Vol. 15, No. 2, 35-61
doi:10.17708/DRMJ.2026.v15n02a02

Dynamic Relationships Management Journal

WHEN CONTROLS CREATE RISK: A REVIEW OF CONTROL PROBLEMS UNDERLYING OPERATIONAL RISK IN BANKING

Edona Haxhiu
School of Economics and Business, University of Ljubljana
edona.haxhiuu@gmail.com

Mojca Marc*
Associated professor
School of Economics and Business, University of Ljubljana
mojca.marc@ef.uni-lj.si

Abstract

Operational risk losses continue to expose persistent weaknesses in how banks manage and control risk, despite increasingly sophisticated regulatory frameworks. This study examines how behavioural management control problems contribute to the emergence and management of operational risk in banking. Using the Object of Control framework as a theoretical lens, we systematically review research published between 1995 and 2025 to explore how the design and use of management control systems (MCS) influence operational risk management (ORM) outcomes. Synthesising 59 studies across design and use, rules and procedures, structures, incentives, and culture, we show that regulatory-driven control architectures enhance accountability but often shift ORM toward auditability and compliance, producing procedural rigidity and reduced learning. We develop a two-stage explanation of how control problems translate into persistent operational risk exposure: first, design–use misalignment displaces the preventive and mitigating purposes of ORM and transforms risk controls into symbolic assurance; second, structural fragmentation or centralisation, misaligned incentives, and cultural norms stabilise this rigidity by weakening feedback loops and normalising compliance-oriented behaviour. The study advances a behavioural–systems perspective on operational risk, highlighting that resilience depends on aligning control design with enacted use and maintaining adaptive learning alongside regulatory assurance.

Keywords: *Management Control Systems, Control Problems, Operational Risk Management, Banking, Systematic Literature Review*

Statements and Declarations

Competing Interests: Authors declare no competing financial or non-financial interests.

Funding: This research was financially supported by the Slovenian Research Agency within the research program P5–0441. The funders had no role in the study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Data availability: This article is a systematic literature review and does not contain any primary data. All data analyzed during this study are derived from previously published sources, which are cited in the reference list.

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 events in 2023 reached €17.5 billion (an increase of 27 percent over 2022), while the number of loss events rose by 3.7 percent. The ORX Annual Banking Operational Risk Loss Data Report 2025 similarly shows 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 remains a critical challenge 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), and major banking failures have often been associated with deficiencies in internal control arrangements and human misconduct (Raghavan, 2003). Although operational risk management (ORM) frameworks have matured substantially since Basel II and have significantly strengthened governance and risk management in banks, their development has remained largely technical and compliance-driven, leaving limited insight into behavioural mechanisms and organisational dynamics.

Early ORM research primarily focused on quantitative modelling and capital allocation (e.g., Cruz et al., 1998; Cornalba & Giudici, 2004; Fontnouvelle et al., 2005; Power, 2005; Moosa, 2007), with limited attention to the organizational mechanisms underpinning risk. More recent studies shift the focus, and broaden the view of operational risk from a purely statistical construct to a managerial and behavioural phenomenon, increasingly embedded within management control systems (MCS). 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 management control practices.

To understand these behavioural sources of operational risk more systematically, we turn to the MCS literature. In the banking context, a subset of management control mechanisms is mobilised specifically for ORM, aiming to prevent operational risk events and mitigate their consequences. The global financial crisis of 2008 renewed attention to the behavioural underpinnings of control and risk, leading to reforms that strengthened governance, reporting, and compliance frameworks. Yet the persistence of control-related losses indicates that technical refinements alone are insufficient (Rad, 2016) and suggests that risk emerges not only from system failures but also from the ways in which controls are conceived, implemented, and enacted. This calls for an integrative perspective that views ORM as embedded within broader systems of managerial control and organizational behaviour. Understanding *how* management 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.

Prior literature has increasingly recognized this integration. Over the past two decades, risk management has evolved from a specialized financial discipline into an integral component of MCS (Merchant & Otley, 2006; Mikes, 2009; Soin & Collier, 2013; Arena & Arnaboldi, 2014; Lueg & Knapik, 2016; Peljhan, Sprčić & Marc, 2018). MCS have traditionally been conceptualized as tools for aligning managerial behaviour with organizational objectives, facilitating strategic coordination, and ensuring accountability (Anthony, 1965; Simons, 1995;

Malmi & Brown, 2008). 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. We focus on behavioural control problems, defined as dysfunctions arising from lack of direction, motivation, or personal limitations (Merchant & Van der Stede, 2012, 2014). In this context, the persistence of operational losses suggests that these objectives are not consistently achieved, even in environments characterised by increasingly formalised and sophisticated control architectures. The issue therefore lies not in the absence of control, but in how control systems are designed and used in practice, and how mechanisms intended to reduce operational risk may under certain conditions contribute to its emergence.

