of algorithmic and AI-enabled forms of control. These developments may influence how the dissertation's findings should be interpreted in future settings. As banking activities become more system-dependent and more tightly integrated across digital platforms, some traditional branch-level roles and discretionary functions may shift toward central units, automated workflows, and model-based decision processes (Boot et al., 2021; Vives, 2019). At the same time, digitalisation and AI do not eliminate the relevance of management control problems; rather, they may reconfigure how such problems emerge. For instance, action controls may increasingly be embedded in automated procedures and system-enforced workflows, while results controls may become more data-driven and continuously monitored. These developments may reduce certain forms of manual error and information-processing constraints, but they may also introduce new vulnerabilities related to overreliance on automated outputs, data quality, model opacity, system rigidity, and reduced local judgement (Crisanto et al., 2024; Financial Stability Board, 2024; Leitner et al., 2024).

However, the literature does not support the view that digitalisation and AI eliminate the role of branch networks or human judgement. Marinč (2013) shows that internet delivery channels can reduce the availability of soft information typically generated through direct interaction at bank branches, while also discussing evidence that internet banking may complement rather than substitute for branch networks. Jakšič and Marinč (2019) argue that relationship banking remains relevant despite technological change because it relies on soft information and continues to require flexibility, discretion, and trust. Their analysis also suggests that, although IT increases efficiency in transaction banking, human bankers continue to play an important role in activities where soft information, judgement, and relationship-specific knowledge remain important. As a result, the role of branch managers is not eliminated but reconfigured, with some routine and standardised decisions becoming more centralised, while local discretion remains important in relationship-based contexts.

These developments matter for the interpretation of the findings of this dissertation in several ways. First, digitalisation changes where banking work is performed: in some activities, branch-based interaction may be reduced, while remote channels, centralised processes, and digital platforms become more important (Boot et al., 2021; Vives, 2019). Second, it changes how control operates: data analytics, automated workflows, and centralised monitoring may strengthen consistency and oversight, but they may also create new blind spots and coordination risks. More recent AI applications make this point even sharper. On the one hand, AI may be used in an analytical or decision-support role, for example, to process large volumes of information, support fraud detection, assist compliance, enhance risk monitoring, and summarise complex data for managerial review (Financial Stability Board, 2024; Leitner et al., 2024). On the other hand, AI may also be embedded more directly in operational or

decision processes, such as credit assessment, customer-facing interactions, or workflow automation, thereby shifting parts of judgement and execution from local managers to models, systems, and central infrastructures (Crisanto et al., 2024; Leitner et al., 2024). This may strengthen standardisation and speed, but it also raises concerns about model risk, data quality, explainability, third-party dependence, overreliance on automated outputs, and incident-related losses when AI systems malfunction or generate harmful outcomes (Crisanto et al., 2024; Durongkadej et al., 2024; Financial Stability Board, 2024; Leitner et al., 2024).

Third, it changes where operational knowledge and discretion are located within the organisation: as some traditional branch-level decision functions shift toward systems and central units, operational risk may increasingly depend on technology governance, third-party dependencies, data quality, model-based decision processes, and the resilience of critical infrastructure. This interpretation is consistent with recent evidence suggesting that technological innovation can increase operational risk in banks by introducing technical complexity, increasing the likelihood of technical malfunctions, and creating misalignment between staff capabilities and advanced system demands (Hu et al., 2024). These developments are also consistent with broader evidence on digital disruption in banking, which highlights increasing reliance on digital platforms, more extensive use of hard information, and reduced in-person interaction (Boot et al., 2021; Vives, 2019). In this respect, Berger and Boot's (2024) emphasis on digital competition and on preserving the distinct value of financial intermediation is directly relevant, because it suggests that technological change may alter the form of intermediation without eliminating the need for effective organisational control and risk governance.

Therefore, these developments do not reduce the relevance of this dissertation; rather, they reinforce its continuing relevance while shifting the organisational context in which management control problems arise. The core issues identified in this study, such as the alignment of behaviour, the functioning of control arrangements, and the possibility that control weaknesses materialise as operational risk remain important in increasingly digital banking environments. What changes is the form through which these issues emerge. Design-related problems may become more consequential as banking becomes more dependent on integrated systems, automated routines, and centralised control architectures, because weaknesses in system design, data governance, model configuration, or escalation structures can affect larger parts of the organisation simultaneously.

At the same time, use-related issues also remain important. If AI and digital tools reduce some information-processing burdens, speed up the synthesis of large volumes of quantitative and textual information, and make exception patterns more visible, management control systems may be used more continuously, more interactively, and with greater reliance on system-generated signals than in more traditional settings (Financial Stability Board, 2024; Leitner et al., 2024). This may reduce some of the time and managerial attention required to review complex control information and allow managers to engage

more frequently with operational signals, emerging exceptions, and cross-unit patterns that would otherwise be difficult to process manually (Financial Stability Board, 2024; Leitner et al., 2024). Yet such developments do not remove the need for managerial judgement; instead, they shift it toward interpreting, challenging, and governing model outputs, exceptions, and system-generated alerts. In this respect, use problems may increasingly take the form of overreliance on automated outputs, insufficient critical challenge, weak cross-functional understanding, or limited capacity to question model-based recommendations (Crisanto et al., 2024; Financial Stability Board, 2024; Leitner et al., 2024). Behavioural and cultural problems therefore remain relevant even in more technology-intensive settings, particularly where discretion, customer interaction, exception handling, and escalation continue to matter. Future research could examine more directly how the balance between centralised, technology-enabled controls and decentralised, judgement-based practices evolves, and how this reshapes the behavioural mechanisms linking management control systems to operational risk identified in this dissertation.

6.5 Theoretical contributions

The dissertation makes several contributions to theory at the intersection of management control systems and operational risk.

First, we advance understanding of control problems by systematically mapping how result, action, personnel, and cultural controls, as well as their combinations and design–use patterns, are associated with distinct categories of dysfunctional behaviour (Franco-Santos et al., 2012; Fiolleau et al., 2018; Merchant & Van der Stede, 2017; Van Camp & Braet, 2016). This dissertation is the first study to apply the full management control system classification proposed by Merchant and Van der Stede to a banking context, where this framework has not previously been operationalised to explain behavioural consequences of controls. By doing so, we extend its relevance beyond theoretical classification and demonstrate how different control types produce systematic behavioural vulnerabilities within a regulated financial organisation. The mechanism-based framework we developed moves beyond descriptive cataloguing of unintended consequences and explains why particular control types tend to fail under specific contextual conditions, particularly when design characteristics and enacted use diverge.

This study integrates management control theory with operational risk research by demonstrating how structural weaknesses, rigid rules, incentive misalignments, cultural and ethical drift, and design–use misalignment operate as pathways through which control systems generate risk exposures that align with Basel II/III classifications (Basel Committee, 2003, 2006, 2011; Mikes, 2009; Müller et al., 2025; Li & Evans, 2022; Power, 2007). This dissertation clarifies that these pathways are not isolated consequences but represent systematic transformation mechanisms through which management control problems translate into risk-relevant outcomes. The distinction between Design-Driven Control

Problems and Human-Capability & Behavioural Control Problems provides a structured lens for understanding how design choices and human factors jointly shape operational risk.

We also contribute a behavioural perspective on people-risk by linking tight controls, risk culture, and self-control to three distinct patterns of risky behaviour: slips and lapses, routine violations, and exceptional violations (Dürst & Kunz, 2025; Shakerian et al., 2019; Tangney et al., 2018). The findings show that self-control constitutes the primary regulatory mechanism that reduces the frequency of these behaviours, while risk culture influences risk-related conduct predominantly through its effect on self-control. This relationship advances behavioural theorisation of control effectiveness in high-risk organisational settings, as it demonstrates that risk-related behaviour does not merely reflect exposure to controls, but depends on the internal self-regulatory capacity that employees mobilise when responding to control requirements. This dissertation deepens theoretical understanding of how management control systems generate behavioural vulnerabilities that influence operational risk in banking, and it offers concepts and mechanisms that can be used in future empirical and conceptual work.

6.6 Implications for practice

The findings from this PhD research have several implications for practice. For banks, the results indicate that tightening controls alone is insufficient to strengthen operational reliability. Introducing additional rules, increasing supervisory oversight, or raising performance standards may reduce certain forms of risk (such as slips or isolated violations), but they can also intensify pressure, encourage workarounds, and contribute to routine violations if not supported by a strong risk culture and realistic resource conditions. Therefore, efforts to enhance operational risk management must address the underlying sources of control problems, rather than intensifying control architecture in isolation.

More broadly, in complex organisational systems, control is inherently bounded, and unintended consequences are not merely possible but often unavoidable. A key managerial question, therefore, is how to balance intended and unintended consequences of control. In particular, it becomes important to distinguish when unintended consequences can be tolerated and when they must be actively managed. Where such outcomes do not materially compromise the underlying objective of control, they may be acceptable (for example, minor forms of symbolic compliance in non-critical tasks). However, when unintended consequences undermine core organisational goals, such as ethical conduct, financial integrity, or safety, they require deliberate and strategic mitigation. Drawing on risk management logic, dysfunctional control outcomes can be treated as behavioural risks that should be anticipated, monitored, and mitigated rather than assumed to be fully preventable. In line with this view, and consistent with the broader aim of risk management, which seeks not to eliminate risk but to manage it within acceptable bounds (Power, 2007), management control systems should be designed and used in ways that anticipate, monitor, and mitigate

dysfunctional outcomes. This implies that banks should not only strengthen formal controls but also develop mechanisms for detecting early signs of symbolic compliance, workarounds, routine violations, and other behavioural responses that may indicate growing operational vulnerability. In practice, this requires identifying early signals of such behaviours and intervening when their frequency or severity exceeds acceptable thresholds.

More concretely, the findings suggest that banks should translate these principles into specific managerial initiatives in the areas of control design, incentives, capability development, behavioural monitoring, and risk governance. Management should therefore:

– **redesign result controls and incentive systems to include explicit risk-adjusted and behavioural criteria**. Performance evaluation and bonus systems should not rely exclusively on output or target achievement, especially where strong pressure may encourage gaming, shortcuts, or procedural circumvention (Merchant & Van der Stede, 2017; Hopwood, 1972). In practice, this may involve lowering excessively steep bonus thresholds, integrating risk-management quality indicators into appraisal systems, including KPIs related to timely and appropriate escalation of issues, adherence to key controls, near-miss reporting, and cross-functional cooperation, and withholding variable pay where risky behaviour, serious rule circumvention, or concealment occurs even if financial or operational targets are met;

– **review action controls and procedures for behavioural fit, not only formal compliance.** Rules, checklists, and procedural requirements should be reviewed regularly to identify where they create unnecessary bottlenecks, contradictory demands, duplication, or workarounds. In areas where legal or prudential requirements allow, procedures should function as enabling guides rather than purely coercive constraints (Adler & Borys, 1996; Ahrens & Chapman, 2006). Practical initiatives may include periodic rule-review workshops, structured feedback from frontline employees, exception logs, and escalation routines for procedures that are repeatedly bypassed because they are experienced as impractical or overly rigid;

– **strengthen socio-technical control reliability by reducing manual workarounds and improving system integration**. The qualitative findings show that operational vulnerabilities often emerge not only from poor rules, but from fragmented systems, incomplete automation, vendor dependencies, and organisational growth that outpaces system capacity. Banks should therefore invest in cross-system integration, automated reconciliations, early-warning mechanisms, and real-time monitoring of critical operational processes. Such interventions are particularly important where operational losses are linked to execution, delivery, and process-management weaknesses (Basel Committee on Banking Supervision, 2003; Dechow & Mouritsen, 2005; Xu et al., 2022);

– **treat people-risk as behaviourally differentiated rather than uniform**. The quantitative findings suggest that slips, routine violations, and exceptional violations have different

antecedents and therefore require different managerial responses. Slips and lapses are more closely linked to attentional demands and self-control, suggesting the importance of workload management, cognitive load reduction, realistic task pacing, and supervision of error-prone routines (Reason et al., 1998; Reason, 1990, 2000). Routine violations are shaped more strongly by cultural norms and local work practices, implying a need to monitor workaround behaviour, local deviations, and "how work is really done" rather than assuming that more rules will solve the problem. Exceptional violations require attention to high-pressure situations, where employees may face tensions between procedural compliance and operational demands;

– **address human capability and capacity as core control conditions.** Banks should not assume that formal controls will function reliably if employees lack the skills, attention, time, or resources needed to enact them consistently. Practical initiatives include structured onboarding for new or rotating staff, targeted refresher training, competence assessments in key operational roles, staffing reviews in control-intensive units, and workload monitoring where attentional fatigue is likely to undermine execution quality. These measures are especially important in digitalising environments where employees must adapt to evolving systems and model-based processes (Merchant & Van der Stede, 2017; Campbell, 2012; Xu et al., 2022);

– **embed risk culture into everyday managerial practice rather than relying on generic cultural messaging.** The findings indicate that risk culture matters because it strengthens self-control and supports responsible conduct, but also because its effects vary across local organisational contexts. Banks should therefore reinforce risk culture through department-level initiatives, leadership signals, and psychologically safe reporting environments, not only through bank-wide statements of values (Financial Stability Board, 2014; Carretta et al., 2017; Kunz & Heitz, 2021). Useful practices may include discussion of near misses in team meetings, visible managerial responses to escalation, local culture reviews in branches and functions, and explicit reinforcement that raising concerns is valued rather than penalised;

– **use behavioural indicators and escalation thresholds as part of operational risk monitoring**. If dysfunctional control outcomes are treated as behavioural risks, banks need indicators that detect them early. These may include repeated overrides, repeated procedural exceptions, high volumes of rework, escalation delays, recurrent manual corrections, signs of symbolic compliance, and concentrations of routine violations in particular units. Such indicators should not be used only for punishment; they should also trigger managerial review, diagnostic discussion, and redesign of controls where necessary (Simons, 1995; Power, 2009; Marc et al., 2023);

– **strengthen cross-functional dialogue where control problems are likely to be fragmented across units.** The evidence from the qualitative and literature-review stages suggests that design–use misalignment, structural fragmentation, and incentive

contradictions are rarely contained within a single function. Banks should therefore create regular cross-functional forums involving risk, operations, compliance, audit, HR, and business units to review emerging vulnerabilities, discuss workarounds, and align control expectations (Simons, 1995; Hall et al., 2015). This is especially important where operational risk information is formally available but weakly used in managerial decision-making;

– **use interactive control selectively and purposefully**. The findings suggest that interactive use may not directly reduce all forms of everyday operational risk behaviour, but it remains valuable for surfacing emerging problems, supporting interpretation, and strengthening organisational learning. Banks should therefore use interactive control practices particularly for discussing near misses, emerging operational vulnerabilities, and cross-unit patterns, rather than assuming that more face-to-face discussion alone will eliminate slips or routine violations (Simons, 1995; Bisbe & Otley, 2004; Marc et al., 2023).

For regulators and supervisory bodies, the findings underscore that operational risk frameworks need to incorporate behavioural mechanisms more explicitly. A narrow emphasis on documentation, formal procedures, or technical compliance may reinforce design–use misalignment and ritualistic compliance practices (Power, 2009; Wahlström, 2009). Supervisory assessments that explicitly consider risk culture, behavioural responses to control demands, and interactions among multiple control systems are likely to provide a more accurate representation of the organisation's risk exposure (Financial Stability Board, 2014; Carretta et al., 2017; Kunz & Heitz, 2021). In practical terms, this suggests that supervisory review could place greater emphasis on incentive design, behavioural risk indicators, quality of escalation, repeated workaround behaviour, and the alignment between formal controls and actual work practices rather than relying primarily on the existence of documented procedures.

7 CONCLUSIONS

Banks operate under sustained pressure to achieve performance targets, comply with regulatory requirements, and maintain operational reliability. In response to these pressures, banks rely extensively on management control systems (MCS) to structure behaviour and manage performance and risk. Prior research shows that such control systems may generate unintended and dysfunctional consequences, labelled control problems, particularly when individuals experience lack of direction, motivational difficulties, or personal limitations in responding to control demands (Merchant & Van der Stede, 2017). This dissertation examines how these management control problems emerge in banking and how they shape operational risk.

By integrating systematic literature reviews, a qualitative banking case study, and a quantitative employee survey, the dissertation demonstrates that operational risk is not only a technical or regulatory construct, but also a behavioural outcome that is produced through

the design and use of management control systems. Across the three research questions, the findings show that result, action, personnel, and cultural controls can generate identifiable categories of control problems through six recurrent mechanisms: overly rigid or coercive design, misfit with values or context, crowding out of intrinsic motivation, lack of participation and autonomy, symbolic or inconsistent use of controls, and design–use misalignment (Franco-Santos et al., 2012; Fiolleau et al., 2018; Merchant & Van der Stede, 2017; Van Camp & Braet, 2016). These mechanisms explain why controls that are intended to reduce risk may simultaneously create behavioural vulnerabilities.

The dissertation further clarifies that these control problems translate into operational risk exposures that align with Basel II/III classifications (Basel Committee, 2003, 2006, 2011). Structural vulnerabilities, rule-induced constraints, incentive misalignments, workforce capability and capacity limitations, and cultural inconsistencies emerge as systematic pathways through which management control problems precede errors, violations, and ethical breaches In this sense, operational risk is shown to arise from the interaction between formal control architectures and lived organisational practices, rather than from isolated process or system failures (Power, 2005; Ringgaard, 2025; Soin & Collier, 2013; Wahlström, 2009).

The empirical findings reinforce this interpretation. The qualitative case study demonstrates how design-driven control problems and human-capability & behavioural control problems materialise in everyday banking operations, shaping how employees interpret, adapt to, or circumvent controls. The quantitative analysis complements these insights by showing that people-risk behaviours, such as slips and lapses, routine violations, and exceptional violations, are differentially influenced by tight controls, risk culture, and self-control. In particular, self-control emerges as a central behavioural mechanism reducing all categories of people-risk behaviour, while risk culture operates primarily by strengthening self-regulatory capacity rather than by directly constraining behaviour (Dürst & Kunz, 2025; Shakerian et al., 2019; Tangney et al., 2018).

In conclusion, this dissertation demonstrates that operational risk in banking does not arise solely from failures in processes, systems, or external events, but is deeply rooted in how management control systems are designed, combined, and used, and in how employees respond to them. By integrating conceptual synthesis, qualitative analysis, and quantitative evidence, the thesis shows that control problems follow identifiable mechanisms, are shaped by contextual conditions, and translate into people-risk behaviours that can precede operational loss events. Overall, the findings of this dissertation indicate that effective operational risk management requires more than robust control architecture; it depends on aligning formal systems with human capabilities, risk culture, and behavioural regulation.

REFERENCE LIST

1. Abdul Rahim, N. F., Ahmed, E. R., & Faeeq, M. K. (2018). Internal Control System and Perceived Operational Risk Management in Malaysian Conventional Banking Industry. *Global Business and Management Research, 10*(1), 135–149.
2. Abdul-Rahman, A., & Yazid, Z. (2015). Developing a framework of Islamic bank operational risk management:'people risk'. *Jurnal Pengurusan, 44*(2015), 129-139
3. Abernethy, M. A., & Stoelwinder, J. U. (1995). The role of professional control in the management of complex organizations. *Accounting, Organizations and Society, 20*(1), 1–17.
4. Abernethy, M. A., Dekker, H. C., & Schulz, A. K.-D. (2015). Are employee selection and incentive contracts complements or substitutes? *Journal of Accounting Research, 53*(4), 633–668.
5. Abubakar, N. A., Baird, K., & Su, S. (2022). The association between the interactive and diagnostic use of financial and non-financial performance measures with individual creativity: The mediating role of perceived fairness. *Journal of Management Control, 33*, 179–215.
6. Acrey, J. C., McCumber, W. R., & Nguyen, T. H. T. (2011). CEO incentives and bank risk. *Journal of Economics and Business, 63*(5), 456–471.
7. Adler, P. S., & Borys, B. (1996). Two types of bureaucracy: Enabling and coercive. *Administrative Science Quarterly, 41*(1), 61–89.
8. Adnan, A. A., Jamil, C. Z. M., & Nor, M. I. (2013). Ethical antecedents of dysfunctional behaviour in performance measurement and control systems. *Asian Social Science, 9*(1), 103–113.
9. Agarwal, S., & Ramaswami, S. N. (1993). Marketing controls and employee responses: The moderating role of Task Characteristics. *Journal of the Academy of Marketing Science, 21*(4), 293–306.
10. Ahrens, T., & Chapman, C. S. (2006). Doing qualitative field research in management accounting: Positioning data to contribute to theory. *Accounting, Organizations and Society*, *31*(8), 819–841.
11. Al-Amri, K., & Davydov, Y. (2016). Testing the Effectiveness of ERM: Evidence from Operational Losses. *Journal of Economics and Business, 87*, 70–82.
12. 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.
13. Anderson, E., & Oliver, R. L. (1987). Perspectives on behavior-based versus outcome-based salesforce control systems. *Journal of Marketing, 51*(4), 76–88.
14. Anthony, R. N. (1965). *Planning and control systems: A framework for analysis*. Harvard University, Division of Research, Graduate School of Business Administration.
15. Anthony, R. N., & Govindarajan, V. (2007). *Management control systems* (12th ed.). McGraw-Hill.
16. Appelbaum, S. H., & Shapiro, B. T. (2006). Diagnosis and remedies for deviant workplace behaviors. *Journal of American Academy of Business, 9*(2), 14–20.
17. Arena, M., & Arnaboldi, M. (2014). Risk and performance management: Are they easy partners? *Management Research Review, 37*(2), 152-166.
18. Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of enterprise risk management. *Accounting, Organizations and Society*, *35*(7), 659-675.

19. Ashraf, B. N., Zheng, C., & Arshad, S. (2016). Effects of National Culture on Bank Risk-Taking Behavior. *Research in International Business and Finance*, *37*, 309–326.
20. Baliga, B. R., & Jaeger, A. M. (1984). Multinational corporations: Control systems and delegation issues. *Journal of International Business Studies, 15*(2), 25–40.
21. Balstad, M. T., & Berg, T. (2020). A long-term bibliometric analysis of journals influencing management accounting and control research. *Journal of Management Control, 30*, 357–380.
22. Balzano, M. (2022). Serendipity in management studies: a literature review and future research directions. *Management Decision, 60*(13): 130–152.
23. Bardoscia, M., & Bellotti, R. (2012). A Dynamical Approach to Operational Risk Measurement.
24. Barth, J. R., Caprio, G., Jr., & Levine, R. (2004). Bank regulation and supervision: What works best? Journal of Financial Intermediation, 13(2), 205–248.
25. Basel Committee on Banking Supervision (2006). *International Convergence on Capital Measurement and Capital Standards (A revised framework, comprehensive version)*. Retrieved from http://www.bis.org/publ/bcbs128.pdf .
26. Basel Committee on Banking Supervision. (1998). *Framework for Internal Control Systems in Banking Organisations*. Basel: BIS.
27. Basel Committee on Banking Supervision. (2003). *Sound practices for the management and supervision of operational risk*. Bank for International Settlements.
28. Basel Committee on Banking Supervision. (2006). *International convergence of capital measurement and capital standards: A revised framework (Comprehensive version)*. Bank for International Settlements.
29. Basel Committee on Banking Supervision. (2011). *Basel III: A global regulatory framework for more resilient banks and banking systems*. Bank for International Settlements.
30. Baumeister, R. F., Schmeichel, B. J., & Vohs, K. D. (2007). Self-regulation and the executive function: The self as controlling agent. *Social psychology*: *Handbook of basic principles, 2*, 516-539.
31. Becker, S., & Green, D. Jr. (1962). Budgeting and employee behavior. *The Journal of Business, 35*(4), 392–402.
32. Bedford, D. S. (2020). Conceptual and empirical issues in understanding management control combinations. *Accounting, Organizations and Society, 86*, 101187.
33. Bellora-Bienengräber, L., Radtke, R. R., & Widener, S. K. (2022). Counterproductive work behaviors and work climate: The role of an ethically focused management control system and peers' self-focused behavior. *Accounting, Organizations and Society, 96*, 101275.
34. Berger, A. N., Curti, F., Mihov, A., & Sedunov, J. (2022). Operational Risk Is More Systemic Than You Think: Evidence from U.S. Bank Holding Companies. *Journal of Banking & Finance, 149*, 106730.
35. Berger, Allen N., Arnoud W.A. Boot (2024), Financial intermediation services and competition analyses: Review and paths forward for improvement, Journal of Financial Intermediation, 57, 101072.
36. Berry, A. J., Coad, A. F., Harris, E. P., Otley, D. T., & Stringer, C. (2009). Emerging themes in management control: A review of recent literature. *The British Accounting Review, 41*(1), 2–20.
37. Bhattacharya, S., & Thakor, A. V. (1993). Contemporary banking theory. Journal of Financial Intermediation, 3(1), 2–50.

38. Bieńkowska, A., & Tworek, K. (2020). Job performance model based on Employees' Dynamic Capabilities (EDC). *Sustainability, 12*(6), 2250.
39. Bisbe, J., and D. Otley. 2004. The Effects of the Interactive Use of Management Control Systems on Product Innovation. *Accounting, Organizations and Society 29* (8): 709–737.
40. Block, J., Brändle, L., Limbach, P., Röth, T., & Sabel, C. A. (2025). Half dead or more alive than ever? New, old, and (increasingly) redundant literature review formats. *Management Review Quarterly, 75*, 993–1008.
41. Bonner, S. E., Hesford, J. W., Van der Stede, W. A., & Young, S. M. (2006). The most influential journals in academic accounting. *Accounting, Organizations and Society, 31*(7), 663–685.
42. Boot, A. W. A., Hoffmann, P., Laeven, L., & Ratnovski, L. (2021). Fintech: What's old, what's new? *Journal of Financial Stability, 53*, 100836.
43. Bourmistrov, A., & Kaarbøe, K. (2013). From comfort to stretch zones: A field study of two multinational companies applying "beyond budgeting" ideas. *Management Accounting Research, 24*(3), 196–211.
44. Braumann, E. C., Grabner, I., & Posch, A. (2020). Tone from the top in risk management: A complementarity perspective on how control systems influence risk awareness. *Accounting, Organizations and Society, 84*, 101128.
45. Braumann, E., Hiebl, M. R. W., & Posch, A. (2024). Enterprise risk management as part of the organizational control package: Review and implications for management accounting research. *Journal of Management Accounting Research, 36*(2), 7–29.
46. Bromwich, M., & Scapens, R. W. (2016). Management accounting research: 25 years on. *Management Accounting Research, 31*, 1–9.
47. Brownell, P., & Hirst, M. (1986). Reliance on accounting information, budgetary participation, and task uncertainty: Tests of a three-way interaction. *Journal of Accounting Research, 24*(2), 241–249.
48. Burns, J., & Scapens, R. W. (2000). Conceptualizing management accounting change: An institutional framework. *Management Accounting Research, 11*(1), 3–25.
49. Butler, T., & Brooks, R. (2024). Time for a paradigm change: Problems with the financial industry's approach to operational risk. Risk Analysis, 44(6), 1285–1304.*
50. Campbell, D. (2012). Employee selection as a control system. *Journal of Accounting Research, 50*(4), 931–966.
51. Carpenter, N. C., Whitman, D. S., & Amrhein, R. (2021). Unit-level counterproductive work behavior (CWB): A conceptual review and quantitative summary. *Journal of management, 47*(6), 1498-1527.
52. Carretta, A., Farina, V., & Schwizer, P. (2017). Risk culture and banking supervision. *Journal of Financial Regulation and Compliance, 25*(2), 209–226.
53. Carretta, A., Fiordelisi, F., Schwizer, P., & Stentella Lopes, F. (2024). Errors and Misbehaviors in Banking and Finance: A Systematic Literature Review. *Journal of Economic Behavior & Organization, 222*, 117–140.
54. Carroll, E., & Marginson, D. (2021). Relative performance information and social comparisons: Exploring managers' cognitive, emotional and dysfunctional behavioral processes. *Management Accounting Research, 53*, 100768.
55. Cerasi, V., & Oliviero, T. (2015). CEO Compensation, Regulation, and Risk in Banks: Theory and Evidence from the Financial Crisis. *International Journal of Central Banking, 11*(3), 241–302.

56. Chanon, R. D., Habahbeh, L., Klumpes, P. J. M., & Mann, S. (2025). Operational Resilience in the UK Financial Sector: Practical Guidance. *British Actuarial Journal, 30*(e25), 1–36.
57. Chapelle, A., Crama, Y., Hubner, G., & Peters, J. P. (2004). *Basel II and Operational Risk: Implications for risk measurement and management in the financial sector* (No. 51). NBB working paper.
58. Charmaz, K. (2014). Constructing Grounded Theory (2nd Ed.). London: SAGE Publications.
59. Cheng, M. M., & Coyte, R. (2014). The effects of incentive subjectivity and strategy communication on knowledge-sharing and extra-role behaviours. *Management Accounting Research, 25*(2), 119–130.
60. Chenhall, R. H. (2003). Management control systems design within its organizational context: Findings from contingency-based research and directions for the future. *Accounting, Organizations and Society, 28*(2–3), 127–168. *
61. Chernobai, A., Ozdagli, A., & Wang, J. (2020). Business Complexity and Risk Management: Evidence from Operational Risk Events in U.S. Bank Holding Companies. *Journal of Finance, 75*(5), 2579–2627.
62. Christ, M. H., Emett, S. A., Summers, S. L., & Wood, D. A. (2012). The effects of preventive and detective controls on employee performance and motivation. *Contemporary Accounting Research, 29*(2), 432–452.
63. Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Lawrence Erlbaum Associates.
64. Cohn, A., Fehr, E., & Maréchal, M. A. (2014). Business culture and dishonesty in the banking industry. *Nature, 516*(7529), 86–89.
65. Collier, P., Berry, A. J., & Burke, G. T. (2007). *Risk and management accounting: Best practice guidelines for enterprise-wide internal control procedures*. CIMA Publishing.
66. Cornalba, C., & Giudici, P. (2004). Statistical models for operational risk management. *Physica A: Statistical Mechanics and Its Applications, 338*(1-2), 166-172.
67. Cornwell, N., Bilson, C., Gepp, A., Stern, S., & Vanstone, B. J. (2023). Modernising operational risk management in financial institutions via data-driven causal factors analysis: A pre-registered report. *Pacific-Basin Finance Journal, 77*, 101906.
68. Cravens, D. W., Ingram, T. N., LaForge, R. W., & Young, C. E. (1993). Behavior-based and outcome-based salesforce control systems. *Journal of Marketing, 57*(4), 47–59.
69. Cravens, D. W., Lassk, F. G., Low, G. S., Marshall, G. W., & Moncrief, W. C. (2004). Formal and informal management control combinations in sales organizations: The impact on salesperson consequences. *Journal of Business Research, 57*(3), 241–248.
70. Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches (4th ed.). Sage.
71. Crisanto, J. C., Leuterio, C. B., Prenio, J., & Yong, J. (2024). *Regulating AI in the financial sector: Recent developments and main challenges* (FSI Insights on policy implementation No. 63). Bank for International Settlements.
72. Cruz, M. (2002). *Modeling, measuring and hedging operational risk*. Chichester: John Wiley & Sons.
73. Cruz, M., Coleman, R., & Salkin, G. (1998). Modeling and measuring operational risk. *The Journal of Risk, 1*(1), 63-72.

74. Cugueró-Escofet, N., & Rosanas, J. M. (2017). The ethics of metrics: Overcoming the dysfunctional effects of performance measurements through justice. *Journal of Business Ethics, 140*(4), 615–631.
75. Czarniawska, B. (2014). Social science research: From field to desk. SAGE.
76. Daley, L. A., Jiambalvo, J., Sundem, G. L., & Kondo, Y. (1985). Attitudes toward financial control systems in the United States and Japan. *Journal of International Business Studies, 16*(2), 91–106.
77. Davila, T. (2000). An empirical study on the drivers of management control systems' design in new product development. *Accounting, Organizations and Society*, 25(4–5), 383–409.
78. De Baerdemaeker, J., & Bruggeman, W. (2015). The impact of participation in strategic planning on managers' creation of budgetary slack: The mediating role of autonomous motivation and affective organizational commitment. *Management Accounting Research*, 29, 1–12.
79. De Ridder, D. T., Lensvelt-Mulders, G., Finkenauer, C., Stok, F. M., & Baumeister, R. F. (2012). Taking stock of self-control: A meta-analysis of how trait self-control relates to a wide range of behaviors. *Personality and social psychology review, 16*(1), 76-99.
80. De Vaus, D. (2001). Research design in social research. SAGE
81. de Waal, A. A., & Coevert, V. (2007). The effect of performance management on the organizational results of a bank. *International Journal of Productivity and Performance Management, 56*(5/6), 397-416.
82. Dechow, N., & Mouritsen, J. (2005). Enterprise resource planning systems, management control and the quest for integration. *Accounting, Organizations and Society, 30*(7–8), 691–733.
83. Denyer, D., & Tranfield, D. (2009). Producing a systematic review. In D. A. Buchanan &A. Bryman (Eds.), The Sage handbook of organizational research methods (pp. 671–689). Sage Publication.
84. Deore, A., Gallani, S., & Krishnan, R. (2023). The effect of systems of management controls on honesty in managerial reporting. *Accounting, Organizations and Society, 107*, 101471.
85. Deschamps, C. (2019). Stages of management control in a large public organization: From top to frontline managers. *Journal of Management Control, 30*(2), 153–184.
86. Di Antonio, M. (2017). Risk culture in different bank businesses. In Risk culture in Banking (pp. 31-71). Cham: Springer International Publishing.
87. Diamond, D. W. (1984). Financial intermediation and delegated monitoring. The Review of Economic Studies, 51(3), 393–414.
88. Diamond, D. W., & Dybvig, P. H. (1983). Bank runs, deposit insurance, and liquidity. Journal of Political Economy, 91(3), 401–419.
89. Duarte, H., Palermo, O. A., & Arriaga, P. (2018). The role of emotions in the control-resistance dyad. *Scandinavian Journal of management*, *34*(1), 91-102.
90. Duckworth, A. L., Milkman, K. L., & Laibson, D. (2018). Beyond willpower: Strategies for reducing failures of self-control. *Psychological Science in the Public Interest, 19*(3), 102-129.
91. Dunk, A. S. (1993). The effect of budget emphasis and information asymmetry on the relation between budgetary participation and slack. *The Accounting Review*, *68*(2), 400–410.
92. Durongkadej, I., Hu, W., & Wang, H. E. (2024). How artificial intelligence incidents affect banks and financial services firms? A study of five firms. *Finance Research Letters, 70*, 106279.

93. Dürst, N., & Kunz, J. (2025). The Risk Culture Scale: A Measurement Tool to Comprehensively Assess Banks' Risk Culture. *Abacus.*
94. Edwards, J., & Wolfe, S. (2004). The Compliance Function in Banks. *Journal of Financial Regulation and Compliance, 12*(3), 216–224.
95. Eisenhardt, K. M. (1985). Control: Organizational and economic approaches. *Management Science*, 31(2), 134–149.
96. Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review, 14*(4), 532–550.
97. Elmassri, M., & Harris, E. (2011). Rethinking budgetary slack as budget risk management. *Journal of Applied Accounting Research*, *12*(3), 278–293.
98. European Banking Authority (2023). Operational Risks and Resilience Report 2023. EBA, Paris. Available at https://www.eba.europa.eu/publications-and-media/publications/operational-risks-and-resilience-0
99. Fakhri, G., Menacere, K., & Pegum, R. (2010). Organizational Specificities That Affect The Use Of Corporate Performance Measurements Process In The Banking Sector. *Journal of Performance Management, 23*(3).
100. Faugère, C., & Stul, O. (2021). Harmful events and misconducts in financial organizations: Human biases and root causes. *Research in International Business and Finance,* 56, 101382.
101. Feldman, M. S., & Pentland, B. T. (2003). Reconceptualizing organizational routines as a source of flexibility and change. *Administrative Science Quarterly, 48*(1), 94–118.
102. 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.
103. Ferreira, S., & Dickason-Koekemoer, Z. (2019). A conceptual model of operational risk events in the banking sector. *Cogent Economics & Finance, 7*(1).
104. Financial Stability Board (2014). *Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture*. Basel: FSB.
105. Financial Stability Board. (2024). *The financial stability implications of artificial intelligence*. Financial Stability Board.
106. Fiolleau, K., Libby, T., & Thorne, L. (2018). Dysfunctional behavior in organizations: Insights from the management control literature. Auditing: A Journal of Practice & Theory, 37(4), 117–141.
107. Flick, U. (2018). The SAGE handbook of qualitative data collection. SAGE.
108. Florio, C., & Leoni, G. (2017). Enterprise Risk Management and Firm Performance: The Italian Case. *The British Accounting Review, 49*(1), 56–74.
109. Fontnouvelle, P. D., Jordan, J., & Rosengren, E. (2005). *Implications of Alternative Operational Risk Modeling Techniques*. Working Papers 04-9, Federal Reserve Bank of Boston.
110. Ford, J. D., Ford, L. W., & D'amelio, A. (2008). Resistance to change: The rest of the story. *Academy of management Review, 33*(2), 362-377.
111. Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50.
112. Franco-Santos, M., & Otley, D. (2018). Reviewing and theorizing the unintended consequences of performance management systems. *International Journal of Management Reviews*, *20*(3), 696–730.

113. Franco-Santos, M., Lucianetti, L., & Bourne, M. (2012). Contemporary performance measurement systems: A review of their consequences and a framework for future research. *Management Accounting Research*, *23*(2), 79–119.
114. Frese, M., & Keith, N. (2015). Action Errors, Error Management, and Learning in Organizations. *Annual Review of Psychology, 66*, 661–687.
115. Frigo, M. L., & Anderson, R. J. (2014). Risk management frameworks: adapt, don't adopt: here's a primer on how to use two well-known approaches. *Strategic Finance, 95*(7), 49-54.
116. Gehman, J., Glaser, V. L., Eisenhardt, K. M., Gioia, D. A., Langley, A., & Corley, K. G. (2018). Finding theory–method fit: A comparison of three qualitative approaches to theory building. *Journal of Management Inquiry, 27*(3), 284–300
117. Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. *Organizational research methods, 16*(1), 15-31.
118. Glaser, B. G. (2001). *The Grounded Theory Perspective Conceptualization Contrasted with Description*. Mill Valley, CA Sociology Press.
119. Gneezy, U., Meier, S., & Rey-Biel, P. (2011). When and why incentives (don't) work to modify behavior. *Journal of Economic Perspectives*, *25*(4), 191–210.
120. Goebel, S., & Weißenberger, B. E. (2016). The dark side of tight financial control: Causes and remedies of dysfunctional employee behaviors. *Schmalenbach Business Review*, 17, 69–101.
121. Goebel, S., & Weißenberger, B. E. (2017). The relationship between informal controls, ethical work climates, and organizational performance. *Journal of Business Ethics*, 141(3), 505–528.
122. Gontarek, W. (2016). Risk Governance of Financial Institutions: The Growing Importance of Risk Appetite and Culture. *Journal of Risk Management in Financial Institutions, 9*(2), 120–129.
123. Gooneratne, T. N., & Hoque, Z. (2013). Management control research in the banking sector: A critical review and directions for future research. *Qualitative Research in Accounting & Management, 10*(2), 144-171.
124. Göstl, P., & Schwaiger, W. S. A. (2016). *Risk-Based Planning and Control Systems: Integration of Different Risk Types into Strategic, Financial, and Operational Management Systems*. Vienna University of Technology.
125. Greenbaum S, Thakor A., Boot, A.W.A., 2019. Contemporary Financial Intermediation. New York: Elsevier. 4th ed.
126. Grieser, F., & Pedell, B. (2022). Exploring risk culture controls: to what extent can the development of organizational risk culture be controlled and how?. *Journal of Accounting & Organizational Change, 18*(5), 752-788.
127. Grizzle, G. A. (2002). Performance measurement and dysfunction: The dark side of quantifying work. *Public Performance & Management Review*, 25(4), 363–369.
128. Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Field Methods, 18*(1), 59–82.
129. Gurd, B., & Helliar, C. (2017). Looking for leaders: 'Balancing' innovation, risk and management control systems. *The British Accounting Review, 49*(1), 91–102.
130. Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). A primer on partial least squares structural equation modeling (PLS-SEM) (3rd ed.). Sage.
131. Hale, A., & Borys, D. (2013). Working to rule, or working safely? Part 1: A state of the art review. Safety science, 55, 207-221.

132. Hall, M., Mikes, A., & Millo, Y. (2015). How do risk managers become influential? A field study of toolmaking in two financial institutions. *Management Accounting Research*, 26(3), 241–257.
133. Hansen, S. C., & Van der Stede, W. A. (2004). Multiple facets of budgeting: An exploratory analysis. *Management Accounting Research*, 15(4), 415–439.
134. Hartman, F., & Slapničar, S. (2007). Corporate Governance in Banks: Characteristics of Internal Management Control Systems in Slovenian Banks. *Research Report, University of Ljubljana*.
135. Heitger, A. A., Heitger, D. L., & Heitger, L. E. (2021). Driving performance in the retail and banking industries: The consequences of dysfunctional management control systems at W. T. Grant and Wells Fargo. *Issues in Accounting Education*, 36(2), 65–92.
136. Henri, J.-F. (2006). Organizational culture and performance measurement systems. *Accounting, Organizations and Society*, 31(1), 77–103.
137. Henseler, J., & Fassott, G. (2010). Testing moderating effects in PLS path models: An illustration of available procedures. In V. E. Vinzi, W. W. Chin, J. Henseler, & H. Wang (Eds.), Handbook of partial least squares: Concepts, methods and applications (pp. 713–735). Springer.
138. Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43*(1), 115–135.
139. Hirst, M. K. (1981). Accounting information and the evaluation of subordinate performance: A situational approach. *The Accounting Review, 56*(4), 771–784.
140. Hirst, M. K. (1983). Reliance on accounting performance measures, task uncertainty, and dysfunctional behavior: Some extensions. *Journal of Accounting Research, 21*(2), 596–605.
141. Hofmann, W. (2024). Going beyond the individual level in self-control research. *Nature Reviews Psychology*, 3(1), 56-66.
142. Hofstede, G. (1978). The poverty of management control philosophy. *Academy of Management Review, 3*(3), 450–461.
143. Hofstede, G. (1998). Identifying organizational subcultures: An empirical approach. *Journal of Management Studies, 35*(1), 1–12.
144. Holland, J. (2019). Bank top management teams, disclosure, learning, survival and failure: 1990–2017. *Qualitative Research in Financial Markets, 11*(1), 31–59.
145. Hopwood, A. G. (1972). An empirical study of the role of accounting data in performance evaluation. *Journal of Accounting Research, 10*(Empirical Research in Accounting: Selected Studies), 156–182.
146. Houston, J. F., & James, C. (1995). CEO Compensation and Bank Risk. *Journal of Monetary Economics, 36*(2), 405–431.
147. Hu, M., Zhang, Y., Feng, X., & Xiong, X. (2024). How technological innovation influence operational risk: Evidence from banks in China. *International Review of Financial Analysis, 95*, 103480.
148. Huang, J. C., Newell, S., & Galliers, R. D. (2002). The impact of organizational sub cultures on the implementation of component based development: A case study of an international investment bank. ECIS 2002 Proceedings, 66.
149. Hunton, J. E., Mauldin, E. G., & Wheeler, P. R. (2008). Potential functional and dysfunctional effects of continuous monitoring. *The Accounting Review, 83*(6), 1551–1569.
150. Hussain, M. (2005). Management accounting performance measurement systems in Swedish banks. *European Business Review, 17*(6), 566-589.

151. Hussain, M. M., & Gunasekaran, A. (2002). Non-financial management accounting measures in Finnish financial institutions. *European Business Review, 14*(3), 210–229.
152. Institute of Risk Management [IRM] (2012). *Risk culture. Under the microscope*. *Guidance for boards.*
153. Jacobs, G., Belschak, F. D., & Den Hartog, D. N. (2013). (Un)ethical behavior and performance appraisal: The role of affect, support, and organizational justice. *Journal of Business Ethics, 117*(3), 667–681.
154. Jakšič, M., & Marinč, M. (2019). Relationship banking and information technology: The role of artificial intelligence and FinTech. Risk Management, 21(1), 1–18.
155. Jaworski, B. J. (1988). Toward a theory of marketing control: Environmental context, control types, and consequences. *Journal of Marketing, 52*(3), 23–39.
156. Jensen, M. C. (2003). Paying people to lie: The truth about the budgeting process. *European Financial Management, 9*(3), 379–406.
157. Jermier, J. M., Slocum, J. W., Fry, L. W., & Gaines, J. (1991). Organizational subcultures in a soft bureaucracy: Resistance behind the myth and façade of an official culture. *Organization Science, 2*(2), 170–194.
158. Jia, J. S., Khan, U., & Litt, A. (2015). The effect of self-control on the construction of risk perceptions. *Management Science, 61*(9), 2259-2280.
159. Johnson, R. E., Lin, S. H., & Lee, H. W. (2018). Self-control as the fuel for effective self-regulation at work: Antecedents, consequences, and boundary conditions of employee self-control. *In Advances in motivation science* (Vol. 5, pp. 87-128). Elsevier.
160. Jurkiewicz, C. L., & Giacalone, R. A. (2014). Organizational determinants of ethical dysfunctionality. *Journal of Business Ethics, 120*(1), 1–17.
161. Kaplan, R. S., & Mikes, A. (2020). Managing risks: a new framework. Harvard Business Review Press.
162. Kaptein, M. (2011). From inaction to external whistleblowing: The influence of the ethical culture of organizations on employee responses to observed wrongdoing. *Journal of Business Ethics, 98*, 513–530.
163. Kashyap, A. K., Rajan, R., & Stein, J. C. (2002). Banks as liquidity providers: An explanation for the coexistence of lending and deposit-taking. *Journal of Finance, 57*(1), 33–73.
164. Khajehnejad, S., & Linder, S. (2022). Why the type of information observable to peers matters: Peer monitoring and performance measure manipulation. *Management Accounting Research, 57*, 100815.
165. Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of e-Collaboration*, 11(4), 1–10.
166. Kominis, G., & Dudau, A. I. (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.
167. Kuckertz, A., & Block, J. (2021). Reviewing systematic literature reviews: Ten key questions and criteria for reviewers. *Management Review Quarterly, 71*(3), 519–524.
168. Kühn, R., & Neu, P. (2003). Functional correlation approach to operational risk in banking organizations. Physica A: Statistical Mechanics and its Applications, 322(1–4), 650–666.
169. Kunz, A. H. (2025). Management accountants' roles and management controls in hospitals at times of strain—Experiences during the Corona pandemic. *Journal of Management Control.* Advance online publication.

170. Kunz, J., & Heitz, M. (2021). Banks' risk culture and management control systems: A systematic literature review. *Journal of Management Control, 32(*4), 439–493.
171. Kvale, S., & Brinkmann, S. (2009). InterViews: Learning the craft of qualitative research interviewing (2nd ed.). SAGE.
172. Laeven, L., & Levine, R. (2009). Bank governance, regulation and risk taking. *Journal of financial economics, 93*(2), 259-275.
173. Lagios, C., Nguyen, N., Stinglhamber, F., & Caesens, G. (2023). Dysfunctional rules in organizations: The mediating role of organizational dehumanization in the relationship between red tape and employees' outcomes. *European Management Journal*, *41*(5), 802-813.
174. Laguecir, A., & Leca, B. (2022). Organized Decoupling of Management Control Systems: An Exploratory Study of Traders' Unethical Behavior. *Journal of Business Ethics, 181*(1), 153–169.
175. Langfield-Smith, K. (1997). Management control systems and strategy: A critical review. *Accounting, Organizations and Society, 22*(2), 207–232.
176. Langfield-Smith, K., & Smith, D. (2003). Management control systems and trust in outsourcing relationships. *Management Accounting Research, 14*(3), 281–307.
177. Lau, C. M., & Eggleton, I. R. C. (2004). Cultural differences in managers' propensity to create slack. *Advances in Accounting Behavioral Research, 7*, 133–153.
178. Leitner, G., Singh, J., van der Kraaij, A., & Zsámboki, B. (2024). The rise of artificial intelligence: Benefits and risks for financial stability. *Financial Stability Review*, Issue 1. European Central Bank.
179. Lewis, R. L., Sutton, N., & Brown, D. A. (2024). How senior managers use interactive control to manage strategic uncertainties: An attention-based view. *Management Accounting Research, 62*, 100864.
180. Li, X., & Evans, J. M. (2022). Incentivizing performance in health care: A rapid review, typology and qualitative study of unintended consequences. *BMC Health Services Research, 22*(1), 690.
181. Liang, L., Dai, T., & Zhang, M. (2024). Generation mechanism of behavioral risk for organizational decision-makers in financial institutions: organizational and human errors. *Humanities and Social Sciences Communications,* 11(1), 1196.
182. Libby, T., & Lindsay, R. M. (2013). The effects of trust and budget-based controls on budget gaming and budget value. *Accounting, Organizations and Society, 38*(7–8), 507–520.
183. Lim, C. Y., Woods, M., Humphrey, C., & Seow, J. L. (2017). The paradoxes of risk management in the banking sector. *The British Accounting Review, 49*(1), 75–90.
184. Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry. SAGE.
185. Linder, S., Leca, B., Zicari, A., & Casarin, V. (2020). Designing ethical management control: Overcoming the harmful effect of management control systems on job-related stress. *Journal of Business Ethics, 167*(4), 835–859.
186. Litzky, B. E., Eddleston, K. A., & Kidder, D. L. (2006). The good, the bad, and the misguided: How managers inadvertently encourage deviant behaviors. *Academy of Management Perspectives*, 20(1), 91–103.
187. Liu, X. K., Wright, A. M., & Wu, Y. J. (2015). Managers' unethical fraudulent financial reporting: The effect of control strength and control framing. *Journal of Business Ethics*, 129(2), 295–310.
188. Locke, K. (2001). Grounded Theory in Management Research. London, England: Sage Publication.