To address this gap, we conduct a systematic review of the literature on MCS and ORM in the banking sector. Drawing on the Object of Control Framework (OOC; Merchant and Van der Stede, 2017), we categorize and synthesize evidence on how control problems influence operational risk. The review is guided by two overarching research questions:

RQ1: How do management control problems emerge in the design and use of control systems used for operational risk management in banks?

RQ2: Through which organizational and behavioural mechanisms do these control problems undermine the purpose of operational risk management in banks?

Prior review and conceptual studies on ORM have primarily focused on regulatory frameworks, governance structures, risk measurement techniques, and risk culture (e.g., Power, 2007; Mikes, 2009; Soin & Collier, 2013). Related work linking MCS and risk management emphasizes the integration of controls into enterprise risk management frameworks and governance processes, often highlighting coordination, compliance, and accountability mechanisms (e.g., Merchant & Otley, 2006; Arena & Arnaboldi, 2014; Lueg & Knapik, 2016). While these studies provide important insights into how control systems are designed and embedded within risk governance architectures, they devote limited attention to behavioural control problems and the mechanisms through which the design and use of MCS may unintentionally contribute to operational risk.

This study responds to that need by linking the OOC framework 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), integrating them into a two-stage dynamic model. 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 control problems shape operational risk outcomes in the banking sector and why they persist despite increasingly sophisticated risk management systems. By synthesizing the literature published between 1995 and 2025, the review clarifies how MCS, when misaligned with organizational context or behavioural dynamics, can become sources of operational vulnerability.

The remainder of the paper is structured as follows. The next section outlines the theoretical foundations that connect MCS and ORM, defining the key concepts that motivate the systematic review. A Method section follows with an explanation of the research approach. The Findings section presents the synthesis based on the predefined analytical dimensions and introduces the two-stage dynamic model. Finally, the Discussion and Conclusion sections summarize the contributions and implications of the study.

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) (Soin & Collier, 2013).

Both domains address how organizations seek to influence behaviour, ensure accountability, and manage uncertainty, yet they have evolved largely in parallel: MCS within management accounting and organizational control, and ORM 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; Simons, 1995; Malmi & Brown, 2008). 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) as 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 (Power, 2005, 2009; Mikes, 2009, 2011) 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—an organizational response that seeks to demonstrate control externally but may suppress learning and adaptability internally. 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. In banking, the control mechanisms of ORM are introduced with two fundamental objectives: to reduce the probability of operational risk events and to mitigate their impact when such events occur (Chapelle, 2008). Preventive controls aim to influence behaviour ex ante through standardisation, procedural guidance, and oversight, while mitigating controls support timely detection, escalation, containment, and organisational learning following failures (Xu et al., 2020; Heimeriks et al, 2012).

An important normative reference for understanding effective risk management in banking are the strategic and enterprise risk management (ERM) frameworks. Practitioner-oriented models and regulatory guidelines typically emphasise integration of risk management with strategy, clear risk ownership, coherent structures, aligned incentives, and a strong risk culture (e.g., COSO, 2017; Bromiley et al., 2015; Arena et al., 2010; Sax & Torp, 2015). These frameworks implicitly assume that control systems function as enabling mechanisms that support learning, coordination, and informed decision-making. However, they offer limited insight into how these principles are enacted in practice, or why formally well-designed risk management architectures often fail to deliver their intended benefits.

To complement this literature, we adopt a management control perspective and analyse these interactions based on Merchant and Van der Stede's (2017) Object of Control Framework (OOC). This framework distinguishes four complementary types of control: result, action, personnel, and cultural. Result controls steer behaviour through measurable outcomes and incentive systems; action controls prescribe or restrict specific behaviours; personnel controls focus on selecting and developing competent and motivated employees; and cultural controls embed shared values and norms that guide action in uncertain or ambiguous situations. To enable a more granular synthesis of the reviewed literature, these theoretical control types were operationalized into four analytical categories that capture recurring themes in the ORM context: rules and procedures, structure, incentives, and culture (Table 1). *Rules and*

procedures correspond to action controls in the OOC, encompassing the formal standards, processes, and regulatory mechanisms that prescribe acceptable behaviour and constrain operational variability. *Structure* reflects organisational arrangements that shape accountability and communication in risk management systems. *Incentives* derive from result controls, capturing the motivational and performance-based mechanisms that align individual objectives with organizational risk tolerance. *Culture* represents cultural controls, encompassing shared norms, values, and ethical orientations that influence risk perception, behavioural compliance, and collective learning. By synthesizing empirical findings through these four categories, the review translates Merchant and Van der Stede's abstract OOC typology into a framework specifically tailored for analysing control problems within the operational risk domain. This approach not only provides conceptual coherence across diverse studies but also enables a systematic examination of how design and use of controls across different control objects contribute to operational risk outcomes in banking.