189. Lopez-Valeiras, E., Gomez-Conde, J., Naranjo-Gil, D., & Malagueño, R. (2024). Employees' perception of management control systems as a threat: Effects on deliberate ignorance and workplace deviance. *Accounting Forum*, 48(2), 251–278.
190. Lueg, R., & Knapik, M. (2016). Risk management with management control systems: A pragmatic constructivist perspective. *Corporate Ownership and Control, 13*(3), 72-81.
191. Lui, A. (2015). Greed, recklessness and/or dishonesty? An investigation into the micro-regulation and culture of five UK banks between 2004–2009. *Journal of Banking Regulation, 16*(2), 106–129.
192. Mabwe, K., Ring, P., & Webb, R. (2022). The status of people risk management in UK banks. *Journal of Operational Risk*, 17(2), 83–10
193. MacKenzie, C., Garavan, T. N., & Carbery, R. (2011). Understanding and preventing dysfunctional behavior in organizations: Conceptualizing the contribution of human resource development. *Human Resource Development Review*, 10(4), 346–380.
194. MacLane, C. N., & Walmsley, P. T. (2010). Reducing counterproductive work behavior through employee selection. *Human Resource Management Review*, 20(1), 62–72.
195. Madhani, P. M. (2016). Salesforce control and compensation system: A game theory model approach. *Compensation & Benefits Review*, 47(4), 190–202.
196. Malmi, T., & Brown, D. A. (2008). Management control systems as a package: Opportunities, challenges and research directions. *Management Accounting Research*, 19(4), 287–300.
197. Malmi, T., Kolehmainen, K., & Granlund, M. (2022). Explaining the unintended consequences of management control systems: Managerial cognitions and inertia in the case of Nokia Mobile Phones. *Contemporary Accounting Research*, 40(2), 1013–1045.
198. Marc, M., & Peljhan, D. (2019). Calculative culture in management control systems: Scale and typology development. *Spanish Journal of Finance and Accounting / Revista Española de Financiación y Contabilidad*, 48(1), 30–54.
199. Marc, M., Arena, M., & Peljhan, D. (2023). The role of interactive style of use in improving risk management effectiveness. *Risk Management, 25*(2), 9.
200. Marelli, A., & Dello Sbarba, A. (2025). Insights on the role of performance measurement systems in the digital servitization landscape: a longitudinal case study. *Qualitative Research in Accounting & Management, 22*(3), 286-320.
201. Marinč, M. (2013). Banks and information technology: Marketability vs. relationships. *Electronic Commerce Research*, 13(1), 71–101.
202. Massaro, M., Dumay, J., & Guthrie, J. (2016). On the shoulders of giants: Undertaking a structured literature review in accounting. *Accounting, Auditing & Accountability Journal*, 29(5), 767–801.
203. Merchant, K. A. (1981). The design of the corporate budgeting system: Influences on managerial behavior and performance. *The Accounting Review*, 56(4), 813–829.
204. Merchant, K. A. (1990). The effects of financial controls on data manipulation and management myopia. *Accounting, Organizations and Society*, 15(4), 297–313.
205. Merchant, K. A., & Otley, D. T. (2006). A review of the literature on control and accountability. *Handbooks of Management Accounting Research*, 2, 785–802.
206. Merchant, K., & Van der Stede, W. A. (2017). Management control systems: Performance measurement, evaluation and incentives (4th ed.). Pearson Education Limited

207. Merchant, K., & Van der Stede, W. A. (2024). *Management control systems: Performance measurement, evaluation and incentives* (5th ed.). Pearson Education Limited.
208. Merriam, S. B., & Tisdell, E. J. (2016). Qualitative research: A guide to design and implementation (4th ed.). Jossey-Bass.
209. Middaugh II, J. K. (1988). Management control in the financial-services industry. Business Horizons, 31(3), 79-86.
210. Mikes, A. (2009). Risk Management and Calculative Cultures. *Management Accounting Research, 20*(1), 18–40.
211. Mikes, A. (2011). From Counting Risk to Making Risk Count: Boundary-Work in Risk Management. *Accounting, Organizations and Society, 36*(4–5), 226–245.
212. Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). Qualitative data analysis: A methods sourcebook (3rd ed.). SAGE.
213. Miller, P., Kurunmäki, L., & O'Leary, T. (2008). Accounting, hybrids and the management of risk. *Accounting, Organizations and Society, 33*(7–8), 942–967.
214. Molamohamadi, Z., Samani, M. A., & Karimi, M. (2024). Reviewing the Historical Milestones of Risk Management. SN Business & Economics, 4(161), 1–20.
215. Moosa, I. A. (2007). The Basel Committee, Basel I and Basel II. *Operational Risk Management, 26*-41.
216. Moosa, I. A. (2017). Good Regulation versus Bad Regulation. *Journal of Banking Regulation, 19*(1), 55–63.
217. Muermann, A., & Oktem, U. (2002). The near-miss management of operational risk. *The Journal of Risk Finance, 4*(1), 25-36.
218. Mukherjee, D., Lim, W. M., Kumar, S., & Donthu, N. (2022). Guidelines for advancing theory and practice through bibliometric research. *Journal of Business Research, 148*, 101–115.
219. Müller, J., Gomez-Ruiz, L., & Naranjo-Gil, D. (2025). Do management control systems reduce dysfunctional behaviours? Insights from a literature review on the levers of control framework and research agenda. *Journal of Accounting & Organizational Change.*
220. Mundy, J. (2010). Creating dynamic tensions through a balanced use of management control systems. *Accounting, Organizations and society, 35*(5), 499-523.
221. Nunnally, J. C., & Bernstein, I. H. (1994). Psychometric theory (3rd ed.). McGraw-Hill.
222. Onsi, M. (1973). Factor analysis of behavioral variables affecting budgetary slack. *The Accounting Review*, 48(3), 535–548.
223. ORX (2024). Top 5 Losses May 2024 – *Human Error Events* (Citi and Barclays). Podcast and summary available at https://orx.org/podcast/orx-news-top-5-losses-may-2024-human-error-events.
224. ORX (2024). Top 5 Operational Risk Losses Q4 2024 – Mastercard Case. Available at https://orx.org/blog/top-5-orx-news-losses-q4-2024
225. ORX (2025). Annual Banking Operational Risk Loss Data Report 2025. Oxford Risk Exchange Consortium. Public summary at https://orx.org/blog/global-banks-report-lowest-financial-losses-in-a-decade
226. Otley, D. (1999). Performance management: A framework for management control systems research. Management Accounting Research, 10(4), 363–382.
227. Otley, D. T. (1978). Budget use and managerial performance. *Journal of Accounting Research*, 16(1), 122–149.

228. Otley, D., Broadbent, J., & Berry, A. (1995). Research in management control: An overview of its development. *British Journal of Management*, 6, 31–44.
229. Ouchi, W. G. (1980). Markets, bureaucracies, and clans. *Administrative Science Quarterly*, 25(1), 129–141.
230. Pakhchanyan, S. (2016). Operational risk management in financial institutions: A literature review. *International Journal of Financial Studies, 4*(4), 20.
231. Palinkas, L. A., et al. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health*, 42(5), 533–544.
232. Pang, B., Otto, A. R., & Worthy, D. A. (2015). Self-Control Moderates Decision-Making Behavior When Minimizing Losses versus Maximizing Gains. *Journal of Behavioral Decision Making*, 28(2), 176-187.
233. Patton, M. Q. (2015). Qualitative research and evaluation methods (4th ed.). SAGE.
234. Payne, S. L. (1980). Organization ethics and antecedents to social control processes. *Academy of Management Review, 5*(3), 409–414.
235. Peljhan, D., Miloš Sprčić, D., & Marc, M. (2018). Strategy and Organizational Performance: The Role of Risk Management System Development. In Epstein, M.J., Verbeeten, F.H.M., & Widener, S.K. (Eds.), *Performance Measurement and Management Control: The Relevance of Performance Measurement and Management Control Research* (Studies in Managerial and Financial Accounting, Vol. 33), Emerald Publishing Limited, pp. 65-91.
236. Pilonato, S., & Monfardini, P. (2020). Performance measurement systems in higher education: How levers of control reveal the ambiguities of reforms. *The British Accounting Review,* 52(3), 100908.
237. Podsakoff, P. M., MacKenzie, S. B., & Podsakoff, N. P. (2012). Sources of method bias in social science research and recommendations on how to control it. *Annual review of psychology, 63*(1), 539-569.
238. Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of applied psychology*, *88*(5), 879.
239. Posch, A. (2020). Integrating risk into control system design: The complementarity between risk-focused results controls and risk-focused information sharing. *Accounting, Organizations and Society*, 86, 101126.
240. Power, M. (2005). The invention of operational risk. *Review of International Political Economy, 12*(4), 577-599.
241. Power, M. (2007). *Organized uncertainty: Designing a world of risk management*. Oxford University Press.
242. Power, M. (2009). The Risk Management of Nothing. *Accounting, Organizations and Society*, 34(6–7), 849–855.
243. Rad, A. (2016). Risk management–control system interplay: Case studies of two banks. *Journal of Accounting & Organizational Change*, 12(4), 522–546.
244. Raghvan R.S. (2003). Risk management in Banks. Chartered accountant, pp (841-851).
245. Ramaswami, S. N. (1996). Marketing controls and dysfunctional employee behaviors: A test of traditional and contingency theory postulates. *Journal of Marketing, 60*(2), 105–120.
246. Ranjan, R. (2025). Behavioural Finance in Banking and Management: A Study on the Trends and Challenges in the Banking Industry. *Asian Journal of Economics, Business and Accounting,* 25(1), 374–386.
247. Reason, J. (1990). Human error. Cambridge university press.

248. Reason, J. (2000). Human error: Models and management. *BMJ, 320*(7237), 768–770.
249. Reason, J., Parker, D., & Lawton, R. (1998). Organizational controls and safety: The varieties of rule-related behaviour. *Journal of Occupational and Organizational Psychology,* 71(3), 289–304.
250. Ridgway, V. F. (1956). Dysfunctional consequences of performance measurements. *Administrative Science Quarterly, 1*(2), 240–247.
251. Rikhardsson, P., Rohde, C., Christensen, L., & Batt, C. E. (2021). Management controls and crisis: evidence from the banking sector. *Accounting, Auditing & Accountability Journal*, 34(4), 757-785.
252. Ringgaard, A., Bukh, P. N., & Sandalgaard, N. (2025). Operating the boundary system: A case study of Anti-Money Laundering risk management in a bank. *Journal of Management Control.*
253. Riyono, B. (1998). Cultural issues in personnel selection. *Buletin Psikologi, 1*, 1–9.
254. Rojon, C., McDowall, A., & Saunders, M. N. K. (2021). On the experience of conducting a systematic literature review in industrial, work, and organizational psychology: An illustrative example and methodological insights. *International Journal of Management Reviews, 23*(3), 302–323.
255. Rosanas, J. M., & Velilla, M. (2005). The ethics of management control systems: Developing technical and moral values. *Journal of Business Ethics, 57*(1), 83–96. *
256. Rubin, H. J., & Rubin, I. S. (2012). Qualitative interviewing: The art of hearing data (3rd ed.). SAGE.
257. Sabanova, J., & Kudinska, M. (2022). New tendencies in operational risk management in banks: challenges and opportunities. *Humanities and Social Sciences*: Latvia, 30(1–2), 109–125.
258. Sabanova, J., & Kudinska, M. (2023). The reasons for human errors in banks and employees' mindsets. *Economy and Market Communication Review*, 13(2), 362–378.
259. Sabanova, J., & Kudinska, M. (2024). Management response to human errors and key controls in banks. *Marketing and Management of Innovations*, 15(2), 89–99.
260. Sandelin, M. (2008). Operation of management control practices as a package—A case study on control system variety in a growth firm context. *Management accounting research,* 19(4), 324-343.
261. Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., & Jinks, C. (2018). Saturation in qualitative research: Exploring its conceptualization and operationalization. *Quality & Quantity, 52*(4), 1893–1907.
262. Schiff, M., & Lewin, A. Y. (1970). The impact of people on budgets. *The Accounting Review, 45*(2), 259–268.
263. Schweitzer, M. E., Ordóñez, L. D., & Douma, B. (2002). The dark side of goal setting: The role of goals in motivating unethical decision making. *Academy of Management Proceedings, 2002*(1), B1–B6.
264. Seidman, I. (2013). Interviewing as qualitative research (4th ed.). Teachers College Press.
265. Shakerian, M., Choobineh, A., Jahangiri, M., Hasanzadeh, J., & Nami, M. (2019). Is' invisible gorilla'self-reportedly measurable? Development and validation of a new questionnaire for measuring cognitive unsafe behaviors of front-line industrial workers. *International Journal of Occupational Safety and Ergonomics*: JOSE, 27(3), 852-866.

266. Shields, M. D., Deng, F. J., & Kato, Y. (2000). The design and effects of control systems: Tests of direct- and indirect-effects models. *Accounting, Organizations and Society, 25*(2), 185–202.
267. Shmueli, G., Ray, S., Velasquez Estrada, J. M., & Chatla, S. B. (2016). The elephant in the room: Predictive performance of PLS models. *Journal of Business Research*, 69(10), 4552–4564.
268. Siaw Ofori, B., Padi, A., & Musah, A. (2025). Corporate governance effectiveness and operational risk of banks. *Discover Global Society*, 3(23), 1–20.
269. Simons, R. (1995). *Levers of control: How managers use innovative control systems to drive strategic renewal*. Harvard Business School Press.
270. Simons, R. L. (2000). *Performance measurement and control systems for implementing strategy*. Pearson.
271. Siverbo, S., Cäker, M., & Åkesson, J. (2019). Conceptualizing dysfunctional consequences of performance measurement in the public sector. *Public Management Review, 21*(12), 1801–1823.
272. Slapničar, S., Axelsen, M., & Eulerich, M. (2025). Cyber risk management: an illusion of a risk-based approach. *Journal of Management Control.*
273. Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333–339.
274. Soin, K., & Collier, P. (2013). Risk and Risk Management in Management Accounting and Control. *Management Accounting Research*, 24(2), 82–87.
275. Soin, K., & Scheytt, T. (2010). Risk and risk management in management accounting and control. In C. S. Chapman, A. G. Hopwood, & M. D. Shields (Eds.), Handbook of management accounting research. Vol. 2, pp. 729–755. Elsevier.
276. Soin, K., Varoutsa, E., & Taylor, L. (2020). Blurred lines. *Enterprise Risk: The official magazine of The Institute of Risk Management*, 28-29.
277. Sorauren, I. F. (2000). Non-monetary incentives: Do people work only for money? *Business Ethics Quarterly, 10*(4), 925–944.
278. Speklé, R. F., & Verbeeten, F. H. M. (2014). The use of performance measurement systems in the public sector: Effects on performance. *Management Accounting Research, 25*(2), 131–146.
279. Sponem, S., & Lambert, C. (2016). Exploring differences in budget characteristics, roles and satisfaction: A configurational approach. *Management Accounting Research, 30*, 47–61.
280. Staal, M. A. (2004). Stress, cognition, and human performance: A literature review and conceptual framework.
281. Stake, R. E. (1995). The art of case study research. Sage.
282. Strauss, L. (2015). Management control system design: Conditional inter-dependencies between behavioral constraints, incentives and employee selection. *Marble Series: Research in Business and Economics, 2*, 81–103.
283. Suh, W. (2019). Intrinsic nature of management control systems: Legislated and contextual elements. *Kindai Management Review, 7*, 115–128.
284. Tangney, J. P., Boone, A. L., & Baumeister, R. F. (2018). High self-control predicts good adjustment, less pathology, better grades, and interpersonal success. *Self-Regulation and Self-Control,* 173–212.
285. Tannenbaum, A. S. (1962). Control in organizations: Individual adjustment and organizational performance. *Administrative Science Quarterly, 7*(2), 236–257.
286. Tayler, W. B., & Bloomfield, R. J. (2011). Norms, conformity, and controls. *Journal of Accounting Research, 49*(3), 753–790.
287. The Committee for the Prize in Economic Sciences in Memory of Alfred Nobel.

(2022). *Financial intermediation and the economy: Scientific background on the Sveriges Riksbank Prize in Economic Sciences in Memory of Alfred Nobel 2022.* The Royal Swedish Academy of Sciences.
288. Tran, T.-V., Lepistö, S., & Järvinen, J. (2021). The relationship between subjectivity in managerial performance evaluation and the three dimensions of justice perception. *Journal of Management Control, 32*(3), 369–399.
289. Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management, 14*(3), 207–222.
290. Tyler, T. R., & Blader, S. L. (2005). Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings. *Academy of Management Journal, 48*(6), 1143–1158.
291. Vakkuri, J., & Meklin, P. (2006). Ambiguity in performance measurement: A theoretical approach to organisational uses of performance measurement. *Financial Accountability & Management, 22*(3), 235–250.
292. Van Camp, J., & Braet, J. (2016). Taxonomizing performance measurement systems' failures. *International Journal of Productivity and Performance Management, 65*(5), 672–693.
293. van den Tillaart, A. H. A. J. (2003). Controlling operational risk: concepts and practices. A participant-observer research on the development of concepts and practices in controlling operational risk in a banking environment. PhD dissertation: University of Twente.
294. Van der Kolk, B., & Schokker, T. (2016). Strategy implementation through hierarchical couplings in a management control package: An explorative case study. *Journal of Management Control, 27*(2–3), 129–154.
295. Van der Kolk, B., van Veen-Dirks, P. M., & ter Bogt, H. J. (2019). The impact of management control on employee motivation and performance in the public sector. *European Accounting Review, 28*(5), 901–928.
296. Van der Stede, W. A. (2000). The relationship between two consequences of budgetary controls: Budgetary slack creation and managerial short-term orientation. *Accounting, Organizations and Society, 25*(6), 609–622.
297. Van der Stede, W. A. (2001). Measuring 'tight budgetary control'. *Management Accounting Research, 12*(1), 119–137.
298. Van Fleet, D. D., & Griffin, R. W. (2006). Dysfunctional organization culture: The role of leadership in motivating dysfunctional work behaviors. *Journal of Managerial Psychology, 21*(8), 698–708.
299. Verburg, R. M. (2017). The role of organizational control systems in employees' organizational trust. *Frontiers in Psychology*, 8, 702.
300. Vives, X. (2019). Digital disruption in banking. *Annual Review of Financial Economics, 11*, 243–272.
301. Wahlström, G. (2009). Risk management versus operational action: Basel II in a Swedish context. *Management Accounting Research*, 20(1), 53–68.
302. Wang, Y. J., Chen, K. Y., Dou, K., & Liu, Y. Z. (2021). Linking self-control to voluntary behaviors at workplace: The mediating role of job satisfaction. *Frontiers in Psychology*, 12, 530297.
303. Weaver, G. R., Treviño, L. K., & Cochran, P. L. (1999). Corporate ethics programs as control systems: Influences of executive commitment and environmental factors. *Academy of Management Journal*, 42(1), 41–57.
304. Widener, S. K. (2007). An empirical analysis of the levers of control framework. *Accounting, organizations and society*, 32(7-8), 757-788.

305. Willert, J., Israelsen, P., Rohde, C., & Toldbod, T. (2017). Senior management use of management control systems in large companies. *Corporate Ownership and Control*, 14(4), 58–76.
306. Wright, J. F. (2018). Risk Management: A Behavioural Perspective. Oslo and Akershus University College of Applied Sciences.
307. Xu, Y., Pinedo, M., & Xue, M. (2017). Operational risk in financial services: A review and new research opportunities. *Production and Operations Management*, 26(3), 426–445.
308. Xu, Y., Tan, T. F., & Netessine, S. (2022). The impact of workload on operational risk: Evidence from a commercial bank. Management Science, 68(4), 2668-2693.
309. Yin, R. K. (2009). Case study research: Design and methods (4th ed.). Sage.
310. Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). Sage.
311. Yokoi-Arai, M. (2003). The Evolving Concept of Operational Risk and Its Regulatory Treatment. Law and Business Review of the Americas, 9(1), 105–152. *
312. Young, S. M. (1985). Participative budgeting: The effects of risk aversion and asymmetric information on budgetary slack. *Journal of Accounting Research*, 23(2), 829–842.
313. Zéman, Z., Gacsi, R., Lukács, J., & Hajós, L. (2013). Management control system in banks. BIATEC, 21(6), 14-17.
314. Zhao, X., Lynch, J. G., & Chen, Q. (2010). Reconsidering Baron and Kenny: Myths and truths about mediation analysis. *Journal of Consumer Research*, 37(2), 197–206.

APPENDICES

Appendix 1: Daljši povzetek (Extended summary in Slovene language)

Naslov: Vpliv managerske kontrole na obvladovanje operativnih tveganj v bankah

Raziskava izhaja iz obsežne literature s področja managementa, poslovodnega računovodstva in organizacijskih ved, ki poudarja, da lahko sistemi managerske kontrole poleg želenih učinkov povzročijo tudi nepredvidene in disfunkcionalne posledice. Tradicionalno so bili sistemi managerske kontrole obravnavani kot mehanizmi, namenjeni usklajevanju vedenja z organizacijskimi cilji ter krepitvi koordinacije aktivnosti in uspešnosti poslovanja (Anthony, 1965; Malmi & Brown, 2008; Simons, 1995). Kasnejša raziskovanja pa so pokazala, da lahko sistemi managerske kontrole sprožijo vrsto neželenih vedenjskih odzivov, kot so izigravanje sistema, ustvarjanje rezerv z neoptimalnim načrtovanjem bodočega poslovanja, simbolno izpolnjevanje zahtev, erozija etičnih standardov, odpor zaposlenih in povečanje stresa. Na podlagi konceptualne opredelitve disfunkcij v sistemih managerske kontrole, kot jih navajata Merchant in Van der Stede, ki poudarjata, da se problemi sistemov managerske kontrole kažejo kot posledica pomanjkanja usmeritev, motivacijskih spodbud ali osebnih zmožnosti zaposlenih, smo v prvem poglavju raziskali, kako so različni tipi sistemov managerske kontrole povezani z specifičnimi oblikami disfunkcionalnega vedenja.

Čeprav so že zgodnja dela (npr. Hopwood, 1972; Ridgway, 1956; Van der Stede, 2000) opozarjala na možnost nastanka neželenih posledic managerske kontrole, so bila empirična dognanja razdrobljena, brez enotne razlage o tem, kako različne vrste managerske kontrole sprožajo specifične oblike disfunkcionalnega vedenja. Obstoječe pregledne študije (Franco-Santos et al., 2012; Van Camp & Braet, 2016) so prispevale k oblikovanju pomembnih taksonomij, vendar večinoma niso sistematično povezale tipov sistemov managerske kontrole z vrstami disfunkcionalnega vedenja (t.j. z vedenjskimi odkloni). Podobno so raziskave, ki so se opirale na konceptualne okvire, kot je na primer Simonsov okvir vzvodov managerske kontrole (ang. Levers of Control) (Müller et al., 2025), ali sektorski pregledi literature, na primer v zdravstvu in reviziji (Fiolleau et al., 2018; Li & Evans, 2022), razkrile določene vzorce, vendar niso zagotovile analitično jasne povezave med posameznimi tipi managerske kontrole in značilnimi vedenjskimi odzivi. V prvem poglavju smo zato naslovili raziskovalno vrzel na tem področju, ki je nastala zaradi pomanjkanja sinteze, ki bi tipologijo sistemov managerske kontrole povezala z vedenjskimi mehanizmi in kontekstualni dejavniki, ki oblikujejo pojav disfunkcij.

V raziskavi smo za teoretično osnovo uporabili okvir objektov nadzora (ang. Object of Control – OOC), ki sta ga razvila Merchant in Van der Stede (2017) in ki razlikuje med štirimi tipi managerske kontrole glede na vedenjski objekt kontrole: kontrola nad rezultati, kontrola nad dejanji, kontrola nad osebami ter kontrola nad organizacijsko kulturo. Ta pristop omogoča vedenjsko usmerjeno analizo, ki se ne osredotoča na sistem kot celoto, temveč na to, kaj natančno je predmet kontrole (rezultati, dejanja, ljudje ali organizacijska kultura). To je omogočilo razvoj bolj preciznega analitičnega okvira, primernega za

preučevanje osrednjega raziskovalnega problema, ki je, kako posamezni nadzorni mehanizmi vodijo do specifičnih vzorcev disfunkcionalnega vedenja.

Metodološko smo uporabili pristop sistematičnega pregleda literature (SPL) v skladu z usmeritvami v Tranfield et al. (2003) ter kasnejšimi nadgradnjami (Kuckertz & Block, 2021; Massaro et al., 2016; Snyder, 2019). Raziskava je bila zasnovana kot teoretsko in fenomenološko usmerjen SPL, ki se je osredotočil na sintetiziranje ugotovitev glede nepredvidenih vedenjskih posledicah sistemov managerske kontrole skozi prizmo OOC. Razvili smo pregleden protokol, ki je opredelil raziskovalno vprašanje, iskalno strategijo, kriterije za vključitev in izključitev enot literature ter kodirni okvir. Skladno z logiko CIMO (Context–Intervention–Mechanism–Outcome) po Denyerju in Tranfieldu (2009), smo ključne koncepte, povezane s sistemi managerske kontrole in njihovimi vedenjskimi posledicami, preoblikovali v nabor iskalnih izrazov.

Zadnjo posodobitev rezultatov iskanja literature, s posebnim poudarkom na najnovejših objavah, smo izvedli januarja 2025 v petih večjih podatkovnih bazah: ScienceDirect, Scopus, Web of Science, JSTOR in Taylor & Francis. Iskanje je bilo omejeno na recenzirane znanstvene članke v angleščini. Po odstranitvi podvojenih zapisov in uporabi predhodno določenih kriterijev za vključitev je bilo v vzorec vključenih 95 člankov, objavljenih med letoma 1956 in 2025. Članki so bili kodirani v strukturirani Excelovi matriki, v kateri so bili za vsak članek zabeleženi tip sistema managerske kontrole (v skladu s tipologijo OOC), opaženi problemi kontrole, opisani vedenjski mehanizmi ter kontekstualni vplivi.

Ugotovitve iz pregleda literature smo oblikovali v šest tematskih sklopov. Prvi sklop se je osredotočil na kontrolo nad rezultati, katere jedro predstavlja povezovanje nagrad ali sankcij z doseženimi rezultati. Štiriinštirideset študij je pokazalo, da lahko slabo zasnovani ali togi sistemi kontrole nad rezultati vodijo v različne oblike disfunkcionalnega vedenja. Med pogostimi problemi so se pojavljali izigravanje sistema in prirejanje poročanja (npr. manipulacija kazalnikov, ustvarjanje rezerve pri načrtovanju ciljev poslovanja), neetično ravnanje (laganje, zavajanje zaradi pridobitve nagrad ali izogibanja sankcijam), osredotočenost na ozek nabor merjenih ciljev, zmanjšanje notranje motivacije, psihološki stres ter ritualizirana uporaba sistemov za načrtovanje poslovanja in sistemov za obvladovanje uspešnosti poslovanja. Ti problemi so izhajali iz nerealnih ciljnih vrednosti, pretirane osredotočenosti na kvantitativne kazalnike, kaznovalne uporabe informacij o uspešnosti ter spodbujevalnih shem, ki nagrajujejo videz uspešnosti namesto dejanskih rezultatov. Kontekstualni dejavniki, kot so negotovost delovnih nalog, organizacijska kultura, vključenost zaposlenih v postavljanje ciljev ter slog vodenja, so pomembno oblikovali intenzivnost disfunkcij.

Drugi tematski sklop je preučeval kontrolo nad dejanji, kjer se vedenje usmerja z natančno določenimi pravili, postopki in nadzorom. Šest študij je ugotovilo, da togo ali prisilno uvajanje takih kontrolnih orodij pogosto vodi do odtujenosti, demotivacije, rutinskih kršitev pravil, oblikovanja obvodnih načinov delovanja, neetičnega vedenja in konflikta vlog

posameznika. Mehanizmi, ki so povzročali te izide, so vključevali pretirano intenziven nadzor, pomanjkanje diskrecije ter neustrezno ujemanje med podrobnimi pravili in kompleksnimi nalogami. Učinki kontrole nad dejanji so bili močno odvisni od značilnosti nalog (rutinske vs. kompleksne), organizacijske in profesionalne kulture ter načina, kako so bila pravila utemeljena in komunicirana.

Tretji sklop je preučeval kontrolo nad osebami, ki naj bi z izbiro, razvojem in motiviranjem »pravih ljudi« zagotavljala ustrezno vedenje in posledično doseganje ciljev poslovanja. Čeprav se pogosto predpostavlja, da so ti kontrolni mehanizmi benigni, je šest študij pokazalo, da lahko vodijo do nezaupanja, zmanjšane zavzetosti pri delu, odklonskega vedenja pri delu, kulturnega neskladja, neskladja vrednot ter neskladne motivacije. Ti problemi so se pojavljali, kadar postopki izbire niso dovolj preverjali integritete ali vrednot kandidatov za zaposlitev, ko so bili procesi socializacije in povratnih informacij šibki ali ko je bila kontrola nad osebami v nasprotju z drugimi kontrolnimi sistemi (npr. selekcija za ustvarjalnost ob hkratno togih delovnih procedurah). Nacionalna kultura, negotovost delovnih nalog ter način vodenja so pomembno vplivali na to, ali so sistemi kontrole učinkoviti ali disfunkcionalni.

Četrti sklop se je osredotočil na kontrolo nad organizacijsko kulturo, kjer je cilj vplivati na vedenje preko skupnih norm, vrednot in prepričanj. Deset študij je ugotovilo različne disfunkcionalne posledice, kot so zbeganost glede norm, drsenje etičnih standardov, simbolna etika in cinizem, neskladja vrednot, odpor, pritiski sodelavcev, rigidnost organizacijske kulture ter molk ob nepravilnostih. Te težave so pogosto izvirale iz razkoraka med formalno izraženimi vrednotami in dejanskim vedenjem vodstva, površnih etičnih programov, neuspele ali neobstoječe integracije vrednot organizacijske kulture v sisteme zaposlovanja in sisteme nagrajevanja ter toge organizacijske (sub)kulture, ki se ni želela prilagoditi potrebnim spremembam. Vodstveni zgled, nacionalna in profesionalna kultura, zgodovina organizacije ter zunanji šoki so pomembno oblikovali delovanje kontrole nad organizacijsko kulturo.

Peti tematski sklop je preučeval težave, ki izhajajo iz sočasne uporabe več tipov kontrole. Enajst študij je pokazalo, da lahko kombinacije kontrole nad rezultati, dejanji, osebami in kulture postanejo same po sebi vir disfunkcij, kadar niso ustrezno usklajene. Pojavljali so se kratkoročna usmerjenost, oportunizem, preobremenjenost s cilji ali nejasnost ciljev (kadar sistemi kontrole pošiljajo neujemajoča se sporočila), oslabljena uveljavitev pravil, etični zdrs ter moralna odtujenost (kadar trde metrike nasprotujejo mehkim vrednotam). Ti izidi so izvirali iz neusklajenosti med posameznimi tipi kontrole, fragmentirane zasnove managerske kontrole, razhajanja med formalnimi vrednotami in dejanskim ravnanjem ter pretiranega plastenja kontrolnih mehanizmov.

Šesti sklop se je osredotočil na neskladja med zasnovo in uporabo sistemov kontrole. Osemnajst študij je pokazalo, da lahko zaznava sistema kontrole kot prisilnega, kaznovalnega ali nepravičnega sproži odpor, odklonsko vedenje ali umik. Pomanjkanje

ujemanja z organizacijskim kontekstom je lahko povzročilo, da sistemi kontrole postanejo nepomembni ali celo škodljivi, fragmentacija in protislovja v zasnovi pa so oslabila odgovornost in uspešnost. Nejasni kazalniki ali napačna uporaba sistemov kontrole, denimo izključno diagnostična raba, kjer bi bila bolj primerna interaktivna raba, dodatno spodbujajo izigravanja sistema, napačne interpretacije in stres. Kontekstualni dejavniki kot so dinamičnost zunanjega okolja organizacije, zrelost organizacije ter jasnost komunikacije strategije vplivajo na intenzivnost teh disfunkcij.

Na podlagi teh ugotovitev smo razvili konceptualni okvir, ki povezuje tipe sistemov kontrole, mehanizme, vedenjske manifestacije in kontekstualne moderatorje. Identificirali smo šest prevladujočih mehanizmov: i) preveč toga ali prisilna zasnova sistema, ii) pomanjkanje kontekstualne ustreznosti, iii) izrinjanje notranje motivacije, iv) nezadostna udeležba in avtonomija, v) simbolična ali nedosledna uporaba sistema kontrole ter vi) neskladje med zasnovo in uporabo. Čeprav so ti mehanizmi pogosto privedli do negativnih vedenjskih posledic, so kontekstualni pogoji, kot so močna etična infrastruktura, usklajeni sistemi kontrole in jasna komunikacija strategije, lahko ublažili disfunkcionalnost ali celo privedli do pozitivnih učinkov, kot sta učenje in inovativnost. Izpostavili smo pet kontekstualnih vplivov: kompleksnost nalog, kulturne in profesionalne norme, ton vodenja, organizacijska struktura in pritiski iz zunanjega okolja.

Glavni prispevek tega dela disertacije je empirično podprto kartiranje, ki prikazuje, kako so različne vrste sistemov kontrole (rezultatov, dejavnosti, oseb in kulture) ter njihove kombinacije in vzorci uporabe povezani z različnimi ponavljajočimi se problemi kontrole. Obstoječo literaturo smo tako nadgradili s prehodom od kategorizacije problemov kontrole k vzročno-posledičnim razlagam ter s predlogom analitično podrobnega, na vedenju temelječega konceptualnega okvira, ki je uporaben tako za znanstvenike kot za praktike. Orisali smo možnosti za prihodnje raziskave, ki vključujejo empirično preverjanje identificiranih mehanizmov in poglobljeno analizo premalo raziskanih tipov sistemov kontrole. Spoznanja tega poglavja so zagotovila teoretično podlago za preučevanje problemov managerske kontrole v specifičnem kontekstu obvladovanja operativnih tveganj v bančništvu, ki smo jih preučili v 2. poglavju.

Analiza v poglavju 2 se je tako osredotočila na razmerje med problemi managerske kontrole in obvladovanjem operativnega tveganja v bančnem sektorju. V tem delu disertacije smo želeli spoznati, kako takšni problemi managerske kontrole nastajajo v okviru oblikovanja in uporabe sistemov obvladovanja operativnih tveganj in skozi katere organizacijske in vedenjske mehanizme povzročajo operativna tveganja. Takšna usmeritev odraža naraščajoče prepoznavanje v regulativnih okvirih in akademski literaturi, da operativno tveganje ni le tehnična kategorija, ampak je tesno povezano z organizacijskimi strukturami, vedenjskimi odzivi in delovanjem sistemov kontrole. Od uvedbe okvirov Basel II in Basel III, ki poudarjajo sistematične pristope k prepoznavanju, ocenjevanju in zmanjševanju tveganj, ki izhajajo iz napak ljudi, procesov, sistemov ali zunanjih dogodkov (Basel Committee, 2003, 2006, 2011), raziskave vse bolj poudarjajo, kako operativne ranljivosti izhajajo iz interakcij

med formalnimi kontrolami in vedenjskimi prilagoditvami zaposlenih (Mikes, 2009; Power, 2007).

Tudi za analizo teh interakcij smo se oprli na okvir OOC (Merchant & Van der Stede, 2017), ki razlikuje štiri tipe kontrol na podlagi vedenjskega objekta, na katerega so usmerjene: kontrole nad rezultati, kontrole nad dejanji, kontrole nad osebjem in kontrole nad kulturo. Kontrole rezultatov vplivajo na vedenje in ravnanje prek merljivih rezultatov in sistemov spodbud; kontrole dejavnosti predpisujejo ali omejujejo določena ravnanja; kontrole osebja se osredotočajo na izbor in razvoj kompetentnih in motiviranih zaposlenih; kontrole nad kulturo pa vključujejo skupne norme in vrednote, ki usmerjajo vedenje v negotovih razmerah. Da bi omogočili podrobnejšo sintezo pregledane literature, so bile te teoretične vrste kontrole operacionalizirane v štiri analitične kategorije (pravila in postopki, struktura, spodbude in kultura), ki so zajemale ponavljajoče se teme v kontekstu obvladovanja operativnih tveganj. Pravila in postopki so ustrezali kontroli nad dejanji in so vključevali formalne standarde in regulativne mehanizme, ki predpisujejo sprejemljivo vedenje in omejujejo operativno variabilnost. Struktura odraža elemente kontrole nad osebjem, poudarja pa, kako organizacijske hierarhije, ločevanje nalog in linije poročanja oblikujejo odgovornost in pretok informacij. Spodbude izhajajo iz kontrole rezultatov in zajemajo motivacijske in na uspešnosti temelječe mehanizme, ki usklajujejo individualne cilje s stopnjo organizacijske tolerance do tveganja. Kultura predstavlja kontrolo nad kulturo in se nanaša na skupne norme, vrednote in etične usmeritve, ki vplivajo na dojemanje tveganja, skladnost vedenja in kolektivno učenje.

Skupaj ti tipi kontrole tvorijo celovito arhitekturo preko katere managerji vplivajo na vedenje in ravnanje ljudi s ciljem zmanjševanja negotovosti. Vendar pa lahko vsaka od njih postane tudi vir disfunkcionalnosti. Preveč strogi in togi kontrolni ukrepi lahko omejujejo presojanje, neusklajena kontrola nad rezultati lahko spodbujajo prevzemanje tveganj, šibki kadrovski kontrolni ukrepi lahko vodijo do utrujenosti ali neskladja kompetenc, krhke kulturne kontrole pa lahko spodkopavajo etično ozaveščenost (Acrey et al., 2011; Cohn et al., 2014; Gurd & Helliar, 2017; Lui, 2015). Postavljeni okvir je zato zagotovil analitično perspektivo za preučevanje, kako se napake v zasnovi teh tipov kontrole ter njihove vedenjske posledice prelevijo v operativne ranljivosti.

V pregledanih študijah se je pojavilo več kategorij problemov kontrole, ki so ključne za razumevanje, kako kontrolni mehanizmi lahko nenamerno ustvarijo ali okrepijo operativna tveganja. Problemi, povezani s strukturo, izhajajo iz razdrobljene organizacijske zasnove, ločenih poročevalskih linij in šibke koordinacije med poslovnimi enotami, obvladovanjem tveganj, zagotavljanjem skladnosti in revizijo. Takšni vzorci ustvarjajo slepe točke, ki ovirajo odkrivanje nepravilnosti in preprečujejo pravočasno sporočanje nastajajočih problemov. Problemi, povezani s pravili, se pojavijo, ko regulativni ali notranji postopki postanejo pretirano podrobni ali neprožni, kar vodi v avtomatsko vedenje, zmanjšano pozornost ali spodbujanje obvodov, ki spodkopavajo zanesljivost procesov. Problemi, povezani s spodbudami, vključujejo neusklajene cilje za merjenje uspešnosti, agresivne

prodajne cilje in kazalnike ter kulturo, usmerjeno v doseganje bonusov, ki povzroča iskanje bližnjic, napačne prodajne taktike, manipulacijo podatkov in kognitivno preobremenitev. Kulturne in etične težave nastanejo, ko se pojavijo neskladja med formalnimi vrednotami glede tveganj in vsakdanjimi praksami, kar vodi do nepopolnega poročanja, normalizacije deviacij in nezmožnosti postaviti se po robu neprimernemu vedenju. Dodatna kategorija zadeva neskladje med zasnovo in uporabo kontrol, kjer kontrole, ki se na papirju zdijo robustne, v praksi postanejo neučinkovite zaradi ritualne uporabe, površinske skladnosti ali pomanjkanja smiselnega nadaljnjega ukrepanja.

Te kategorije odražajo širši mehanizem vedenjske in institucionalne povezanosti, preko katerega vedenjske prilagoditve zaposlenih v medsebojnem delovanju z institucionaliziranimi instrumenti kontrole ustvarjajo operativne ranljivosti. Tudi če se formalni sistemi zdijo robustni, lahko vsakodnevna vedenja, kot so obvodi, neformalno usklajevanje, selektivno upoštevanje predpisov ali dajanje prednosti finančnim ciljem, spremenijo dejanski način delovanja kontrol v praksi. Ta pojav pomaga pojasniti, zakaj lahko kontrole, namenjene preprečevanju napak ali neprimernega ravnanja, v določenih okoliščinah prispevajo k operativnim napakam.

Prispevek tega dela disertacije je v povezovanju teorije managerske kontrole z raziskovanjem operativnega tveganja ter v razvoju strukturiranega analitičnega okvira za preučevanje, kako problemi managerske kontrole vplivajo na operativne rezultate. V poglavju pokažemo, da operativnega tveganja ni mogoče razumeti zgolj kot napako procesov ali sistemov, ampak ga je treba analizirati v širšem okviru zasnove sistemov kontrol, vedenjskih odzivov in kulturne dinamike. To konceptualno izhodišče je usmerjalo empirične analize v poglavjih 3 in 4, kjer smo preučevali, kako se ti mehanizmi udejanjajo v organizacijski praksi in kako vplivajo na tveganja, povezana z vedenjem ljudi (zaposlenih), v bančnem kontekstu.

V tretjem poglavju disertacije smo prešli od konceptualne analize k empiričnemu preučevanju, s ciljem razumeti, kako se problemi managerske kontrole dejansko udejanjajo v bančni organizaciji. Namen tega dela ni bil preverjanje modela iz pregleda literature v poglavju 2, temveč ga empirično dodatno raziskati, izostriti in nadgraditi s pomočjo kvalitativne analize. Zato smo se v tretjem poglavju osredotočili na razumevanje, kako takšni problemi nastajajo, kako so vgrajeni v vsakodnevne prakse in strukture banke ter kako prispevajo k operativnemu tveganju, kot je opredeljeno v okvirih Basel II/III.

Ugotovitve na podlagi intervjujev z managerji različnih organizacijskih enot kažejo, da se slabosti sistema kontrol v banki pojavljajo prek petih mehanizmov: i) strukturne ranljivosti, ii) omejitve zaradi pravil, iii) omejitve zmogljivosti in sposobnosti zaposlenih, iv) neusklajenosti spodbud ter v) kulturni in etični zdrs. Ti mehanizmi skupaj razložijo, kako so kontrole rezultatov, kontrole dejanj, kontrole osebja in kontrole kulture uporabljene v vsakodnevnih operacijah ter kje se v tem procesu pojavijo ranljivosti.

Strukturne ranljivosti zajemajo slabosti v socio-tehnični infrastrukturi, vključno z nepopolno avtomatizacijo, napačnimi konfiguracijami in nastavitvami sistemov, razdrobljenimi procesi in zanašanjem na ročne obvode. Te težave so vplivale na zanesljivost procesov ter ustvarjale izpostavljenosti tveganjem, povezanih z izvedbo, dostavo in managementom procesov, ter tveganjem sistemskih okvar. Omejitve zaradi pravil zajemajo učinke pravnih in regulativnih zahtev ter strogo predpisanih notranjih postopkov, ki omejujejo operativno fleksibilnost in ustvarjajo ozka grla ali napetosti glede skladnosti. Te omejitve so bile povezane z izpostavljenostjo tveganjem, ki so povezana s strankami, produkti in poslovnimi praksami, kadar so stroga pravila zaposlene prisilila k improvizaciji ali razvoju obvodov. Omejitve zmogljivosti in sposobnosti zaposlenih izhajajo iz vrzeli v znanju, kadrovskih pomanjkljivosti, odpora do digitalne transformacije ter vztrajna prisotnost človeških napak na področjih, kjer so avtomatizirani nadzori omejeni. Te omejitve so prispevale predvsem k izpostavljenosti tveganjem, povezanih z izvedbo, dostavo in managementom procesov, ter tveganjem, povezanih s kadrovskimi praksami in varnostjo na delovnem mestu, zlasti tam, kjer je zmanjšan nadzor ali pretirano zanašanje na ročne procese povečalo verjetnost napak. Neusklajenost spodbud izvira iz oblikovanja zasnove in načina uporabe kontrole rezultatov, zlasti visokih pragov za izplačilo bonusov in pritiskov, povezanih s ciljno naravnanostjo, kar vpliva na to, kako zaposleni določajo prioritete in lahko spodbuja vedenje na meji dovoljenega. Ti pritiski so bili povezani z izpostavljenostjo tveganjem, povezanih z izvedbo, dostavo in managementom procesov ter tveganjem, povezanih s strankami, produkti in poslovnimi praksami, zlasti kadar so odzivi zaposlenih vključevali postopkovne bližnjice ali vedenje na meji dopustnega. Kulturni in etični zdrs se pojavi, kadar etična disciplina, skupne norme in zavedanje tveganj ne vodijo dosledno vedenja zaposlenih, kar omogoča neprimerno ravnanje, prikrivanje, obhajanje postopkov ali odstopanja, utemeljena na osebnem zaupanju. Ti procesi so ustvarjali izpostavljenosti tveganjem, ki so povezana z notranjimi prevarami, tveganjem, ki so povezana s strankami, produkti in poslovnimi praksami, ter tveganjem izvedbe, dostave in managementa procesov.

Identificirani mehanizmi so nakazali empirične poti, preko katerih so se pokazali širši vzorci izvora ranljivosti. Prvi vzorec so predstavljale težave, ki izvirajo iz oblikovanja zasnove kontrol (strukturne ranljivosti, omejitve zaradi pravil, neusklajenosti spodbud). Drugi vzorec pa je zajemal težave, povezane s sposobnostmi in vedenjem zaposlenih (omejitve zmogljivosti in sposobnosti, kulturni in etični zdrs). Z opredelitvijo teh dveh poti je analiza pokazala, da operativne ranljivosti (in s tem tveganja) niso naključne, temveč sistematično povezane z načinom, kako so kontrole oblikovane, interpretirane in izvajane v praksi.

Analiza je prav tako pokazala, da se ti mehanizmi odražajo v specifičnih kategorijah operativnih tveganj po okvirih Basel II/III. Strukturne ranljivosti ustvarjajo predvsem tveganja izvajanja, dostave in managementa procesov ter tveganja, povezana s sistemi, zlasti tam, kjer ročni procesi, odvisnost od zunanjih izvajalcev ali nestabilni sistemi zmanjšujejo zanesljivost procesov. Omejitve zaradi pravil so povezane s tveganji, ki izhajajo iz poslovnih praks, strank in produktov, ter s tveganji skladnosti, kjer toga pravila ustvarjajo situacije, ki

zahtevajo prilagajanje procesov ali uvajanje obvodov. Omejitve zmogljivosti in sposobnosti zaposlenih prispevajo predvsem k tveganjem izvajanja, dostave in managementa procesov ter k tveganjem, povezanim z zaposlenimi, saj kadrovske vrzeli, pomanjkanje znanja in odpor do digitalnih procesov povečujejo verjetnost napak in zmanjšujejo učinkovitost nadzora. Neusklajenosti spodbud so povezane s tveganji izvajanja procesov ter tveganji, ki izhajajo iz poslovnih praks, strank in produktov, saj pritiski zaradi ciljev vplivajo na ravnanje zaposlenih v odnosu do postopkov, strank in dokumentacije. Kulturni in etični zdrs ustvarja tveganja notranjih prevar, tveganja poslovnih praks ter tveganja izvajanja procesov, kadar popusti etična pozornost, preglednost ali disciplina pri upoštevanju postopkov.

V celoti je analiza pokazala, da operativno tveganje v banki ne izhaja iz izoliranih napak, temveč iz prepoznavnih mehanizmov, povezanih z oblikovanjem sistemov kontrole in s sposobnostmi zaposlenih. Z raziskovanjem teh procesov je kvalitativna analiza razkrila, kako se managerske kontrole v praktičnem okolju prevedejo v operativne ranljivosti.

Tretje poglavje disertacije tako prispeva k akademskemu razumevanju, kako problemi managerske kontrole oblikujejo operativno tveganje v bančnem sektorju. Empirična analiza je nadgradila obstoječo literaturo, saj je pokazala, kako se konceptualni mehanizmi, predstavljeni v literaturi, udejanjajo v vsakodnevnih praksah realne organizacije. Ugotovljeni dve širši skupini ranljivosti (t.j. težave, ki izvirajo iz oblikovanja kontrol, ter težave, povezane s sposobnostmi in vedenjem zaposlenih) ponujata strukturiran način razlage, kako organizacijske odločitve o oblikovanju sistemov kontrole in vedenjski odzivi skupaj oblikujejo operativna tveganja. Z razporeditvijo teh mehanizmov v specifične kategorije operativnih tveganj po Baslu II/III je naša raziskava razvila tudi integrirano perspektivo, ki povezuje raziskave s področja managerske kontrole z literaturo na področju operativnih tveganj v bančništvu. S tem je poglobila teoretično razumevanje, kako operativna tveganja nastajajo na presečišču organizacijskih struktur, kontrolnih praks in vedenja zaposlenih.

Na podlagi ugotovitev kvalitativne raziskave iz poglavja 3, ki je med drugim izpostavila, kako se težave managerske kontrole pojavijo preko prepoznavnih organizacijskih mehanizmov, se je analiza v poglavju 4 preusmerila na kvantitativno preučevanje vpliva takšnih težav na pogostost tveganih ravnanj, ki prispevajo k operativnemu tveganju. Raziskava se je osredotočila na razumevanje, kako strogi sistemi kontrole, kultura tveganja, interaktivna uporaba obvladovanja tveganj in samokontrola oblikujejo tri različne kategorije tveganega ravnanja: i) spodrsljaji in napake, ii) rutinska kršitve in iii) izjemne kršitve. Vodilno raziskovalno vprašanje je bilo, kako strogost managerske kontrole vpliva na pogostost tveganih ravnanj, ki prispevajo k operativnemu tveganju.

Strogi sistemi managerske kontrole so v bančnem kontekstu pojmovani kot potencialno dvorezni meč. Stroga kontrola nad rezultati je opredeljena kot kontrola, ki vsebuje jasne in zahtevne cilje uspešnosti na delovnem mestu, z omejeno toleranco za odstopanja, medtem ko je stroga kontrola nad dejanji opredeljena kot kontrola, ki temelji na podrobnih pravilih,

postopkih, kontrolnih seznamih in standardiziranih procesih, ki omejujejo način izvajanja nalog. Čeprav je namen takšne kontrole zmanjšati verjetnost človeških napak z večjo predvidljivostjo vedenja, so raziskave pokazale, da lahko ustvarijo tudi nove ranljivosti (in s tem tveganja), saj povečajo časovni pritisk in kognitivno obremenitev ali spodbujajo obvodne rešitve pri delu, kadar se postopki zdijo preveč togi. V skladu s tem smo se osredotočili na tri oblike tveganega vedenja ljudi: i) spodrsljaji in napake, ki predstavljajo nenamerne napake, povezane z pozornostjo; ii) rutinske kršitve, ki se nanašajo na običajne namerne bližnjice pri spoštovanju pravil; in ii) izjemne kršitve, ki se nanašajo na namerna odstopanja od pravil, ki se pojavijo kot odziv na situacijske pritiske. Analizirali smo, kako so strogi sistemi kontrole rezultatov in kontrole dejanj, skupaj s kulturo tveganja, interaktivno uporabo obvladovanja tveganj in samokontrolo, povezani s pogostostjo vsake od treh kategorij tveganega vedenja.

V teoretičnem okviru smo združili spoznanja iz področij managerske kontrole, operativnega tveganja in kognitivne psihologije. Strogi sistemi kontrole naj bi delovali tako koristno kot škodljivo: kontrola rezultatov bi lahko izboljšala osredotočenost, vendar poveča kognitivno obremenitev, kontrola dejanj pa bi lahko preprečila kršenje pravil, vendar hkrati zmanjša notranjo motivacijo, če se izvaja (pre)strogo. Skladno z literaturo, smo samokontrolo opredelili kot osrednji psihološki mehanizem, ki odraža sposobnost zaposlenih, da uravnavajo impulze, ohranjajo pozornost in upoštevajo vedenjske standarde. Na podlagi literature smo postavili hipotezo, da visoka samokontrola zmanjšal vse tri vedenjske rezultate (t.j. spodrsljaji in napake, rutinske kršitve pravil, izjemne kršitve pravil). Poleg tega smo pričakovali, da bo kultura tveganja, ki odraža skupne norme in pričakovanja glede odgovornega ravnanja, spodbujala previdno vedenje in okrepila samokontrolo. Interaktivna uporaba obvladovanja tveganj, ki se nanaša na učenje usmerjene razprave o informacijah o tveganjih, naj bi skladno s teorijo okrepila kulturo tveganja, saj bi pričakovanja glede odgovornega ravnanja postala bolj izrazita. Na podlagi takšnega konceptualnega okvira smo razvili hipoteze o neposrednih, posrednih in moderacijskih učinkih med omenjenimi konstrukti.

Empirično raziskavo smo izvedli v isti srednje veliki banki, ki smo jo proučevali kvalitativno, vendar se je kvantitativna analiza osredotočila na osebje, ki je v neposrednem stiku s strankami, ter operativno osebje v petih največjih poslovalnicah banke. Vsi zaposleni v teh poslovalnicah, razen direktorjev poslovalnic, so bili povabljeni k sodelovanju. Podatki so bili zbrani s spletno anketo, izvedeno med 18. septembrom 2025 in 30. oktobrom 2025, ki je prinesla 150 uporabnih odgovorov iz ciljne populacije 216 oseb. Za oceno treh modelov smo uporabili metodo strukturnega modeliranja najmanjših kvadratov (PLS-SEM): prvi model je preučeval spodrsljaje in napake v povezavi s strogo kontrolo rezultatov, drugi je preučeval rutinske kršitve v povezavi s strogo kontrolo dejanj, tretji pa je preučeval izjemne kršitve v povezavi s strogo kontrolo dejanj. V vseh modelih smo samokontrola obravnavali kot osrednji mediacijski konstrukt, kulturo tveganja in interaktivno uporabo obvladovanja tveganj pa smo vključili kot kontekstualna (moderacijska) dejavnika. Lastnosti merskega

modela smo ocenili z uporabo meril zanesljivosti, konvergentne veljavnosti in diskriminantne veljavnosti, vsi reflektivni konstrukti pa so izpolnili priporočene vrednosti.

Prvi model je preučeval spodrsljaje in napake. Stroga kontrola rezultatov je bila statistično značilno negativno povezana s spodrsljaji in napakami, kar potrjuje njihovo pričakovano (in nameravano) vlogo pri zmanjševanju nenamernih napak. Samokontrola je bila prav tako statistično značilno negativno povezana s spodrsljaji in napakami, kar kaže na njen pomen kot vedenjskega zaščitnega mehanizma pred operativnimi tveganji. V nasprotju s pričakovanji, da zahtevni cilji krepijo notranjo disciplino, v raziskavi nismo ugotovili statistično značilnega učinka stroge kontrola rezultatov na samokontrolo. Iz rezultatov tudi sledi, da kultura tveganja ne zmanjša neposredno pogostosti spodrsljajev in napak, vendar smo identificirali statistično značilen pozitiven učinek na samokontrolo, kar posledično zmanjša pogostost napak. Interakcija med kulturo tveganja in strogo kontrolo rezultatov statistično značilno okrepi samokontrolo in preko tega pogostost spodrsljajev in napak, ne vpliva pa statistično značilno neposredno na njihovo pogostost. Za interaktivno uporabo obvladovanja tveganj v tem modelu nismo identificirali nobenega statistično značilnega učinka.

Drugi model se je osredotočil na rutinske kršitve. Za strogo kontrolo dejanj proti pričakovanjem nismo našli statistične potrditve učinka niti na zmanjšanje rutinskih kršitev niti na zmanjšanje samokontrole, kar kaže, da podrobnejši postopki in pravila ne odvračajo zaposlenih od uporabe običajnih rutinskih bližnjic. Samokontrola je statistično značilno negativno povezana z rutinskimi kršitvami, kar kaže, da so zaposleni z močnejšo sposobnostjo samokontrole manj nagnjeni k takšnemu ravnanju. Kultura tveganja tudi v tem modelu statistično značilno pozitivno krepi samokontrolo in tako posredno zmanjšuje rutinske kršitve, vendar nima statistično značilnega neposrednega učinka. Za interaktivno uporabo obvladovanja tveganj nismo našli nobenega statistično značilnega učinka, ravno tako za moderacijske učinke stroge kontrole nad dejanji. Rutinske kršitve pravil se tako zdijo relativno odporne na formalno zaostrovanje pravil in postopkov, namesto tega pa ima nanje močnejši vpliv notranja samoregulacija vedenja, podprta z močno kulturo tveganja.

Tretji model je preučeval izjemne kršitve. Stroga kontrola dejanj je bila statistično značilno negativno povezana z izjemnimi kršitvami in predstavlja najmočnejši neposreden učinek kontrole od vseh treh modelov. Za tovrstno kontrolo pa nismo našli pričakovanega statično značilnega učinka na samokontrolo. Tudi v tem modelu smo potrdili pričakovan statistično značilen negativen učinek samokontrole na izjemne kršitve, kultura tveganja pa je statistično značilno okrepila samokontrolo, vendar ni neposredno zmanjšala izjemnih kršitev. Posredni negativni učinek kulture tveganja na pogostost izjemnih kršitev pravil se je statistično značilno pokazal skozi njen vpliv na samokontrolo. Podobno kot v drugih dveh modelih interaktivna uporaba ni statično značilno prispevala k pojasnjevanju. rezultati nakazujejo, da so izjemne kršitve pravil povezane tako s strogimi postopki in pravili kot tudi z notranjo vedenjsko samodisciplino.

Skupaj so rezultati kvantitativne raziskave pokazali, da se je samokontrola dosledno izkazala kot edini konstrukt, ki je znatno zmanjšal vse tri vrste tveganega vedenja. Kultura tveganja ni neposredno zmanjšala tveganega vedenja, vendar je okrepila samokontrolo, kar je zmanjšalo spodrsljaje in napake, rutinske kršitve in izjemne kršitve. Stroga kontrola rezultatov je neposredno zmanjšala spodrsljaje in napake, vendar ni okrepila samokontrole. Stroga kontrola dejanj je neposredno zmanjšala izjemne kršitve, vendar ni bila učinkovita pri rutinskih kršitvah. Zlasti za rutinske kršitve se zdi, da jih je težko obvladovati s formalnimi poostritvami pravil, ker nanje vpliva (preko vedenjskega mehanizma) predvsem samokontrola. Interaktivna uporaba obvladovanja tveganj ni imela pomembnih učinkov v nobenem od modelov.

Naša študija je s tem pokazala, da tveganje, povezano z ljudmi, ni homogeno, ampak vsebuje različne vedenjske kategorije, ki imajo različne organizacijske antecedente. Rezultati nakazujejo, da samo dodajanje novih pravil ali poostritev pričakovanj glede uspešnosti ne zmanjša enotno vedenjskega tveganja. Namesto tega je bila učinkovitost kontrol odvisna od kulturnega konteksta tveganj in od sposobnosti zaposlenih za samokontrolo. Ugotovitve so pokazale, da splošni odzivi na tvegane dogodke, kot je dodajanje postopkov, morda ne rešijo temeljnih vedenjskih dejavnikov in lahko povečajo kompleksnost, ne da bi izboljšali zanesljivost kontrol. Učinkovitejši pristop bi zahteval uskladitev formalnih kontrol s kulturnimi normami, ki podpirajo samokontrolo, in prilagajanje kontrolnih strategij specifičnim oblikam vedenja, ki prispevajo k operativnemu tveganju.

Rezultate raziskave je potrebno interpretirati tudi v luči njenih omejitev. Študija je temeljila na samoporočanju in subjektivnem merjenju konstruktov, kljub uporabi uveljavljenih in validiranih merskih instrumentov (lestvic) te morda niso zajele celotne kompleksnosti konstruktov. Vzorec respondentov izhaja iz ene same organizacije, kar omejuje splošno veljavnost sklepov. Kot velja za kvantitativne pristope na splošno, ocenjeni modeli predstavljajo poenostavljeno vedenjsko sliko s poudarkom na izbranih konstruktih, kar pomeni, da obstaja možnost vpliva drugih, nevključenih spremenljivk. prečni prerez pa ni omogočal močne vzročne sklepe. Te omejitve so nakazale tudi smernice za prihodnje raziskave, kot so na primer longitudinalni modeli, ponovitev v drugih organizacijskih kontekstih in preučitev dodatnih organizacijskih dejavnikov, kot so slog vodenja ali etična klima.

Kljub njenim omejitvam so ugotovitve raziskave omogočile bolj poglobljeno in natančnejše razumevanje vpliva, ki ga imajo sistemi managerske kontrole na vedenjske dejavnike operativnega tveganja. V celoti gledano smo v naši študiji potrdili, da strogi sistemi kontrole delujejo kot dvorezni mehanizmi: zmanjšujejo nekatere tvegane oblike vedenja, vendar so učinkoviti le v določenih organizacijskih in kulturnih pogojih. Kultura tveganja je dosledno krepila samokontrolo, samokontrola pa je zmanjšala vse preučene oblike tveganega vedenja, medtem ko interaktivna uporaba obvladovanja tveganj pri tem ni imela pomembne vloge. Z opredelitvijo samokontrole kot osrednjega mediacijskega mehanizma med sistemi managerske kontrole in tveganim vedenjem ter z razlikovanjem med organizacijskimi potmi,

ki vodijo do nenamernih napak, namernih rutinskih bližnjic pri upoštevanju pravil ter namernih kršitev v izjemnih primerih, je študija poglobila razumevanje izvora nekaterih operativnih tveganj v bančništvu, hkrati pa nadgradila literaturo s področja managerske kontrole glede vedenjskih posledic kontrole.

Appendix 2: Search strings used and results for databases included in the literature review

DATABASE	SEARCH STRING
Science Direct	management control systems MCS OR performance measurement systems AND control problems AND dysfunctional behavior management control systems MCS OR performance measurement systems AND data manipulation AND gaming behavior management control systems MCS OR behavioral control AND control problems AND dysfunctional behavior management control systems MCS OR organizational rules AND data manipulation AND gaming behavior management control systems MCS OR staff control AND control problems AND dysfunctional behavior management control systems OR human resource management AND data manipulation AND gaming behavior management control systems MCS OR organizational culture AND control problems AND dysfunctional behavior **RESULTS: 4869, after data filters 356**
Scopus-Elsevier	TITLE-ABS-KEY (management control system* OR performance measurement system*) AND control problem* AND dysfunctional behavior*) TITLE-ABS-KEY (management control system*OR performance measurement system*) AND data manipulation AND gaming behavior) TITLE-ABS-KEY (management control system* OR behavioral control*) AND control problem* AND dysfunctional behavior*) TITLE-ABS-KEY (management control system* OR organizational rule*) AND data manipulation AND gaming behavior) TITLE-ABS-KEY (management control system*OR staff control* OR personnel control*) AND control problem* AND dysfunctional behavior*) TITLE-ABS-KEY(management control system* OR human resource management) AND data manipulation AND gaming behavior) TITLE-ABS-KEY(management control system* OR organizational culture) AND control problem* AND dysfunctional behavior*) **RESULTS: 3745, after data filters 48**
Web of Science	TS=((management control system* OR performance measurement system*) AND control problem* AND dysfunctional behavior*) AND LANGUAGE:(English) TS=((management control system* OR performance measurement system*) AND data manipulation AND gaming behavior) AND LANGUAGE:(English) TS=((management control system*OR behavioral control*) AND control problem* AND dysfunctional behavior*) AND LANGUAGE:(English) TS=((management control system* OR organizational rule*) AND data manipulation AND gaming behavior) AND LANGUAGE:(English) TS=((management control system* OR staff control*OR personnel control*) AND control problem* AND dysfunctional behavior*) AND LANGIAGE:(English) TS=((management control system* OR human resource management) AND data manipulation AND gaming behavior) AND LANGIAGE:(English) TS=((management control system* OR organizational culture)

	AND control problem* AND dysfunctional behavior*) AND LANGUAGE:(English) **RESULTS: 3996, after data filters 78**
JSTOR	(management control systems OR performance measurement systems) AND control problems AND dysfunctional behavior (management control systems OR performance measurement systems) AND data manipulation AND gaming behavior (management control systems OR organizational rules) AND data manipulation AND gaming behavior (management control systems OR staff control OR personnel control) AND control problems AND dysfunctional behavior (management control systems OR human resource management) AND data manipulation AND gaming behavior (management control systems OR organizational culture) AND control problems AND dysfunctional behavior **RESULTS: 4422, after data filters 113**
Taylor & Francis	[All: management control systems MCS] OR [All: performance management systems] AND [All: control problems] AND [All: dysfunctional behavior] [All: management control systems MCS] OR [All: performance management systems] AND [All: and data manipulation] AND [All: gaming behavior] All: management control systems MCS] OR [All: behavioral control] AND [All: control problems] AND [All: dysfunctional behavior] [All: management control systems MCS] OR [All: organizational rules] AND [All: control problems] AND [All: and dysfunctional behavior] [All: management control systems MCS] OR [All: staff control] AND [All: control problems] AND [All: dysfunctional behavior] [All: management control systems MCS] OR [All: human resource management] AND [All: data manipulation] AND [All: gaming behavior] [All: management control systems MCS] OR [All: organizational culture] AND [All: control problems] AND [All: dysfunctional behavior] **RESULTS: 4478, after data filters 97**
Total	**Initial search results: 21, 510;** **After data filters (peer-reviewed journals, English language, and subject areas of management, accounting, business, and organizational studies): 692 records;** **After removing duplicates and data cleaning: 158 records**

Source: Own work.

Appendix 3: Thematic analysis of studies included in the literature review

CONTROL TYPE	STUDIES (in chronological order)	CONTROL PROBLEM CODINGS
Result Controls **44 studies**	Ridgway (1956); Becker & Green (1962); Schiff & Lewin (1970); Hopwood (1972); Onsi (1973); Otley (1978); Merchant (1981); Hirst (1981); Hirst (1983); Young (1985); Brownell & Hirst (1986); Merchant (1990); Dunk (1993); Grizzle (2002); Schweitzer et al. (2002); Jensen (2003); Hansen & Van der Stede (2004); Hussain (2005); Vakkuri & Meklin (2006); Hunton et al. (2008); Elmassri & Harris (2011); Gneezy et al. (2011); Franco-Santos et al. (2012); Adnan et al. (2013); Bourmistrov & Kaarbøe (2013); Jacobs et al. (2013); Libby & Lindsay (2013); Cheng & Coyte (2014); Speklé & Verbeeten (2014); De Baerdemaeker & Bruggeman (2015); Goebel & Weißenberger (2016); Sponem & Lambert (2016); Cugueró-Escofet & Rosanas (2017); Franco-Santos & Otley (2018); Siverbo et al. (2019); Linder et al. (2020); Van der Stede (2000); Van der Stede (2001); Carroll & Marginson (2021); Heitger et al. (2021); Khajehnejad & Linder (2022); Deore et al. (2023); Lopez-Valeiras et al. (2024)	Gaming (50%), slack (33%), data manipulation (41%); unethical conduct (41%); tunnel vision (9%), myopia (14%), short-termism (34%); motivational crowding-out (25%); stress (16%), tension (25%); ritualistic (5%) or symbolic (2%) use
Action Controls **6 studies**	Abernethy & Stoelwinder (1995); Adler & Borys (1996); Reason et al. (1998); Christ et al. (2012); Jurkiewicz & Giacalone (2014); Lagios et al. (2023)	Alienation (33%), demotivation and reduced initiative (50%); routine or rule violations (33%); unethical behaviors (33%); role conflict (33%)
Personnel Controls **6 studies**	Riyono (1998); MacLane & Walmsley (2010); MacKenzie et al. (2011); Campbell (2012); Abernethy et al. (2015); Strauss (2015)	Disengagement (50%); workplace deviance (33%), unethical behavior (33%); cultural misfit (33%); misaligned motivation and effort (67%)
Cultural Controls **10 studies**	Payne (1980); Daley et al. (1985); Weaver et al. (1999); Langfield-Smith & Smith (2003); Appelbaum & Shapiro (2006); Van Fleet & Griffin (2006); Kaptein (2011), Tayler & Bloomfield (2011); Marc & Peljhan (2019); Malmi et al. (2022)	Norm confusion (50%), ethical drift (40%); symbolic ethics (20%); values (30%) misalignment (40%); peer pressure (50%), silence (10%); cultural rigidity (20%)
Multiple Controls (Joint Use) **11 studies**	Cravens et al. (1993); Ramaswami (1996); Sorauren (2000); Alvesson & Kärreman (2004); Cravens et al. (2004); Malmi & Brown (2008); Madhani (2016); Fiolleau et al. (2017); Goebel & Weißenberger (2017); Bedford, D. S. (2020); Bellora-Bienengräber et al. (2022);	Short-term opportunism (27%); goal incongruence, confusion (55%), overload of measures (18%); underenforcement (45%); moral disengagement (45%)

To be continued

Appendix 3: Thematic analysis of studies included in the literature review (cont.)

CONTROL TYPE	STUDIES (in chronological order)	CONTROL PROBLEM CODINGS
Design & Use Misalignments **18 studies**	Tannenbaum (1962); Baliga & Jaeger (1984); Eisenhardt (1985); Anderson & Oliver (1987); Jaworski (1988); Davila (2000); Shields et al. (2000); Duarte et al. (2018); Hussain & Gunasekaran (2002); Chenhall (2003); Rosanas & Velilla (2005); Henri (2006); Litzky et al. (2006); Ferreira & Otley (2009); Liu et al. (2015); Willert et al. (2017); Suh (2019); Abubakar et al. (2022)	Conflicting signals (17%); stress, frustration (39%); gaming (39%); short-termism, narrow focus (28%); demotivation, disengagement, low effort (67%); fraud, unethical behavior (6%); workplace resistance, deviance (22%); rigidity, suppressed initiative (50%)
Total: 95		

Notes: Percentages are calculated based on the number of studies within each theme; control problem codes are not mutually exclusive.

Source: Own work

Appendix 4: Overview of all reviewed studies and identified dysfunctional behaviours

Results control	Gaming and mispreporting (30)	Unethical conduct (18)	Tunnel vision (16)	Crowding-out intrinsinc motivation (11)	Psychological stress and tension (15)	Ritualistic use (3)
Adnan, A. A., Jamil, C. Z. M., & Nor, M. I. (2013)	✓	✓	✓			
Becker, S., & Green, D., Jr. (1962)	✓			✓	✓	
Bourmistrov, A., & Kaarbøe, K. (2013)	✓		✓			✓
Brownell, P., & Hirst, M. (1986)					✓	
Carroll, E., & Marginson, D. (2021)	✓				✓	
Cheng, M. M., & Coyte, R. (2014)				✓		
Cugueró-Escofet, N., & Rosanas, J. M. (2017)	✓	✓	✓	✓		
De Baerdemaeker, J., & Bruggeman, W. (2015)	✓					
Deore, A., Gallani, S., & Krishnan, R. (2023)		✓				
Dunk, A. S. (1993)	✓	✓				
Elmassri, M., & Harris, E. (2011)	✓	✓			✓	
Franco-Santos, M., & Otley, D. (2018)	✓	✓				
Franco-Santos, M., Lucianetti, L., & Bourne, M. (2012)	✓	✓	✓	✓		
Gneezy, U., Meier, S., & Rey-Biel, P. (2011)			✓	✓		
Goebel, S., & Weißenberger, B. E. (2016)	✓	✓	✓	✓	✓	
Grizzle, G. A. (2002)	✓	✓				
Hansen, S. C., & Van der Stede, W. A. (2004)			✓		✓	
Heitger, A. A., Heitger, D. L., & Heitger, L. E. (2021)	✓	✓			✓	
Hirst, M. K. (1981)		✓			✓	
Hirst, M. K. (1983)		✓			✓	
Hopwood, A. G. (1972)	✓	✓	✓		✓	
Hunton, J. E., Mauldin, E. G., & Wheeler, P. R. (2008)			✓	✓	✓	
Hussain, M. M. (2005)						✓

Results control (continued)	Gaming and mispreporting (30)	Unethical conduct (18)	Tunnel vision (16)	Crowding-out intrinsinc motivation (11)	Psychological stress and tension (15)	Ritualistic use (3)
Jacobs, G., Belschak, F. D., & Den Hartog, D. N. (2013)		✓				
Jensen, M. C. (2003)	✓	✓				
Khajehnejad, S., & Linder, S. (2022)	✓	✓				
Lau, C. M., & Eggleton, I. R. C. (2004)	✓					
Libby, T., & Lindsay, R. M. (2013)	✓					
Linder, S., Leca, B., Zicari, A., & Casarin, V. (2020)				✓	✓	
Lopez-Valeiras, E., Gomez-Conde, J., Naranjo-Gil, D., & Malagueño, R. (2024)				✓	✓	
Merchant, K. A. (1981)				✓	✓	
Merchant, K. A. (1990)	✓	✓	✓			
Onsi, M. (1973)	✓	✓				
Otley, D. T. (1978)	✓	✓	✓		✓	
Ridgway, V. F. (1956)	✓					
Schiff, M., & Lewin, A. Y. (1970)	✓	✓				
Schweitzer, M. E., Ordóñez, L. D., & Douma, B. (2002)		✓				
Siverbo, S., Cäker, M., & Åkesson, J. (2019)	✓		✓	✓		
Speklé, R. F., & Verbeeten, F. H. M. (2014)	✓	✓				
Sponem, S., & Lambert, C. (2016)	✓		✓			✓
Vakkuri, J., & Meklin, P. (2006)	✓	✓	✓			
Van der Stede, W. A. (2000)	✓		✓			
Van der Stede, W. A. (2001)			✓			
Young, S. M. (1985)	✓					

Action control	Alienation and demotivation (3)	Routine violations and workarounds (2)	Unethical behaviors (3)	Role conflict (2)
Abernethy, M. A., & Stoelwinder, J. U. (1995)				✓
Adler, P. S., & Borys, B. (1996)	✓	✓	0	
Christ, M. H., Emett, S. A., Summers, S. L., & Wood, D. A. (2012)	✓		✓	
Lagios et al. (2023)	✓			✓
Jurkiewicz, C. L., & Giacalone, R. A. (2014)			✓	
Reason, J., Parker, D., & Lawton, R. (1998)		✓		

Personnel control	Mistrust, passivity, disengagement (3)	Workplace deviance, uunethical behavior (3)	Cultural misfit (3)	Misaligned motivation and effort (4)
Abernethy, M. A., Dekker, H. C., & Schulz, A. K.-D. (2015)	✓			✓
Campbell, D. (2012)	✓		✓	✓
MacLane, C. N., & Walmsley, P. T. (2010)		✓		✓
Riyono, B. (1998)			✓	
Strauss, L. (2015)	✓	✓		✓
MacKenzie, C., Garavan, T. N., & Carbery, R. (2011)		✓	✓	

Cultural control	Norm confusion and ethical drift (9)	Symbolic ethics (2)	Value misalignment, resistance (6)	Peer pressure and silence (5)	Cultural rigidity (2)
Appelbaum, S. H., & Shapiro, B. T. (2006)	✓	✓	✓		
Daley, L. A., Jiambalvo, J., Sundem, G. L., & Kondo, Y. (1985)			✓	✓	
Kaptein (2011)	✓		✓	✓	
Langfield-Smith, K., & Smith, D. (2003)	✓				
Malmi, T., Kolehmainen, K., & Granlund, M. (2022)	✓		✓		✓
Marc, M., & Peljhan, D. (2019)	✓				✓
Payne, S. L. (1980)	✓			✓	
Tayler, W. B., & Bloomfield, R. J. (2011)	✓		✓	✓	

Cultural control (continued)	Norm confusion and ethical drift (9)	Symbolic ethics (1)	Value misalignment, resistance (5)	Peer pressure and silence (5)	Cultural rigidity (2)
Van Fleet, D. D., & Griffin, R. W. (2006)	✓			✓	
Weaver, G. R., Treviño, L. K., & Cochran, P. L. (1999)	✓	✓	✓		

Joint control	Short-term focus, opportunism (3)	Goal confusion, overload of measures (6)	Underenforcement and ethical drift (5)	Moral disengagement (5)
Alvesson, M., & Kärreman, D. (2004)			✓	✓
Bedford, D. S. (2020)		✓		
Bellora-Bienengräber, L., Radtke, R. R., & Widener, S. K. (2022)			✓	✓
Cravens, D. W., Ingram, T. N., LaForge, R. W., & Young, C. E. (1993)		✓		
Cravens, D. W., Lassk, F. G., Low, G. S., Marshall, G. W. & Moncrief, W. C. (2004)		✓		
Fiolleau, K., Libby, T., & Thorne, L. (2017)		✓	✓	✓
Goebel, S., & Weißenberger, B. E. (2017)	✓		✓	✓
Madhani, P. M. (2016)	✓			
Malmi, T., & Brown, D. A. (2008)		✓		
Ramaswami, S. N. (1996)	✓			
Sorauren, I. F. (2000)		✓	✓	✓

Source: Own work

Design and use of control	Confusion, conflicting signals (3)	Stress, frustration (7)	Gaming (7)	Short-termism, narrow focus (5)	Demotivation, disengagement, low effort (12)	Fraud, workplace resistance, deviance (5)	Rigidity, suppressed initiative and creativity (9)
Abubakar, N. A., Baird, K., & Su, S. (2022)					✓		✓
Anderson, E., & Oliver, R. L. (1987)			✓	✓	✓		
Baliga, B. R., & Jaeger, A. M. (1984)			✓		✓		✓
Chenhall, R. H. (2003)		✓				✓	✓
Davila, T. (2000)	✓			✓	✓		✓
Eisenhardt, K. M. (1985)					✓		✓
Ferreira, A., & Otley, D. (2009)	✓		✓				
Henri, J.-F. (2006)				✓	✓		✓
Hussain, M. M., & Gunasekaran, A. (2002)	✓				✓		
Jaworski, B. J. (1988)		✓	✓		✓		
Litzky, B. E., Eddleston, K. A., & Kidder, D. L. (2006)		✓	✓			✓	
Liu, X. K., Wright, A. M., & Wu, Y. J. (2015)						✓	
Duarte, H., Palermo, O. A., & Arriaga, P. (2018)		✓				✓	✓
Rosanas, J. M., & Velilla, M. (2005)			✓	✓	✓		
Shields, M. D., Deng, F. J., & Kato, Y. (2000)		✓	✓		✓		
Suh, W. (2019)				✓	✓		✓
Tannenbaum, A. S. (1962)		✓			✓	✓	
Willert, J., Israelsen, P., Rohde, C., & Toldbod, T. (2017)		✓					✓

Source: Own work

Appendix 5: Overview of reviewed studies by domains and coding by analytical categories

Nr.	Author(s)	Domain	Analytical categories				
			Design & use	Rule and procedure	Structural and organizational	Incentive-related	Cultural and behavioural
1	Abdul Rahim, N. F., Ahmed, E. R., & Faeeq, M. K. (2018).	ORM	X				
2	Abdul-Rahman, A. & Yazid, Z. (2015)	ORM	X				
3	Acrey, J. C., McCumber, W. R., & Nguyen, T. H. T. (2011).	Incentives				X	
4	Al-Amri, K., & Davydov, Y. (2016)	ORM			X		
5	Ashraf, B. N., Zheng, C., & Arshad, S. (2016).	Culture					
6	Bardoscia, M., & Bellotti, R. (2012).	ORM		X			
7	Basel Committee on Banking Supervision. (1998)	Regulation					
8	Berger, A. N., Curti, F., Mihov, A., & Sedunov, J. (2022).	ORM	X				
9	Braumann, E., Grabner, I., & Posch, A. (2020).	RMS and MCS					X
10	Butler, T., & Brooks, R. (2024).	ORM			X	X	X
11	Carpenter, N. C., Whitman, D. S., & Amrhein, R. (2021).	People risk					X
12	Carretta, A., Fiordelisi, F., Schwizer, P., & Stentella Lopes, F. (2024).	People risk				X	X
13	Cerasi, V., & Oliviero, T. (2015).	Incentives			X	X	
14	Chanon, R. D., Habahbeh, L., Klumpes, P. J. M., & Mann, S. (2025).	Regulation					X
15	Chernobai, A., Ozdagli, A., & Wang, J. (2020).	ORM	X				
16	Cohn, A., Fehr, E., & Maréchal, M. A. (2014).	Culture				X	X
17	Cornwell, N., Bilson, C., Gepp, A., Stern, S., & Vanstone, B. J. (2023).	ORM			X		
18	Deschamps, C. (2019).	RMS and MCS	X				
19	Edwards, J., & Wolfe, S. (2004).	Regulation					X

20	Faugère, C., & Stul, O. (2021).	ORM					X
21	Financial Stability Board (2014).	Culture					
22	Florio, C., & Leoni, G. (2017).	ORM	X	X			
23	Frese, M., & Keith, N. (2015).	Culture					X
24	Gontarek, W. (2016).	Culture			X		
25	Göstl, P., & Schwaiger, W. S. A. (2016).	RMS and MCS	X				
26	Gurd, B., & Helliar, C. (2017).	RMS and MCS		X	X		X
27	Hall, M., Mikes, A., & Millo, Y. (2015).	Risk management	X				
28	Hartman, F., & Slapničar, S. (2007).	Incentives			X		
29	Holland, J. (2019).	Culture					X
30	Houston, J. F., & James, C. (1995).	Incentives				X	
31	Kunz, J., & Heitz, M. (2021).	Culture					X
32	Laguecir, A., & Leca, B. (2022).	ORM					X
33	Liang, L., Dai, T., & Zhang, M. (2024).	People risk				X	
34	Lim, C. Y., Woods, M., Humphrey, C., & Seow, J. L. (2017).	RM	X	X	X		
35	Lui, A. (2015).	Culture					X
36	Mabwe, K., Ring, P., & Webb, R. (2022).	ORM		X	X		
37	Marc, M., Arena, M., & Peljhan, D. (2023).	RMS and MCS	X				X
38	Mikes, A. (2009).	Culture	X				X
39	Mikes, A. (2011).	Culture	X				
40	Molamohamadi, Z., Samani, M. A., & Karimi, M. (2024).	RM	X				
41	Moosa, I. A. (2017).	Regulation		X		X	
42	Muermann, A., & Oktem, U. (2002).	ORM	X				
43	Posch, A. (2020).	RMS and MCS				X	
44	Power, M. (2005).	ORM	X	X			
45	Power, M. (2009).	RMS and MCS	X	X		X	X
46	Rad, A. (2016).	RMS and MCS	X	X	X		

47	Ranjan, R. (2025).	RM		X			
48	Rikhardsson, P., Rohde, C., Christensen, L., & Batt, C. E. (2021).	RMS and MCS		X			
49	Ringgaard, A., Bukh, P. N., & Sandalgaard, N. (2025).	RMS and MCS	X		X	X	
50	Sabanova, J., & Kudinska, M. (2022).	Regulation		X	X		
51	Sabanova, J., & Kudinska, M. (2023).	People risk					X
52	Sabanova, J., & Kudinska, M. (2024).	Regulation					X
53	Siaw Ofori, B., Padi, A., & Musah, A. (2025).	ORM			X		
54	Slapničar, S., Axelsen, M., & Eulerich, M. (2025).	ORM	X				
55	Soin, K., & Collier, P. (2013).	RMS and MCS	X	X	X		
56	Tran, T.-V., Lepistö, S., & Järvinen, J. (2021).	Incentives				X	
57	Wright, J. F. (2018).	People risk			X		
58	Xu, Y., Pinedo, M., & Xue, M. (2017).	ORM	X				
59	Yokoi-Arai, M. (2003).	Regulation			X		

Source: Own Work

Notes:

"ORM": Operational RM;

"RMS and MCS": RM Systems and Management Control Systems;

"RM": Risk Management

Appendix 6: Participant information and Consent Form

PARTICIPANT INFORMATION SHEET AND CONSENT FOR

You are invited to voluntarily participate in the research: “The Impact of Management Control Systems on Managing Operational Risk in Banks”.

What is the purpose of the research?

You are invited to participate in doctoral research titled "The Impact of Management Control on Managing Operational Risk in Banks." Before you decide to participate in this study, it is important that you understand why the research is being done and what it will involve. Please read the following information carefully. Please ask the researcher if there is anything that is not clear or if you need more information.

The purpose of this study is to identify and explain the relationship between Management Control Systems and Operational Risk Management, with specific emphasis on the role of human errors in this context. This study is undertaken by Edona Haxhiu, a doctoral candidate in the Faculty of Economics, University of Ljubljana and is supervised by the esteemed Professor Dr. Mojca Marc.

What will be my role in the research?

If you choose to participate, your role will involve the following tasks:

- Participating in an initial interview to discuss your experiences and insights regarding management control systems and operational risk management in the banking sector.
- Providing input and feedback on how management control systems are implemented and utilized within your organization to mitigate human errors and operational risks.

What are the benefits of my participation?

You will not receive any compensation for taking part in the research. Your participation in this research will contribute to a better understanding of the relationship between management control systems and operational risk management in the banking sector. Additionally, by sharing your experiences and perspectives, you may gain insights into best practices and strategies for enhancing risk management practices within your organization. Based on the findings of this research, your bank will receive a comprehensive report, and implementation strategies to improve the working conditions with respect to operational risk management.

What are the possible risks associated with my participation in the research?

Participation in this research does not entail any risks.

Can I decide not to participate in the study?

Your participation in the research is entirely voluntary, and you may withdraw at any time by notifying the researcher in writing or verbally of your decision, up to when the researcher begin the analysis of the data. If you choose to withdraw from the study, all information you provided during the interview will be withdrawn from the study and deleted.

What will happen to my personal data?

We will treat all your information confidentially. We will do everything we can to protect your privacy. Your experiences and demographic information will be stored under a unique research code. This code will facilitate the connection between questions without linking them directly to your identity. Any summary interview content, or direct quotations from the interview, that are made available through academic publications will be anonymized so that you cannot be identified. Your identity will not be revealed under any circumstances.

How my information will be used?

This research is being conducted as partial completion of my PhD degree requirement and will be used for my PhD dissertation. The information that you and other participants provide will be analyzed to answer the key research questions and meet the study objectives. The research findings will be presented in a thesis required for completion of my PhD degree, and may also be used for conference publications, presentations, and published in academic journals. It is important to note that in all forms of publication, the identities of both the organization and individual participants will not be disclosed, and it will always remain confidential.

How interviews will be conducted?

- To maintain the essence of your words for the research, the interview will be audio-recorded, and a transcript will be produced.
- You will be sent the transcript and given the opportunity to correct any factual errors.
- All data and information derived from the interview will be stored on a password-protected computer by the researcher (Edona Haxhiu).
- The transcript of the interview will be analysed by the researcher (Edona Haxhiu).
- All individual identification will be removed from the hard copy of the transcript.
- Participants identity and confidentiality will be concealed using coding procedures.

Where can I get more information?

If you have any additional questions, you can contact the researcher, Edona Haxhiu (edona.haxhiuu@gmail.com)

VOLUNTARY AND INFORMED CONSENT FORM

I was informed in writing and orally about the purpose and goals of the research titled:" The Impact of Management Control Systems on Managing Operational Risk in Banks".

I know how my research safety will be ensured and that I can ask for and receive additional information from the researcher at any time. It was also explained to me that I could withdraw my consent without having to justify the withdrawal.

Consent and Conditions of Consent

I have read and understand the information provided above, and hereby consent to participate in this research under the following conditions:

I consent to the interview being audio recorded.	☐ Yes	☐ No
I wish to review the notes, transcripts, or other data collected during the research pertaining to my participation.	☐ Yes	☐ No
I agree to be quoted directly.	☐ Yes	☐ No
I agree to be quoted directly if my name is not published and only a code is used.	☐ Yes	☐ No

By signing, I voluntarily confirm my willingness to participate in the research. I also allow my demographic and experience information to be used in an anonymized form for the academic research purposes.

I am signing the form in the presence of the researcher.

Signature: _____

Date: _____

Name and surname of the researcher: _____

Signature of the researcher: _____

Date: _____

Appendix 7: Interview protocol

Interview Questions:

General Questions: Participant Background

1. What are your current and previous positions in the organization?

2. How long have you been employed here?

3. What are your formal responsibilities regarding risk management?

Specific Questions: Operational Risk Management

1. Can you provide an overview of the operational risk management framework currently in place within our bank?

2. What are the top operational risks in your bank?

3. When did your bank start to collect data for operational risk events?

4. How is operational risk management integrated into the overall risk management strategy of the bank?

5. How does the bank assess and quantify its exposure to operational risk across different business lines and functions?

6. What measures are in place to monitor and mitigate the exposure to operational risk effectively?

7. Can you explain the role of the people risk within the context of operational risk management?

8. How does your bank identify people risk? For example human errors?

9. How does your bank evaluate the impact of human errors?

10. What measures does your bank have in place to prevent or minimize the occurrence of human errors?

Specific Questions: Management Control Systems

1. How do you perceive the level of control for the operational risk in your bank?

2. Can you describe the types of management control systems currently in place within your bank to manage operational risks?

3. What type of management control systems are in place to manage employee behaviours

Closing questions:

1. Is there anything else you would like to share with me as it relates to operational risk management in your organization?

2. Can you recommend anyone else I can talk to in this organization concerning the issue of Operational risk?

Appendix 8: Examples of coding

This appendix provides an illustrative excerpt from the coding matrix used in the qualitative analysis. The selection demonstrates the structure and format of the coding process.

Participant ID	Transcript Excerpt /Quote	1ST Oder combined (OCF + CP) 1st-Order Combined Mechanism + Problem	2nd Order Themes	Aggregate Dimensions
INT-BM-01	"The most frequent errors that we have are errors in the description of transactions, instead of deposit is written withdrawal, then we have the allocation of funds to the wrong account.	Segment 1 Action Control + Structure Problem: “Frequent procedural errors show insufficient clarity or robustness in process design” Segment 2 Action Control + Structure Problem: “Mistyped transaction type reflects weak error-prevention mechanisms” Segment 3 Action Control + Structure Problem: “Incorrect fund allocation reveals gaps in procedural control architecture”	Personnel Capability Problem	Human Capability & Behavioral Control Problems
INT-HR-02	The performance evaluation takes at least 20 minutes for one employee, and currently it is done in simple excel form - we have the forms where the formulas are set. This is how the performance measurement and evaluation process is conducted, who has achieved the performance objectives and competencies of at least 101% enters the category to receive a reward"	Segment 1 Result Control + Structural Problem: “Manual performance evaluations create structural inefficiencies.” Segment 2 Action Control + Rigid Problem: “Excel-based, formula-locked evaluation forms constrain flexibility.” Segment 3 Action Control + Rigid Problem: “Evaluation procedures are overly formalized and outdated.” Segment 4	Structural Vulnerabilities	Design -Driven Control Problems

		Result Control + Incentive Problem: “High quantitative thresholds (101%) create motivational distortions.”		
INT-HR-02	"Currently, the way the performance evaluation is conducted is a problem. The evaluation process is still done in excel, so it is not worked directly in any special system. The data (numbers) are extracted from the system and placed in the form/template which is in excel"	Segment 1 Action Control + Structure Problem: “Performance evaluation process design is outdated and inefficient.” Segment 2 Action Control + Structure Problem: “Manual Excel-based evaluation reflects missing system integration.” Action Control + Rigid Problem: “Template-driven evaluation creates overly fixed procedures.” Personnel Control + Structure Problem: “Employee assessment depends on an inadequate manual process.” Segment 3 Action Control + Structure Problem: “Manual extraction and re-entry of data creates procedural vulnerability.”	Structural Vulnerabilities	Design -Driven Control Problems
INT-HR-02	"The threshold level is very high because it is necessary to push the employees to work harder to achieve the objectives -"90 to 100% you already get paid - you don't get bonus; 101% gets a bonus, and that bonus then varies. An average for all bank employees, excluding managerial positions, is up to two bonus salaries within the calendar year"	Segment 1 Result Control + Incentive Problem: “High performance threshold used to motivate employees” Segment 2 Result Control + Incentive Problem: “Bonus activation depends on surpassing 101% target” Segment 3 Result Control + Incentive Problem: “Bonus amount varies; average reward up to two monthly salaries”	Incentive Misalignments	Design -Driven Control Problems
INT-HR-02	"Yes, there were cases that due to inappropriate behavior, the disciplinary procedure has been initiated. We have regulations for determining	• Personnel Control + Cultural/Behavioral Problem - “Inappropriate employee behavior triggering disciplinary processes”	Cultural and Ethical Drift	Human Capability & Behavioral Control Problems

	the disciplinary procedure in the bank, which can be initiated by the board of directors, by each employee, by the leader, and by the customer"	• Action Control (no CP) - “Presence of formal disciplinary rules” • Personnel/Structure Control (no CP) - “Multiple actors authorized to initiate disciplinary procedure”		
INT-HR-02	"when the performance evaluation drops to 89%, we organize a meeting with the person who did the evaluation, with the evaluated employee, and one person in the hierarchy. In this meeting, we must see what happened, is there a subjectivism, are there any problems, are there any medical leave that impacted the performance, or are there any other issues . Only after all the circumstances are checked then the monitoring is set. There are cases when we do not set the monitoring for 30 days because we understand the situation and we all agree, and the process continues"	Segment 1 Personnel Control + Structure Problem - “Hierarchy-driven meetings triggered mechanically by evaluation thresholds.” Segment 2 Result Control + Incentive Problem -“Evaluation procedure vulnerable to subjectivism when performance drops.” Segment C Action Control + Rigid Problem - “Monitoring is imposed based on predefined rules after deviations.” Segment D Personnel Control + Cultural Problem - “Managers override monitoring rules based on shared understanding.”	Incentive Misalignments	Design -Driven Control Problems
IN-IA-03	"I am mentioning here the case of cash management, account opening, e-channels, during the audit in these processes it is identified that a control is not effective, for example in the case of exceeding cash limits, where in this case the staff failed in managing cash limit, and this is then identified as a case of operational risk and addressed as operational risk"	1. Action Control + Structure Problem: “Structural vulnerabilities across multiple processes (cash mgmt., account opening, e-channels)” 2. Action Control + Structure Problem: “Audit identifies ineffective control design/execution” 3. Personnel Control + Structure Problem: “Staff failure to manage cash limits exposes control-design weakness” 4. Action Control (Descriptive): “Issue classified through formal ORM procedures”	Structural Vulnerabilities	Design -Driven Control Problems
IN-IA-03	"in the card process, this was a single card payment option where the system was	1. Action Control + Structure Problem: “Incorrect system configuration reflects	Structural Vulnerabilities	Design -Driven Control Problems

	configured the same as for the options Master-money send and also for the VISA fast fund, where in this process there was a failure of preventive controls, improper configuration of the system, the design of control in the system by the human factor and the loss was about 100,000 Euros"	weakness in designed procedures." 2. Action Control + Structure Problem: "Preventive control failure indicates a breakdown in formal control design." 3. Personnel Control + Structure Problem: "Human factor in configuring controls results in improper control design." 4. Action & Personnel Control + Structure Problem: "Detective control not performed due to procedural and human-execution gaps." 5. Action Control + Structure Problem: "Monitoring control failure indicates weakness in ongoing control activities."		
IN-IA-03	"During the analysis of the controls, we find that the cause is Human Error, and we see that the same person made the same mistake 5 times or many people with similar positions made the same mistake . In this case, we contacted the person to understand the reason, and on the other hand, we looked at the aspect of training and saw that the person in question has not attended training for 4 years"	Action Control + Structure Problem -Human Error Problem: "Detection controls reveal recurring human-error issues" Personnel Control + Personnel Capability Problem: "Repeated mistakes indicate competence or skill gaps" Personnel Control + Behavioral Problem: "Managerial follow-up required due to behavioural deviation" Personnel Control + Training/Competence Problem: "Training gaps undermine employee capability and accuracy"	Workforce Capability and Capacity Limitaions	Human Capability & Behavioral Control Problems
IN-IA-03	Long manual processes, such as opening accounts, data entry/update, often result in operational risks and regulatory risks. Failure to adequately test the configuration/changes in	Action Control + Structure Problem: "Manual processes expose structural weaknesses in procedural design."	Structural Vulnerabilities	Design -Driven Control Problems

	the system; Failure to analyze adequately may cause operational loss. Retesting the systems to verify if the criteria originally established for an automatic process still work - is a control problem.	Personnel Control + Structure Problem: "Staff-dependent data entry creates vulnerability due to manual design." Action Control + Structure Problem: "Inadequate system-testing procedures reflect structural control gaps." Personnel Control + Structure Problem: "Staff lack or insufficient application of required testing responsibilities." Personnel Control + Structure Problem: "Analytical competence gaps weaken control effectiveness." Action Control + Structure Problem: "Automated controls require retesting due to structural weaknesses in setup."		

Source: Own work

Appendix 9: Loss Event Data 2023

Process	Step	LE type	Loss event type	LE cause	Type of loss	Loss effect	Currency	Report of facts
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The client asked to convert the money from SEK to EURO currency, but the main cashier selected wrongly the EURO instead of SEK currency.
Funds transfer	2. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The national bank transfer has been reversed because it has been processed with wrong description, the wrong beneficiaries name.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The cash has been deposited in the wrong client's account.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The main cashier processed cash deposit transaction according to client request but he put the wrong description. He didn't write the description asked by client.

To be continued

Appendix 9: Loss Event Data 20223 (cont.)

Process	Step	LE type	Loss event type	LE cause	Type of loss	Loss effect	Currency	Report of facts
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The main cashier processed again the same cash deposit transaction according to client request but he put the wrong description. He didn't write the description asked by client.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The main cashier processed again the same cash deposit transaction according to client's request but he put the wrong description. He didn't write the description asked by client.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The main cashier processed cash deposit transaction but he pressed the wrong amount.
Funds transfer	2. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The client adviser processed national outgoing money transfer, but he put the wrong description.

Appendix 9: Loss Event Data 20223 (cont.)

Process	Step	LE type	Loss event type	LE cause	Type of loss	Loss effect	Currency	Report of facts
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	USD	The client adviser processed in branch money transfer but she selected wrongly the USD instead of EUR currency.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The client asked for money withdrawal but the cashier forgot to write description and purpose of money withdraw transaction.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	GBP	The client asked for the money exchange transaction but client adviser made a mistake, due to processing the transaction with standard rate instead of processing special exchange rate.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The client asked for the money exchange transaction but client adviser made a mistake, due to processing the transaction with standard rate instead of processing special exchange rate.

Appendix 9: Loss Event Data 20223 (cont.)

Process	Step	LE type	Loss event type	LE cause	Type of loss	Loss effect	Currency	Report of facts
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The cashier wrongly deposited money in to "xxx" SHPK client's account instead of deposit in the NPT "xxx" SHPK client's account.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The cashier wrongly deposited money in to xxx SHPK 170xxx client's account instead of deposit in the xxx SHPK 170xxx client's account.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The cashier wrongly deposited money in to xxx SHPK 1700xx client's account instead of deposit in the xxx SHPK 170xxx client's account.
Funds transfer	1. Data Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The client adviser processed inter bank money transfer transaction according to client request but the it was processed with wrong description.

Appendix 9: Loss Event Data 20223 (cont.)

Process	Step	LE type	Loss event type	LE cause	Type of loss	Loss effect	Currency	Report of facts
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	CHF	The client asked to deposit cash in EUR currency but the cashier wrongly processed the transaction in CHF currency.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The main cashier processed cash deposit transaction based on client request but he credited the wrong client's account.
Funds transfer	2. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The main cashier processed municipality payment for the Company "xxx" according to client request but he put the wrong description. He didn't write the description asked by client.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	USD	The main cashier processed the cash deposit transaction according to client's request but he selected the wrong currency (USD).

Appendix 9: Loss Event Data 20223 (cont.)

Process	Step	LE type	Loss event type	LE cause	Type of loss	Loss effect	Currency	Report of facts
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	USD	The client adviser processed in branch money transfer based on client's request but he wrongly processed the transaction in USD instead on EUR currency.
Funds transfer	2. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The client adviser processed international outgoing money transfer, for invoice payment, but she debited the wrong client's account.
Funds transfer	2. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The client adviser processed international outgoing money transfer, for invoice payment, but she debited the wrong client's account.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The same withdrawal transaction has been processed twice.

Appendix 9: Loss Event Data 20223 (cont.)

Process	Step	LE type	Loss event type	LE cause	Type of loss	Loss effect	Currency	Report of facts
Funds transfer	2. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The client adviser processed international outgoing money transfer based on client's request but he processed wrongly the description; name of ordering customer, on payment order.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	USD	The client asked to deposit cash in EUR currency but the cashier wrongly processed the transaction in USD currency.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	CHF	The client asked to convert the money with special exchange rate but the cashier made a mistake, he used the wrong exchange rates.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	USD	The main cashier processed cash deposit transaction according to client's request but he wrongly selected the USD instead of EUR currency.

Appendix 9: Loss Event Data 20223 (cont.)

Process	Step	LE type	Loss event type	LE cause	Type of loss	Loss effect	Currency	Report of facts
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The client asked for money withdrawal but the cashier instead of select the option for money withdrawal he wrongly selected the option for money deposit.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The cash withdrawal transaction has been cancelled because it has been processed without description.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The client adviser processed cash deposit transaction but she put the wrong amount. She pressed wrongly 38,900 instead of EUR 28,900. The gross loss for reporting is 10.000 Euro, the difference between the correct and the incorrect amount.
Cash		2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The cashier processed Customs payment transaction according to client's request but she pressed the wrong amount.

Appendix 9: Loss Event Data 20223 (cont.)

Process	Step	LE type	Loss event type	LE cause	Type of loss	Loss effect	Currency	Report of facts
Funds transfer	2. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	CHF	The client adviser processed international outgoing money transfer transaction according to client request but, it has been processed with wrong description.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The main cashier processed Interbank Outgoing Money Transfer but it has been cancelled because the description was wrong. The beneficiaries surname was incorrect.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	GBP	The cashier processed money converting with special exchange rate based on client's request, but she wrongly selected the GBP instead of EUR currency.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	CHF	The cashier processed the money exchange transaction but he made a mistake, he selected the wrong currency.

Appendix 9: Loss Event Data 20223 (cont.)

Process	Step	LE type	Loss event type	LE cause	Type of loss	Loss effect	Currency	Report of facts
Cash management	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	During processing the cash withdrawal transaction for client "Exchange Office", the cashier processed the wrong fee.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	GBP	The client has requested for currency conversion from GPB to EUR, but cashier made a mistake in the exchange rate.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	GBP	The client has requested for currency conversion from GPB to EUR, but cashier made a mistake in the exchange rate.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The cashier processed cash deposit transaction but he put the wrong amount. He pressed wrongly 85,000 instead of 75,000 Euro.

Appendix 9: Loss Event Data 20223 (cont.)

Process	Step	LE type	Loss event type	LE cause	Type of loss	Loss effect	Currency	Report of facts
Funds transfer	2. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The client adviser instead of processing the tax payment she did the payment contribution.
Funds transfer	1. Data Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The client adviser processed international outgoing money transfer but he wrongly selected the EUR instead of USD currency.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	CHF	The cashier processed the money exchange transaction but incorrectly received the conversion value from treasury.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	USD	The main cashier processed the cash deposit transaction according to client's request but he selected the wrong currency (USD).

Appendix 9: Loss Event Data 20223 (cont.)

Process	Step	LE type	Loss event type	LE cause	Type of loss	Loss effect	Currency	Report of facts
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The client's request was to pay the pension contributions, but the tax payment code was incorrecrly registered by cashier.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The cashier processed cash deposit transaction but she put the wrong amount. She pressed wrongly 11,000 instead of 21,000 Euro. So in this case the gross loss for reporting is 10.000 Euro, the difference between the correct and the incorrect amount.
Funds transfer	2. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The client adviser processed international outgoing money transfer transaction according to client request but, it has been processed with wrong description.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The cashier processed cash deposit transaction according to client request but he put the wrong description. He didn't write the description asked by client.

Appendix 9: Loss Event Data 20223 (cont.)

Process	Step	LE type	Loss event type	LE cause	Type of loss	Loss effect	Currency	Report of facts
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The cashier processed cash deposit transaction according to client request but he put the wrong description. He didn't write the description asked by client.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The customer requested to deposit cash, but the cashier made a mistake in the amount.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The cashier processed cash deposit transaction according to client request but he put the wrong description. He didn't write the description asked by client.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	CAD	The client request was to deposit money in his AUD account while the cashier mistakenly processed the transaction in CAD currency.

Appendix 9: Loss Event Data 20223 (cont.)

Process	Step	LE type	Loss event type	LE cause	Type of loss	Loss effect	Currency	Report of facts
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The main cashier processed the cash deposit transaction according to client's request but he selected the wrong account, instead of xxx CORPORATION she selected xxx COMPANY SHPK.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The main cashier processed cash deposit transaction according to client's request but he selected the wrong account, instead of xxx shpk he selected xxx.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The main cashier processed International Outgoing Money Transfer based on client's request but she selected the wrong provision charge.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	NOK	The main cashier processed International Outgoing Money Transfer according to client's request but he selected the wrong currency. The NOK currency, in which case the Bank stopped to use this currency.

Appendix 9: Loss Event Data 20223 (cont.)

Process	Step	LE type	Loss event type	LE cause	Type of loss	Loss effect	Currency	Report of facts
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	SEK	The client asked to convert the money with special exchange rate but the cashier got from the Treasury Sector the wrong exchange rate.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The client asked for money withdrawal but the cashier instead of select the option for money withdrawal he wrongly selected the option for money deposit.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The cashier processed cash deposit transaction based on client request but he used the wrong client's account
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The cashier processed cash deposit transaction but it has been cancelled because the description was wrong

Appendix 9: Loss Event Data 20223 (cont.)

Process	Step	LE type	Loss event type	LE cause	Type of loss	Loss effect	Currency	Report of facts
Funds transfer	5. Processing of funds transfer orders	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The main cashier processed Interbank Outgoing Money Transfer but it has been cancelled because the description was wrong. The beneficiaries surname was incorrect.
Funds transfer	5. Processing of funds transfer orders	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The main cashier processed Interbank Outgoing Money Transfer but it has been cancelled because the description was wrong.
Cash	5. Processing of funds transfer orders	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The cashier processed cash deposit transaction but it has been cancelled because the description was processed wrongly, by cashier.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The client asked for money withdrawal but the cashier instead of select the option for money withdrawal he wrongly selected the option for money deposit.

Appendix 9: Loss Event Data 20223 (cont.)

Process	Step	LE type	Loss event type	LE cause	Type of loss	Loss effect	Currency	Report of facts
Funds transfer	5. Processing of funds transfer orders	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The client requested for In Branch money transfer, but client adviser credited the wrong client's account.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	USD	The cashier processed cash deposit transaction but she wrongly selected the USD instead of EUR currency.
Funds transfer	5. Processing of funds transfer orders	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	USD	The client adviser processed international outgoing money transfer but he wrongly selected the USD instead of EUR currency.
Funds transfer	5. Processing of funds transfer orders	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	NOK	Client asked for international outgoing money transfer at NOK currency and it was processed by client adviser while the international payment unit didn't approve it.

Appendix 9: Loss Event Data 20223 (cont.)

Process	Step	LE type	Loss event type	LE cause	Type of loss	Loss effect	Currency	Report of facts
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	USD	The cashier processed cash deposit transaction in USD currency account instead of EUR currency account.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The cashier processed the cash deposit transaction at the customer's request, but he made an incorrect amount. He did not write the amount requested by the client.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The client has requested for currency conversion from EURO to USD, but made a mistake in the exchange rate
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	CHF	The client request was to deposit money in his EURO account while the cashier mistakenly processed the transaction in CHF currency.

Appendix 9: Loss Event Data 20223 (cont.)

Process	Step	LE type	Loss event type	LE cause	Type of loss	Loss effect	Currency	Report of facts
Funds transfer	5. Processing of funds transfer orders	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The main cashier processed Interbank Outgoing Money Transfer but it has been cancelled because the data were incomplete.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The client asked to convert the money with special exchange rate but the cashier got from the Treasury Sector the wrong exchange rate.
Funds transfer	4. Capture and acceptance of funds transfer orders	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The main cashier processed money transfer according to client's request but the description was incorrect.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The main cashier processed cash deposit transaction according to client's request but he selected the wrong amount.

Appendix 9: Loss Event Data 20223 (cont.)

Process	Step	LE type	Loss event type	LE cause	Type of loss	Loss effect	Currency	Report of facts
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	GBP	The client asked to convert the money with special exchange rate but the cashier got from the Treasury Sector the wrong exchange rate.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The client asked for money withdrawal but the cashier instead of select the option for money withdrawal he wrongly selected the option for money deposit.
Funds transfer	5. Processing of funds transfer orders	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	USD	A double transaction was performed during conversion of Eur to Usd Account, One from the cashier and one from the client himself with e-banking service.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	CHF	During the process of depositing CHF currency in the customer's account, upon approval of the transaction (according to the procedures) by the manager of the branch, the bank system instead of the approval has deposited the same amount in the customer's account.

Appendix 9: Loss Event Data 20223 (cont.)

Process	Step	LE type	Loss event type	LE cause	Type of loss	Loss effect	Currency	Report of facts
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	USD	The same amount was deposited by the customer on 19.10.2023, but we don't know how the same amount was appeared on the customer's account on 25.10.2023
Collections	6. Processing of collection orders	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The same customs payment has been processed twice, (mistakenly) by the cashier.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The cashier processed cash deposit transaction but it has been cancelled because the description was wrong
Cash	1. Data Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The money withdrawal has been cancelled because it has been processed with wrong description.

Appendix 9: Loss Event Data 20223 (cont.)

Process	Step	LE type	Loss event type	LE cause	Type of loss	Loss effect	Currency	Report of facts
Cash	1. Data Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The cash deposit transaction has been cancelled because it has been processed with wrong description.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The main cashier processed cash deposit transaction according to client's request but he selected the wrong amount. He pressed wrongly 184,401 instead of 18,401 Euro. So in this case the gross loss for reporting is 165,961 Euro, the difference between the correct and the incorrect amount.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The main cashier processed cash deposit transaction according to client's request but he selected the wrong account.
Funds transfer	5. Processing of funds transfer orders	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The main cashier processed Interbank Outgoing Money Transfer but it has been cancelled because it was written wrong amount.

Appendix 9: Loss Event Data 20223 (cont.)

Process	Step	LE type	Loss event type	LE cause	Type of loss	Loss effect	Currency	Report of facts
Funds transfer	5. Processing of funds transfer orders	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The main cashier processed Interbank Outgoing Money Transfer but it has been cancelled because it was written wrong amount.
Cash	1. Data Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The cash deposit transaction has been cancelled because it has been processed with wrong description.
Funds transfer	5. Processing of funds transfer orders	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The cashier processed payment transaction but he pressed the wrong amount.
Funds transfer	5. Processing of funds transfer orders	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The client adviser processed International outgoing money transfer, but the transfer fee was chosen wrongly.

Appendix 9: Loss Event Data 20223 (cont.)

Process	Step	LE type	Loss event type	LE cause	Type of loss	Loss effect	Currency	Report of facts
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	The client adviser processed international outgoing money transfer, while he selected the option "our" instead of “Ben” (parts for transfer fee), thus the amount of transaction was wrong.
Cash	3. Customer Relationship Management	2.2 Transaction execution error	Large loss	1.6 Human error	Negative	Absence of repayment	EUR	Human error of employee

Source: Loss Event Report, internal document provided by the Bank (anonymised), 2023.

Appendix 10: Survey Questionnaire

Survey Questionnaire – Designed for Bank Employees

Dear Participant,

You are invited to participate in the survey for doctoral research titled "**The Impact of Management Control on Managing Operational Risk in Banks**." This study is undertaken by Edona Haxhiu, a doctoral candidate in the Faculty of Economics, University of Ljubljana and is supervised by the esteemed Professor Dr. Mojca Marc.

The primary objective of this survey is to gather insights on how management control systems are perceived and implemented in banks. Your participation will provide valuable data that will contribute to a comprehensive analysis of current practices and help identify areas for improvement.

The survey will take approximately 15-20 minutes to complete. Your responses will be kept strictly confidential and will be used solely for the purpose of this study. We assure you that no personal or identifying information will be disclosed in any reports or publications resulting from this research.

Instructions for Participation:

1. **Access the Survey**: You can access the survey through the following link: (Survel Link)
2. **Complete the Survey**: Please answer all questions to the best of your ability.
3. **Submit the Survey**: Once completed, submit the survey by clicking the 'Submit' button at the end of the questionnaire.

We would be grateful if you could complete the survey by **30 October 2025**. Your input is highly valued and will significantly contribute to the success of this research.

If you have any questions or require further information about the survey or the research study, please feel free to contact the researcher: edona.haxhiuu@gmail.com.

Thank you in advance for your time and participation

Questions:

1. We are interested in understanding how you perceive the role of your supervisor in managing and overseeing your performance results. Please indicate your perception of control over your performance results by rating each statement below from 1 to 5, where 1 means you strongly disagree and 5 means you strongly agree.

a. My supervisor sets specific performance goals for my job.

1	2	3	4	5
Strongly disagree	Disgree	Neither agree Nor disagree	Agree	Strongly agree

b. My supervisor regularly checks how well I meet my performance goals.

c.

1	2	3	4	5
Strongly disagree	Disgree	Neither agree Nor disagree	Agree	Strongly agree

d. I am expected to explain to my supervisor if I do not meet my performance goals.

1	2	3	4	5
Strongly disagree	Disgree	Neither agree Nor disagree	Agree	Strongly agree

e. My immediate superior provides me feedback on how well I achieve my goals.

1	2	3	4	5
Strongly disagree	Disgree	Neither agree Nor disagree	Agree	Strongly agree

f. My pay increases are based upon how my performance compares with my goals.

1	2	3	4	5
Strongly disagree	Disgree	Neither agree Nor disagre	Agree	Strongly agree

2. Please reflect on your experience with your supervisor's involvement in guiding and overseeing your work activities and behaviors. Please indicate your perception of control over actions/behaviors by rating each statement below from 1 to 5, where 1 means you strongly disagree and 5 means you strongly agree.

a) I feel well-informed by my supervisor about the activities I am expected to perform.

1	2	3	4	5
Strongly disagree	Disgree	Neither agree Nor disagree	Agree	Strongly agree

b) In my experience, my supervisor keeps track of how I carry out the required activities.

1	2	3	4	5
Strongly disagree	Disgree	Neither agree Nor disagree	Agree	Strongly agree

c) I regularly receive feedback from my supervisor on whether I meet their expectations in my job activities.

1	2	3	4	5
Strongly disagree	Disgree	Neither agree Nor disagree	Agree	Strongly agree

d) My supervisor readjusts my activities when necessary.

1	2	3	4	5
Strongly disagree	Disgree	Neither agree Nor disagree	Agree	Strongly agree

e) I believe my supervisor would acknowledge and appreciate it if I perform my activities well.

1	2	3	4	5
Strongly disagree	Disgree	Neither agree Nor disagree	Agree	Strongly agree

3. Please share your opinion on how risk management system is used in your bank. Rate each statement below from 1 to 5, where 1 means you strongly disagree and 5 means you strongly agree.

	Strongly Disagree	Disagree	Neither agree Nor disagree	Agree	Strongly Agree
a. My direct supervisor and more senior managers often use risk management tools and information to question and discuss about ongoing decisions within the bank.	1	2	3	4	5
b. There appears to be significant communication between the bank's top management and department managers about risk management issues and tools.	1	2	3	4	5

c. I notice that my direct supervisor uses risk management tools and information when we talk about ongoing changes in the department or in the bank with our team.	1	2	3	4	5

4. Please evaluate how closely the following statements reflect your approach and behavior in the workplace, particularly in financial matters and decisions. Rate each statement on a scale from 1 to 5, where 1 means you strongly disagree and 5 means you strongly agree.

	Strongly Disagree	Disagree	Neither agree Nor disagree	Agree	Strongly Agree
a. a. I am good in resisting temptations, especially those related to financial decisions.	1	2	3	4	5
b. I am diligent and avoid procrastinating in my work tasks.	1	2	3	4	5
c. I am mindful of what I say, especially in professional interactions.	1	2	3	4	5
d. I never allow myself to lose control, particularly in high-pressure work situations.	1	2	3	4	5
e. I refrain from engaging in financial activities that are not beneficial, even if they seem.	1	2	3	4	5
f. I refuse financial activities that are not in my best interest	1	2	3	4	5
g. I recognize the importance of self-discipline in financial decisions.	1	2	3	4	5
h. I stay focused on work tasks and don't get carried away by emotions.	1	2	3	4	5
i. I consider the consequences before making work decisions on the spur of the moment.	1	2	3	4	5
j. I think carefully before acting in work situations.	1	2	3	4	5
k. Pleasure and fun do not compromise my work responsibilities.	1	2	3	4	5
l. I am effective in working toward long-term financial goals.	1	2	3	4	5

5. Please reflect on the most recent mistakes you have made at work. For the following questions, rate how frequently each scenario applies to you, using a scale from 1 to 5. Each number represents the following frequency:

Never (1): This has not happened at all.
Rarely (2): This happens on occasion, perhaps once every few months.
Neutral (3): This occurs sometimes, but not regularly – around once a month or so.
Often (4): This is a regular occurrence, happening weekly.
Very Often (5): This is a frequent and consistent part of my work experience, occurring several times a week.

1. Have you ever started processing a transaction before gathering all the necessary documents due to mental and job engagement?
    - Never
    - Rarely
    - Sometimes
    - Often
    - Very Often
2. Have you ever been temporarily distracted while assisting a customer, causing or nearly causing an error in their transaction?
    - Never
    - Rarely
    - Sometimes
    - Often
    - Very Often
3. Have you ever unconsciously forgotten to follow a standard procedure or safety protocol before starting your task, potentially leading to an error?
    - Never
    - Rarely
    - Sometimes
    - Often
    - Very Often
4. Have you ever unknowingly performed a potentially risky action (e.g., accessing sensitive data, handling large sums of money) due to mental engagement, with the risk passing by chance?
    - Never
    - Rarely
    - Sometimes
    - Often
    - Very Often
5. Have you ever suffered a minor mistake (e.g., misfiling a document, inputting wrong data) while working without noticing it at the time?
    - Never
    - Rarely
    - Sometimes
    - Often
    - Very Often
6. Have you ever temporarily forgotten a regular task you intended to do (e.g., going somewhere in your workplace but not remembering the initial purpose)?
    - Never
    - Rarely
    - Sometimes
    - Often
    - Very Often
7. Have you ever unconsciously forgotten to perform one or more stages of your job and had to think for a moment to remember them?
    - Never
    - Rarely
    - Sometimes
    - Often
    - Very Often

8. Have you ever forgotten to complete the final stages of a task (e.g., logging off a system, filing documents) after finishing your work?
    - Never
    - Rarely
    - Sometimes
    - Often
    - Very Often
9. Have you ever applied a new method to complete your tasks based on your personal thinking without having enough experience or prior information?
    - Never
    - Rarely
    - Sometimes
    - Often
    - Very Often
10. Have you ever experienced an error or near-miss caused by your own mistaken actions due to lack of sufficient information or training?
    - Never
    - Rarely
    - Sometimes
    - Often
    - Very Often
11. Have you ever unknowingly or unintentionally violated company's safety and security regulations because you were not informed about the associated guidelines?
    - Never
    - Rarely
    - Sometimes
    - Often
    - Very Often
12. Have you ever habitually started your tasks without checking for compliance with standard procedures, despite knowing the importance
    - Never
    - Rarely
    - Sometimes
    - Often
    - Very Often

13. Have you ever skipped one or more steps in a process to do your job faster?
    - Never
    - Rarely
    - Sometimes
    - Often
    - Very Often
14. Have you ever ignored using the required security measures (e.g., password protection, secure logins) because you found them cumbersome?
    - Never
    - Rarely
    - Sometimes
    - Often
    - Very Often
15. Have you ever done work other than your main job about which you had no prior training, just to help colleagues without seeking permission from your supervisors?
    - Never
    - Rarely
    - Sometimes
    - Often
    - Very Often
16. Have you ever assumed a problem in your workplace to be easier than it really was due to time limitations, stress, or improper environmental factors, leading to more serious issues?
    - Never
    - Rarely

- Sometimes
- Often
- Very Often

17. Have you ever ignored performing your tasks accurately based on rules and principles due to high job demands or time limitations?
    - Never
    - Rarely
    - Sometimes
    - Often
    - Very Often
18. Have you ever worked in an uncomfortable position, resulting in discomfort or pain, and subsequently ignored some rules and guidelines to shortcut your tasks?
    - Never
    - Rarely
    - Sometimes
    - Often
    - Very Often
19. Has it happened to you that in some stressful situations requiring concentration, your decision might have been influenced by your colleagues?
    - Never
    - Rarely
    - Sometimes
    - Often
    - Very Often
20. In a particular situation, have you ever considered a rule or guideline useless and acted by your own method, which seemed more appropriate to you?
    - Never
    - Rarely
    - Sometimes
    - Often
    - Very Often
21. When performing your regular tasks, have you adopted a method according to your style and creativity that involved higher risk?
    - Never
    - Rarely
    - Sometimes
    - Often
    - Always
    - Often
    - Very Often

6. The following questions deal with the workload that you experience in your job. This survey uses the Subjective Workload Assessment Technique (SWAT) to assess workload across three dimensions: Time Load, Mental Load, and Psychological Stress Load. Each of the dimensions is described below.

I. <u>Time Load</u>

1. **Often have spare time**. Interruptions or overlap among activites occur infrequently or not at all.
2. **Occasonally have spare time**. Interruptions or overlap amon activities occur infrequently.
3. **Almost never have spare time**. Interruptions or overlap among activities are very frequent, or occur all the time.

II. <u>Mental Effort Load</u>

1. **Very little conscious mental effort or concentration required**. Activity is almost automatic, requiring little or no attention.
2. **Moderate conscious mental effort or concentration required**. Complexity of activity is moderately high due to uncertainty, unpredictability, or unfamiliarity. Condiderable attention required.
3. **Extensive mental effort and concentration are necessary**. Very complex activity requiring total attention.

III. Pschycological Stress Load

1. **Little confusion, risk, frustration, or anxiety exists and can be easily accomodated**.
2. **Moderate stress due to confusion, frustration, or anxiety noticeably adds to workload.** Significant compensation is required to maintain adequate performance.
3. **High to very intense stress due to confusion, frustration, or anxiety.** High extreme determination and self-control required.

Based on the above dimensions we aim to understand your perceived workload in various tasks and scenarios in your bank. For each scenario, please rate the perceived workload on a scale from 1 to 3, where **1 means Low**; **2 means medium**; **3 means high.**

Scenario 1: Handling Customer Inquiries During Peak Hours

1. **Time Load**: How would you rate the time pressure for this task?
   - 1 (Low)
   - 2 (Medium)
   - 3 (High)
2. **Mental Load**: How would you rate the cognitive effort required for this task?
   - 1 (Low)
   - 2 (Medium)
   - 3 (High)
3. **Physiological Stress Load**: How would you rate the stress and physical strain for this task?
   - 1 (Low)
   - 2 (Medium)
   - 3 (High)

Scenario 2: Processing Loan Applications

1. **Time Load: How would you rate the time pressure for this task?**
   - 1 (Low)
   - 2 (Medium)
   - 3 (High)
2. **Mental Load**: How would you rate the cognitive effort required for this task?
   - 1 (Low)

- 2 (Medium)
- 3 (High)

3. **Physiological Stress Load**: How would you rate the stress and physical strain for this task?
    - 1 (Low)
    - 2 (Medium)
    - 3 (High)

Scenario 3: Addressing Customer Complaints

1. **Time Load**: How would you rate the time pressure for this task?
    - 1 (Low)
    - 2 (Medium)
    - 3 (High)

2. **Mental Load**: How would you rate the cognitive effort required for this task?
    - 1 (Low)
    - 2 (Medium)
    - 3 (High)
3. **Physiological Stress Load**: How would you rate the stress and physical strain for this task?
    - 1 (Low)
    - 2 (Medium)
    - 3 (High)

Scenario 4: Conducting Financial Advising Sessions

1. **Time Load**: How would you rate the time pressure for this task?
    - 1 (Low)
    - 2 (Medium)
    - 3 (High)
2. **Mental Load**: How would you rate the cognitive effort required for this task?
    - 1 (Low)
    - 2 (Medium)
    - 3 (High)
3. **Physiological Stress Load**: How would you rate the stress and physical strain for this task?
    - 1 (Low)
    - 2 (Medium)
    - 3 (High)

Scenario 5 : End-of-Day Reconciliation

1. **Time Load**: How would you rate the time pressure for this task?
    - 1 (Low)
    - 2 (Medium)
    - 3 (High)
2. **Mental Load**: How would you rate the cognitive effort required for this task?
    - 1 (Low)

- 2 (Medium)
- 3 (High)

3. **Physiological Stress Load**: How would you rate the stress and physical strain for this task?
   - 1 (Low)
   - 2 (Medium)
   - 3 (High)

7. What is "management control"? Please select the appropriate answer based on your understanding.

- Internal control
- Audit
- Planning, organizing, directing, and controlling organizational resources and processes to achieve specific objectives.
- Control by superiors

8. To what extent do you agree or disagree with the following statements that measure risk culture within your bank?

a). Are you adequately informed and aware of the risk culture?

0	1	2	3	4	5
Cannot Judge	Strongly disagree	Disgree	Somewhat Agree	Agree	Strongly agree

b). Is the desired level of risk behaviour communicated to you and monitored by managers?

0	1	2	3	4	5
Cannot Judge	Strongly disagree	Disgree	Somewhat Agree	Agree	Strongly agree

c). Are risk appetite specifications known and understood throughout the organization?

0	1	2	3	4	5
Cannot Judge	Strongly disagree	Disgree	Somewhat Agree	Agree	Strongly agree

d). Are risk responsibilities clearly defined and owned?

0	1	2	3	4	5
Cannot Judge	Strongly disagree	Disgree	Somewhat Agree	Agree	Strongly agree

e). Are you held accountable for your actions related to risk management?

0	1	2	3	4	5
Cannot Judge	Strongly disagree	Disgree	Somewhat Agree	Agree	Strongly agree

f). Are escalation processes adequate to report issues in a timely and appropriate way?

0	1	2	3	4	5
Cannot Judge	Strongly disagree	Disgree	Somewhat Agree	Agree	Strongly agree

g). Are whistleblowing procedures in place and positively supported by management?

0	1	2	3	4	5
Cannot Judge	Strongly disagree	Disgree	Somewhat Agree	Agree	Strongly agree

h). Can you report concerns without fear of detriment?

0	1	2	3	4	5
Cannot Judge	Strongly disagree	Disgree	Somewhat Agree	Agree	Strongly agree

i). Is there a perception that breaching risk requirements negatively impacts career, responsibilities, and remuneration?

0	1	2	3	4	5
Cannot Judge	Strongly disagree	Disgree	Somewhat Agree	Agree	Strongly agree

j). Do managers actively seek and value alternative opinions on risk?

0	1	2	3	4	5
Cannot Judge	Strongly disagree	Disgree	Somewhat Agree	Agree	Strongly agree

k). Are control functions respected and integrated as independent functions?

0	1	2	3	4	5
Cannot Judge	Strongly disagree	Disgree	Somewhat Agree	Agree	Strongly agree

l). Is the compensation structure aligned with corporate values and risks, encouraging appropriate behaviour?

0	1	2	3	4	5
Cannot Judge	Strongly disagree	Disgree	Somewhat Agree	Agree	Strongly agree

m). Do you have sufficient understanding of risk management and risk culture?

0	1	2	3	4	5
Cannot Judge	Strongly disagree	Disgree	Somewhat Agree	Agree	Strongly agree

n). Are opportunities for knowledge-sharing on risk issues actively promoted?

0	1	2	3	4	5
Cannot Judge	Strongly disagree	Disgree	Somewhat Agree	Agree	Strongly agree

9. In the past year, rank on a scale of 1-4 the types of on-the-job training that you have received in order of most to least (1=most time spent in this type of training; 4=least amount of time spent in this type of training).

_____ Specific training for Operational Risk Management

_____ Other Technical, Professional or job-specific training

_____ General business skill training

_____ Personal development training

DEMOGRAPHIC QUESTIONS

10. Please circle your gender:

1. Male
2. Female
3. Other

11. What is your age:

a) 20-30
b) 31-40
c) 41-50
d) 51-60
e) over 61

12. Please mark your level of education:

a) High School Degree
b) Bachelor Degree
c) Master Degree
d) Doctoral Degree

13. Please select your years of work experience in your current job:

a) Less than 1 year
b) 1-2 years
c) 3-5 years
d) 6-10 years
e) More than 10 years

14. In what department you are currently working in?
Department
……

Appendix 11: Descriptive Statistics for Measurement Items

MEASUREMENT ITEMS	Obs	Mean	SD
Results Control (RC)			
RC1 My supervisor sets specific performance objectives for my work.	150	3.95	.85
RC2 My supervisor regularly checks how well I achieve my performance objectives.	149	3.97	.83
RC3 I am expected to explain to my supervisor if I do not meet my performance objectives.	149	3.94	.77
RC4 My supervisor gives me feedback on how well I achieve my objectives.	149	3.78	.88
RC5 My salary increases are based on how my performance compares with my objectives.	149	3.25	1.18
Action Control (AC)			
AC1 I feel well informed by my supervisor about the activities I am expected to perform.	146	4.02	.81
AC2 In my experience, my supervisor closely monitors how I perform the required activities.	146	3.80	.81
AC3 I regularly receive feedback from my supervisor on whether I meet expectations**.**	146	3.72	.92
AC4 My supervisor adjusts my activities when necessary**.**	145	3.65	.95
AC5 I believe my supervisor would appreciate if I perform my activities well**.**	145	3.89	.91
Interactive use (INT			
INT1 My direct supervisor and senior managers often use risk-management tools and information to challenge and debate upcoming decisions within the bank.	143	3.76	.82
INT2 There appears to be meaningful communication between senior management of the bank and department managers regarding risk-management matters and tools.	143	3.81	.82
INT3 I observe that my direct supervisor uses risk-management tools and information when discussing continuous changes in our department or in the bank with our team.	144	3.75	.83
Self-Control (SC)			
SC1 I am good at resisting temptations, especially those related to financial decisions.	142	4.24	.64
SC2 I am punctual and avoid delays or postponing my work tasks.	142	4.36	.76
SC3 I am careful about what I say, especially in professional interactions.	142	4.50	.54
SC4 I never allow myself to lose control, especially in high-pressure work situations.	142	4.40	.70
SC5 I refrain from engaging in financial activities that are not beneficial, even if they appear to be.	142	4.17	.82
SC6 I understand the importance of self-discipline in financial decisions.	142	4.52	.58
SC7 I stay focused on my work tasks and do not get carried away by emotions.	142	4.51	.58
SC8 I consider the consequences before making impulsive work-related decisions.	142	4.44	.65
SC9 I think carefully before acting in work situations.	142	4.56	.53

SC10 Pleasure and entertainment do not compromise my responsibilities at work.	142	4.45	.63
SC11 I am effective in working toward long-term financial goals.	142	4.49	.71
Slips/Lapses (SLIPSLAPS)			
SL1 Have you ever started processing a transaction before collecting all required documents due to mental or workload pressure?	135	1.52	.74
SL2 Have you ever been temporarily distracted while assisting a client, causing or nearly causing an error in their transaction?	135	1.75	.77
SL3 Have you ever unintentionally forgotten to follow a standard procedure or safety protocol before starting your task, potentially leading to an error?	135	1.65	.77
SL4 Have you ever unknowingly performed a potentially risky action due to mental overload, where the risk was overlooked?	135	1.27	.71
SL5 Have you ever made a small mistake during work without noticing it at the moment?	135	2.05	.77
SL6 Have you ever forgotten to complete the final steps of a task after finishing your work?	135	1.91	.86
Mistakes (MIS)			
MIS1 Have you ever implemented a new method to complete your tasks without having sufficient experience or prior information?	135	1.74	1.06
MIS2 Have you ever experienced an error or near-error due to lack of information or insufficient training?	135	1.89	.83
MIS3 Have you ever violated security regulations because you were not informed about the relevant guidelines?	135	1.31	.74
Routine violations (RV)			
RV1 Have you ever begun your tasks without checking compliance with standard procedures?	135	1.34	.72
RV2 Have you ever skipped steps in a process to complete your work faster?	135	1.48	.81
RV3 Have you ever ignored required security measures because you considered them inconvenient?	135	1.25	.74
RV4 Have you ever performed tasks outside your main responsibilities without prior training, just to help colleagues?	135	2.19	1.29
Situational violations (SV)			
SV1 Have you ever assumed a workplace problem was easier than it truly was, leading to more serious issues?	135	1.88	1.01
SV2 Have you ever neglected to perform your tasks correctly due to high job demands?	135	1.50	.84
SV3 Have you ever worked in an uncomfortable position and then ignored guidelines to finish your tasks more quickly?	135	1.53	.91
Exceptional violations (EV)			
EV1 Has it ever happened that your decisions were influenced by colleagues in stressful situations?	135	1.70	.91
EV2 Have you ever acted according to your own method because you considered a rule or guideline unnecessary?	135	1.48	.85
EV3 Have you ever adopted a creative method that involved a higher level of risk?	135	1.36	.78
Risk culture (RCulture)			
RCulture1 Are you sufficiently informed and aware of risk culture?	112	3.96	.88

RCulture2 Has the desired level of risk-related behaviour been communicated and monitored by managers?	115	3.83	.94
RCulture3 Are the specifications of risk appetite known and understood throughout the organization?	116	3.83	.85
RCulture4 Are risk responsibilities clearly defined and accepted?	120	4.03	.78
RCulture5 Are you held accountable for your actions related to risk management?	116	4.00	.91
RCulture6 Are escalation processes sufficient to report issues appropriately and on time?	111	3.85	.79
RCulture7 Are whistleblowing procedures established and positively supported by management?	118	4.04	.84
RCulture8 Can you report your concerns without fear of negative consequences or harm?	119	3.88	.97
RCulture9 Is there a perception that violating risk requirements negatively affects career, responsibility, and rewards?	114	3.93	.97
RCulture10 Do managers actively seek and value alternative views on risk?	118	3.60	1.10
RCulture11 Are control functions respected and integrated as independent functions?	114	3.94	.80
RCulture12 Is the compensation structure aligned with corporate values and risks, encouraging proper behavior?	112	3.90	.80
RCulture13 Do you have sufficient knowledge of risk management and risk culture?	116	3.95	.79
RCulture14 Are opportunities for sharing knowledge about risk issues actively promoted?	117	3.74	.81

Appendix 12: MODEL A

Model A: Measurement model estimations (SmartPLS 4.0)

Construct and measurement items	Standardized Factor Loading	t-value	p-value
Results Control (RC)			
RC1 My supervisor sets specific performance objectives for my work.	0.748	12.481	<0.001
RC2 My supervisor regularly checks how well I achieve my performance objectives.	0.846	19.844	<0.001
RC3 I am expected to explain to my supervisor if I do not meet my performance objectives.	0.747	13.958	<0.001
RC4 My supervisor gives me feedback on how well I achieve my objectives.	0.792	14.492	<0.001
RC5 My salary increases are based on how my performance compares with my objectives.	0.561	5.013	<0.001
Self-Control (SC)			
SC1 I am good at resisting temptations, especially those related to financial decisions.	0.608	10.544	<0.001
SC2 I am punctual and avoid delays or postponing my work tasks.	0.623	8.143	<0.001
SC3 I am careful about what I say, especially in professional interactions.	0.780	18.552	<0.001
SC4 I never allow myself to lose control, especially in high-pressure work situations.	0.707	13.832	<0.001
SC5 I refrain from engaging in financial activities that are not beneficial, even if they appear to be.	0.503	6.354	<0.001
SC6 I understand the importance of self-discipline in financial decisions.	0.837	26.270	<0.001
SC7 I stay focused on my work tasks and do not get carried away by emotions.	0.779	19.287	<0.001
SC8 I consider the consequences before making impulsive work-related decisions.	0.801	21.697	<0.001
SC9 I think carefully before acting in work situations.	0.826	25.860	<0.001
SC10 Pleasure and entertainment do not compromise my responsibilities at work.	0.715	12.322	<0.001
SC11 I am effective in working toward long-term financial goals.	0.712	10.517	<0.001
Slips/Lapses (SLIPSLAPS)			
SL1 Have you ever started processing a transaction before collecting all required documents due to mental or workload pressure?	0.551	4.409	<0.001
SL2 Have you ever been temporarily distracted while assisting a client, causing or nearly causing an error in their transaction?	0.771	11.171	<0.001
SL3 Have you ever unintentionally forgotten to follow a standard procedure or safety protocol before starting your task, potentially leading to an error?	0.719	8.084	<0.001

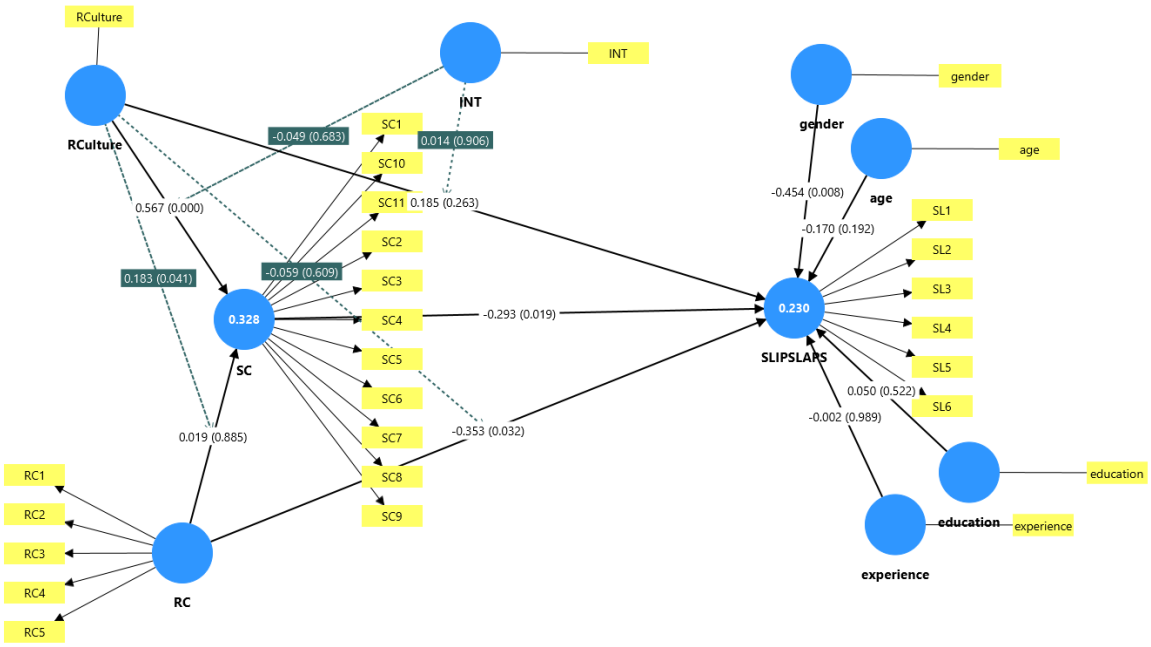
SL4 Have you ever unknowingly performed a potentially risky action due to mental overload, where the risk was overlooked?	0.783	9.831	<0.001
SL5 Have you ever made a small mistake during work without noticing it at the moment?	0.695	6.803	<0.001
SL6 Have you ever forgotten to complete the final steps of a task after finishing your work?	0.748	9.109	<0.001

Construct	Cronbach's α	CR	AVE	*INT*	*RC*	*RCulture*	*SC*	*SLIPS LAPS*
INT	1.000	1.000	1.000	**(1.00)**	0.440	0.361	0.109	0.016
RC	0.805	0.860	0.555	0.663	**(0.745)**	0.300	0.108	0.074
RCulture	1.000	1.000	1.000	0.601	0.548	**(1.00)**	0.291	0.018
SC	0.907	0.922	0.524	0.330	0.328	0.539	**(0.724)**	0.091
SLIPS LAPS	0.810	0.861	0.512	–0.125	–0.272	–0.133	–0.302	**(0.716)**

Notes: Values above the diagonal are squared Pearson correlations, values on the diagonal are square roots of AVE (Fornell–Larcker criterion). Values below the diagonal are Pearson correlations.

Heterotrait-monotrait ratio (HTMT)	Original sample (O)	Sample mean (M)	2.5%	97.5%
RC ↔ INT	0.763	0.760	0.632	0.866
RCulture ↔ INT	0.601	0.600	0.469	0.719
RCulture ↔ RC	0.594	0.592	0.389	0.764
SC ↔ INT	0.349	0.348	0.187	0.498
SC ↔ RC	0.359	0.379	0.252	0.520
SC ↔ RCulture	0.562	0.562	0.416	0.694
SLIPSLAPS ↔ INT	0.138	0.180	0.074	0.344
SLIPSLAPS ↔ RC	0.318	0.355	0.194	0.559
SLIPSLAPS ↔ RCulture	0.155	0.180	0.057	0.368
SLIPSLAPS ↔ SC	0.340	0.371	0.246	0.531

Model A: Result of PLS-SEM estimation – Standardized path coefficients and *p*-values



Model A: Structural model estimations (SmartPLS 4.0)

Standardized path coefficients	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/STDEV|)	P values
RC → SC	0.019	0.049	0.132	0.144	0.885
RC → SLIPSLAPS	-0.353	-0.348	0.165	2.142	0.032
RCulture → SC	0.567	0.572	0.115	4.917	0.000
RCulture → SLIPSLAPS	0.185	0.192	0.165	1.120	0.263
RCulture × RC → SC	0.183	0.174	0.090	2.047	0.041
RCulture × RC → SLIPSLAPS	-0.059	-0.033	0.116	0.511	0.609
SC → SLIPSLAPS	-0.293	-0.301	0.125	2.345	0.019
INT → SC	-0.004	-0.037	0.127	0.030	0.976
INT → SLIPSLAPS	0.092	0.075	0.135	0.680	0.497
INT × RCulture → SC	-0.049	-0.033	0.119	0.409	0.683
INT × RCulture → SLIPSLAPS	0.014	0.002	0.117	0.119	0.906
age → SLIPSLAPS	-0.170	-0.179	0.130	1.304	0.192
education → SLIPSLAPS	0.050	0.050	0.078	0.640	0.522
experience → SLIPSLAPS	-0.002	-0.006	0.126	0.014	0.989
gender → SLIPSLAPS	-0.454	-0.445	0.171	2.658	0.008

Specific indirect effects	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/STDEV|)	P values
INT → SC → SLIPSLAPS	0.001	0.011	0.042	0.026	0.979
RC → SC → SLIPSLAPS	-0.006	-0.014	0.043	0.129	0.897
RCulture → SC → SLIPSLAPS	-0.166	-0.173	0.084	1.969	0.049
RCulture × RC → SC → SLIPSLAPS	-0.054	-0.053	0.038	1.416	0.157
INT × RCulture → SC → SLIPSLAPS	0.014	0.013	0.040	0.357	0.721

Total effects	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/STDEV|)	P values
age → SLIPSLAPS	-0.170	-0.179	0.130	1.304	0.192
education → SLIPSLAPS	0.050	0.050	0.078	0.640	0.522
experience → SLIPSLAPS	-0.002	-0.006	0.126	0.014	0.989
gender → SLIPSLAPS	-0.454	-0.445	0.171	2.658	0.008
INT → SC	-0.004	-0.037	0.127	0.030	0.976
INT → SLIPSLAPS	0.093	0.086	0.138	0.676	0.499
INT × RCulture → SC	-0.049	-0.033	0.119	0.409	0.683
INT × RCulture → SLIPSLAPS	0.028	0.015	0.124	0.227	0.821
RC → SC	0.019	0.049	0.132	0.144	0.885
RC → SLIPSLAPS	-0.359	-0.362	0.163	2.197	0.028
RCulture → SC	0.567	0.572	0.115	4.917	0.000
RCulture → SLIPSLAPS	0.019	0.019	0.143	0.130	0.897
RCulture × RC → SC	0.183	0.174	0.090	2.047	0.041
RCulture × RC → SLIPSLAPS	-0.113	-0.086	0.111	1.013	0.311
SC → SLIPSLAPS	-0.293	-0.301	0.125	2.345	0.019

Appendix 13: MODEL B

Model B: Measurement model estimations (SmartPLS 4.0)

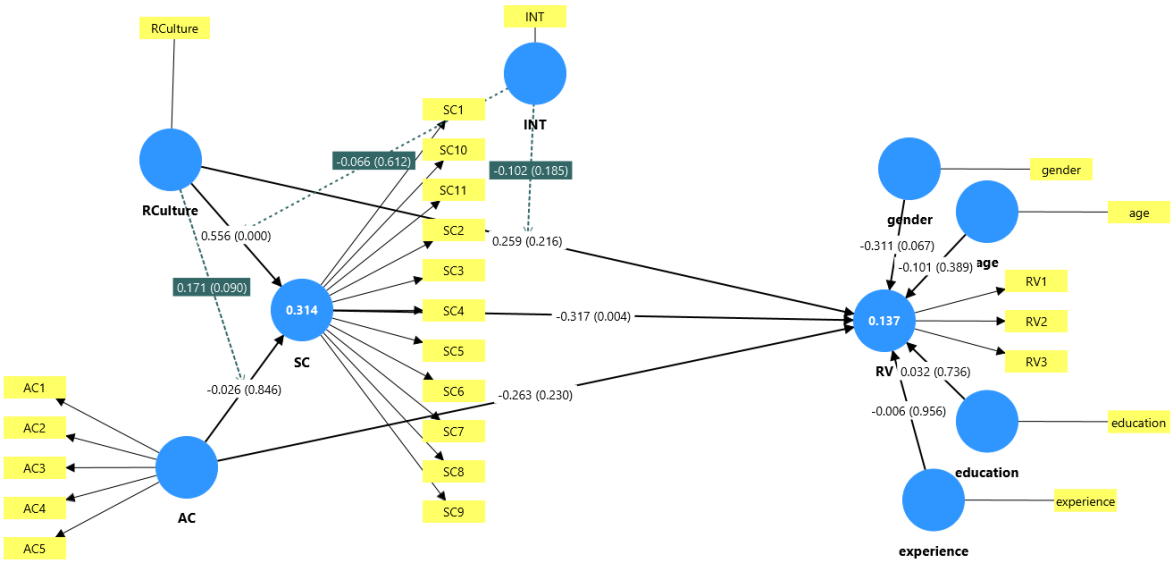
Construct and measurement items	Standardized factor loading	t-value	p-value
Action Control (AC)			
AC1 I feel well informed by my supervisor about the activities I am expected to perform.	0.835	19.712	0.000
AC2 In my experience, my supervisor closely monitors how I perform the required activities.	0.845	16.940	0.000
AC3 I regularly receive feedback from my supervisor on whether I meet expectations**.**	0.819	15.957	0.000
AC4 My supervisor adjusts my activities when necessary**.**	0.782	12.660	0.000
AC5 I believe my supervisor would appreciate if I perform my activities well**.**	0.831	13.945	0.000
Self-Control (SC)			
SC1 I am good at resisting temptations, especially those related to financial decisions.	0.616	10.792	0.000
SC2 I am punctual and avoid delays or postponing my work tasks.	0.618	7.798	0.000
SC3 I am careful about what I say, especially in professional interactions.	0.773	15.981	0.000
SC4 I never allow myself to lose control, especially in high-pressure work situations.	0.708	13.910	0.000
SC5 I refrain from engaging in financial activities that are not beneficial, even if they appear to be.	0.515	6.445	0.000
SC6 I understand the importance of self-discipline in financial decisions.	0.836	21.732	0.000
SC7 I stay focused on my work tasks and do not get carried away by emotions.	0.773	16.271	0.000
SC8 I consider the consequences before making impulsive work-related decisions.	0.798	18.848	0.000
SC9 I think carefully before acting in work situations.	0.823	21.273	0.000
SC10 Pleasure and entertainment do not compromise my responsibilities at work.	0.724	12.879	0.000
SC11 I am effective in working toward long-term financial goals.	0.712	10.487	0.000
Routine violations (RV)			
RV1 Have you ever begun your tasks without checking compliance with standard procedures?	0.934	9.804	0.000
RV2 Have you ever skipped steps in a process to complete your work faster?	0.885	9.447	0.000
RV3 Have you ever ignored required security measures because you considered them inconvenient?	0.822	5.083	0.000

Construct	Cronbach's α	CR	AVE	*AC*	*INT*	*RCulture*	*SC*	*RV*
AC	0.882	0.913	0.676	**(0.822)**	0.504	0.373	0.104	0.018
INT	1.000	1.000	1.000	0.710	**(1.00)**	0.361	0.109	0.008
RCulture	1.000	1.000	1.000	0.611	0.601	**(1.00)**	0.291	0.004
SC	0.907	0.923	0.524	0.323	0.330	0.539	**(0.724)**	0.070
RV	0.859	0.913	0.778	–0.136	–0.087	–0.063	–0.265	**(0.882)**

Notes: Values above the diagonal are squared Pearson correlations, values on the diagonal are square roots of AVE (Fornell–Larcker criterion). Values below the diagonal are Pearson correlations.

Heterotrait-monotrait ratio (HTMT)	Original sample (O)	Sample mean (M)	2.5%	97.5%
INT ↔ AC	0.754	0.748	0.635	0.838
RV ↔ AC	0.160	0.198	0.099	0.337
RV ↔ INT	0.083	0.116	0.028	0.275
RCulture ↔ AC	0.660	0.658	0.517	0.788
RCulture ↔ INT	0.601	0.600	0.469	0.719
RCulture ↔ RV	0.070	0.109	0.019	0.283
SC ↔ AC	0.349	0.361	0.222	0.502
SC ↔ INT	0.349	0.348	0.187	0.498
SC ↔ RV	0.303	0.320	0.180	0.486
SC ↔ RCulture	0.562	0.562	0.416	0.694

Model B: Result of PLS-SEM estimation – Standardized path coefficients and *p*-values



Model B: Structural model estimation (SmartPLS 4.0)

Standardized path coefficients	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/STDEV|)	P values
AC → RV	-0.263	-0.261	0.219	1.199	0.230
AC → SC	-0.026	-0.011	0.132	0.194	0.846
RCulture → RV	0.259	0.266	0.210	1.237	0.216
RCulture → SC	0.556	0.567	0.121	4.608	0.000
RCulture × AC → SC	0.171	0.160	0.101	1.694	0.090
SC → RV	-0.317	-0.317	0.109	2.904	0.004
INT → RV	0.037	0.029	0.138	0.269	0.788
INT → SC	0.037	0.008	0.131	0.281	0.779
INT × RCulture → RV	-0.102	-0.088	0.077	1.326	0.185
INT × RCulture → SC	-0.066	-0.045	0.131	0.507	0.612
age → RV	-0.101	-0.102	0.117	0.862	0.389
education → RV	0.032	0.035	0.096	0.337	0.736
experience → RV	-0.006	-0.010	0.115	0.055	0.956
gender → RV	-0.311	-0.314	0.170	1.832	0.067

Specific indirect effects	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/STDEV|)	P values
RCulture → SC → RV	-0.176	-0.181	0.078	2.249	0.025

RCulture* × *AC* → *SC* → *RV	-0.054	-0.051	0.039	1.390	0.165
INT* × *RCulture* → *SC* → *RV	0.021	0.017	0.045	0.467	0.641
AC* → *SC* → *RV	0.008	0.003	0.044	0.184	0.854
INT* → *SC* → *RV	-0.012	-0.003	0.044	0.263	0.792

Total effects	**Original sample (O)**	**Sample mean (M)**	**Standard deviation (STDEV)**	**T statistics (|O/STDEV|)**	**P values**
AC* → *RV	-0.254	-0.258	0.226	1.127	0.260
AC* → *SC	-0.026	-0.011	0.132	0.194	0.846
RCulture* → *RV	0.083	0.085	0.206	0.403	0.687
RCulture* → *SC	0.556	0.567	0.121	4.608	0.000
RCulture* × *AC* → *RV	-0.054	-0.051	0.039	1.390	0.165
RCulture* × *AC* → *SC	0.171	0.160	0.101	1.694	0.090
SC* → *RV	-0.317	-0.317	0.109	2.904	0.004
INT* → *RV	0.026	0.026	0.140	0.182	0.855
INT* → *SC	0.037	0.008	0.131	0.281	0.779
INT* × *RCulture* → *RV	-0.081	-0.072	0.086	0.935	0.350
INT* × *RCulture* → *SC	-0.066	-0.045	0.131	0.507	0.612
age* → *RV	-0.101	-0.102	0.117	0.862	0.389
education* → *RV	0.032	0.035	0.096	0.337	0.736
experience* → *RV	-0.006	-0.010	0.115	0.055	0.956
gender* → *RV	-0.311	-0.314	0.170	1.832	0.067

Appendix 14: MODEL C

Model C: Measurement model estimations (SmartPLS 4.0)

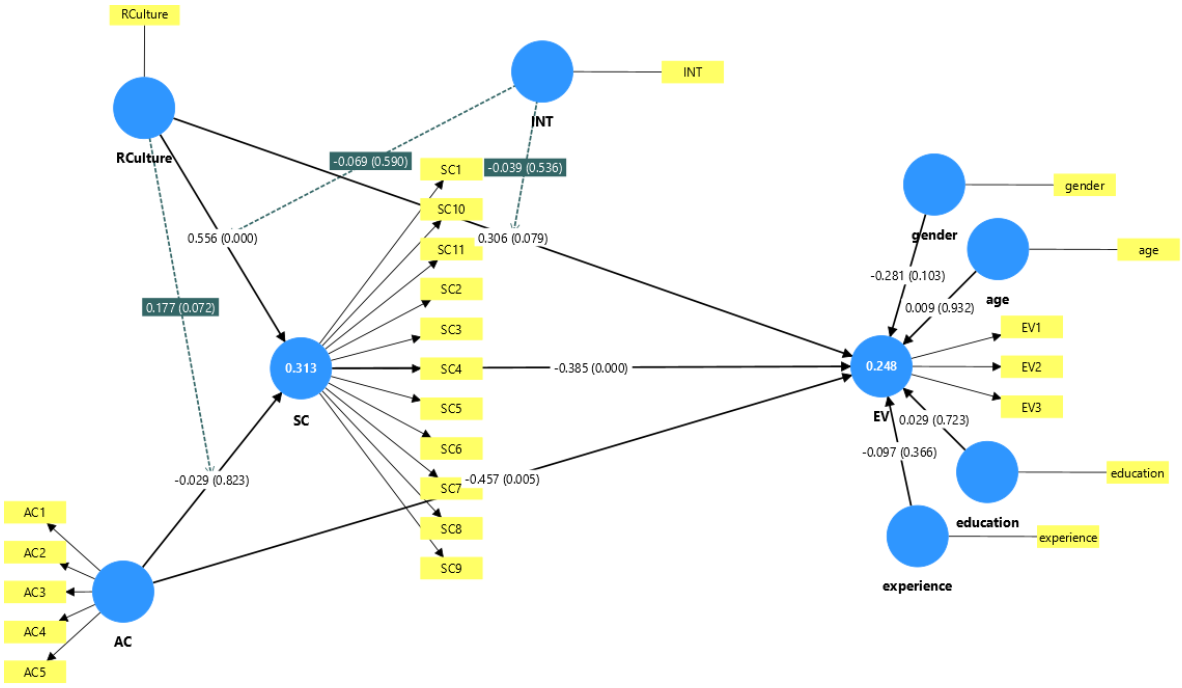
Construct and measurement items	Standardized factor loadings	t-values	p-values
Action Control (AC)			
AC1 I feel well informed by my supervisor about the activities I am expected to perform.	0.831	24.771	0.000
AC2 In my experience, my supervisor closely monitors how I perform the required activities.	0.850	18.959	0.000
AC3 I regularly receive feedback from my supervisor on whether I meet expectations**.**	0.817	17.882	0.000
AC4 My supervisor adjusts my activities when necessary**.**	0.782	13.905	0.000
AC5 I believe my supervisor would appreciate if I perform my activities well**.**	0.832	16.809	0.000
Self-Control (SC)			
SC1 I am good at resisting temptations, especially those related to financial decisions.	0.619	10.856	0.000
SC2 I am punctual and avoid delays or postponing my work tasks.	0.637	9.347	0.000
SC3 I am careful about what I say, especially in professional interactions.	0.768	15.755	0.000
SC4 I never allow myself to lose control, especially in high-pressure work situations.	0.716	15.218	0.000
SC5 I refrain from engaging in financial activities that are not beneficial, even if they appear to be.	0.518	6.474	0.000
SC6 I understand the importance of self-discipline in financial decisions.	0.829	21.393	0.000
SC7 I stay focused on my work tasks and do not get carried away by emotions.	0.765	15.779	0.000
SC8 I consider the consequences before making impulsive work-related decisions.	0.793	18.763	0.000
SC9 I think carefully before acting in work situations.	0.817	20.532	0.000
SC10 Pleasure and entertainment do not compromise my responsibilities at work.	0.731	14.558	0.000
SC11 I am effective in working toward long-term financial goals.	0.712	10.671	0.000
Exceptional violations (EV)			
EV1 Has it ever happened that your decisions were influenced by colleagues in stressful situations?	0.859	24.461	0.000
EV2 Have you ever acted according to your own method because you considered a rule or guideline unnecessary?	0.867	20.476	0.000
EV3 Have you ever adopted a creative method that involved a higher level of risk?	0.891	23.346	0.000

Construct	Cronbach's α	CR	AVE	*AC*	*INT*	*RCulture*	*SC*	*EV*
AC	0.882	0.913	0.677	**(0.823)**	0.503	0.373	0.103	0.110
INT	1.000	1.000	1.000	0.709	**(1.00)**	0.361	0.108	0.045
RCulture	1.000	1.000	1.000	0.611	0.601	**(1.00)**	0.288	0.030
SC	0.907	0.923	0.524	0.321	0.329	0.537	**(0.724)**	0.133
EV	0.844	0.906	0.762	–0.331	–0.213	–0.173	–0.365	**(0.873)**

Notes: Values above the diagonal are squared Pearson correlations, values on the diagonal are square roots of AVE (Fornell–Larcker criterion). Values below the diagonal are Pearson correlations.

Heterotrait-monotrait ratio (HTMT)	Original sample (O)	Sample mean (M)	2.5%	97.5%
EV ↔ AC	0.361	0.371	0.208	0.538
INT ↔ AC	0.754	0.748	0.635	0.838
INT ↔ EV	0.232	0.239	0.066	0.436
RCulture ↔ AC	0.660	0.658	0.517	0.788
RCulture ↔ EV	0.185	0.201	0.071	0.387
RCulture ↔ INT	0.601	0.600	0.469	0.719
SC ↔ AC	0.349	0.361	0.222	0.502
SC ↔ EV	0.421	0.422	0.258	0.597
SC ↔ INT	0.349	0.348	0.187	0.498
SC ↔ RCulture	0.562	0.562	0.416	0.694

Model C: Result of PLS-SEM estimation – Standardized path coefficients and *p*-values



Model C: Structural model estimation (SmartPLS 4.0)

Standardized Coefficients	Path	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/STDEV|)	P values
AC → EV		-0.457	-0.472	0.162	2.820	0.005
AC → SC		-0.029	-0.019	0.131	0.223	0.823
RCulture → EV		0.306	0.328	0.174	1.757	0.079
RCulture → SC		0.556	0.566	0.120	4.645	0.000
RCulture × AC → SC		0.177	0.171	0.098	1.800	0.072
SC → EV		-0.385	-0.391	0.098	3.914	0.000
INT → EV		0.048	0.040	0.135	0.353	0.724
INT → SC		0.039	0.014	0.128	0.303	0.762
INT × RCulture → EV		-0.039	-0.039	0.062	0.620	0.536
INT × RCulture → SC		-0.069	-0.053	0.129	0.539	0.590
age → EV		0.009	0.007	0.107	0.085	0.932
education → EV		0.029	0.028	0.083	0.355	0.723
experience → EV		-0.097	-0.103	0.107	0.905	0.366
gender → EV		-0.281	-0.291	0.173	1.629	0.103

Specific indirect effects	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/STDEV|)	P values

RCulture × AC → SC → EV	-0.068	-0.067	0.044	1.558	0.119
INT × RCulture → SC → EV	0.027	0.022	0.053	0.506	0.613
AC → SC → EV	0.011	0.009	0.053	0.214	0.831
INT → SC → EV	-0.015	-0.005	0.052	0.286	0.775
RCulture → SC → EV	-0.214	-0.223	0.081	2.627	0.009

Total effects	**Original sample (O)**	**Sample mean (M)**	**Standard deviation (STDEV)**	**T statistics (|O/STDEV|)**	**P values**
AC → EV	-0.446	-0.463	0.166	2.681	0.007
AC → SC	-0.029	-0.019	0.131	0.223	0.823
RCulture → EV	0.092	0.105	0.167	0.552	0.581
RCulture → SC	0.556	0.566	0.120	4.645	0.000
RCulture × AC → EV	-0.068	-0.067	0.044	1.558	0.119
RCulture × AC → SC	0.177	0.171	0.098	1.800	0.072
SC → EV	-0.385	-0.391	0.098	3.914	0.000
INT → EV	0.033	0.034	0.135	0.242	0.809
INT → SC	0.039	0.014	0.128	0.303	0.762
INT × RCulture → EV	-0.012	-0.017	0.082	0.144	0.885
INT × RCulture → SC	-0.069	-0.053	0.129	0.539	0.590
age → EV	0.009	0.007	0.107	0.085	0.932
education → EV	0.029	0.028	0.083	0.355	0.723
experience → EV	-0.097	-0.103	0.107	0.905	0.366
gender → EV	-0.281	-0.291	0.173	1.629	0.103