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). The framework therefore provides an analytical lens for examining how design and behavioural failures in these control domains translate into operational vulnerabilities.

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 (i.e. rules, procedures, and escalation processes), while MCS provides the behavioural infrastructure (i.e. 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 formal risk management systems may generate extensive information without necessarily becoming integrated into managerial decision-making, particularly where performance pressures and incentive systems prioritise short-term financial outcomes over prudent decision-making. Similarly, Lim et al. (2017) show that risk management practices in banks are shaped by tensions between formal oversight and the need for open communication, which may limit the effective use of risk-related information in practice. Rad (2016) similarly shows that regulatory frameworks, when operationalised through internal procedures, may not fit local process requirements, which can create overlaps and coordination difficulties. More recent worky by Ringgaard et al. (2025) suggests that boundary and belief systems are most effective in supporting ORM when they are applied interactively, indicating that how controls are implemented in practice can 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 ac-

Table 1: Mapping the Object of Control (OOC) framework to analytical categories used in the systematic literature review

Object of Control (Merchant & Van der Stede, 2017)	Analytical Category	Illustrative Focus in Operational Risk Management Context
Action Controls	Rules and Procedures	Compliance routines, standardization, procedural rigidity
Personnel Controls	Structure	Organizational hierarchies, risk ownership, coordination
Result Controls	Incentives	Reward systems, performance metrics, fairness perception
Cultural Controls	Culture	Norms, values, ethical climate, openness to reporting

tivities 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: the two systems are often treated as distinct domains (one managerial, the other regulatory) rather than as interdependent layers of control. The behavioural dimension of operational risk remains comparatively under-specified (Faugere & Stul, 2021); while dysfunctions such as symbolic compliance (audit-trail driven verification) and gaming of operational risk regimes are acknowledged in the broader risk and operational risk literature (Power, 2009; Aldasoro et al., 2020), few studies trace *how* these arise from the design or use of specific control mechanisms. Finally, the contextual particularities of banking—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.

3 METHOD

3.1 Research Design

Given the fragmentation of research on MCS and ORM across several disciplines, 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 (Tranfield, Denyer, & Smart, 2003; Denyer & Tranfield, 2009). 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 & 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 management.

3.2 Search and Selection Strategy

The literature search 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 2, 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").

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 (Simons, 1995; Merchant & Van der Stede, 2003–2017). To ensure methodological transparency and replicability, the process and reporting followed the PRISMA stages of identification, screening, eligibility, and inclusion (summarized in Figure 1; Page et al., 2021).

Inclusion criteria were applied at two stages. During title/abstract screening, records were retained if they (i) addressed MCS/internal control systems and/or ORM/risk governance, (ii) related to banking/financial institutions or provided clearly transferable insights to banking, and (iii) indicated a focus on control design, control use/enactment, or behavioural/organizational consequences relevant to operational risk. During full-text eligibility assessment, studies were included if the full paper contained substantive conceptual or empirical material linking control mechanisms (rules/procedures, structure, incentives, or culture) to ORM or operational risk outcomes.

Exclusion criteria were also applied in two stages. During title/abstract screening, records were excluded when they were clearly unrelated to MCS/ORM, focused on non-banking contexts without transferable implications, or were purely technical/quantitative modelling papers without organizational or behavioural content. During full-text assessment, papers were excluded when they (i) focused exclusively on credit risk or market risk, (ii) lacked a control-system lens (no discussion of control design/use or behavioural consequences), or (iii) were not available in English.

Records retrieved from all sources were exported and merged into an Excel dataset. Duplicate records were identified and removed using a combination of DOI matching, title comparison, and author–year checks, with manual verification applied to ambiguous cases. Database-level filters were applied where available (English language; publication years 1995–2025; and peer-reviewed sources when supported by the database interface). All records identified through supplementary searching were subjected to the same inclusion and exclusion criteria during screening. As shown in Figure 1, these steps reduced the initial yield (n = 3,831) to the deduplicated and filtered screening set (n = 486). Title/abstract screening was conducted by Author 1 using the predefined criteria. To enhance screening consistency, Author 2 independently screened a subset of records (n = 75) and reviewed all borderline exclusions. Disagreements were discussed and resolved by consensus before proceeding to full-text eligibility assessment. Following title and abstract screening, 125 records were retained for full-text eligibility assessment, of which 59 met all inclusion criteria and were included in the final synthesis.

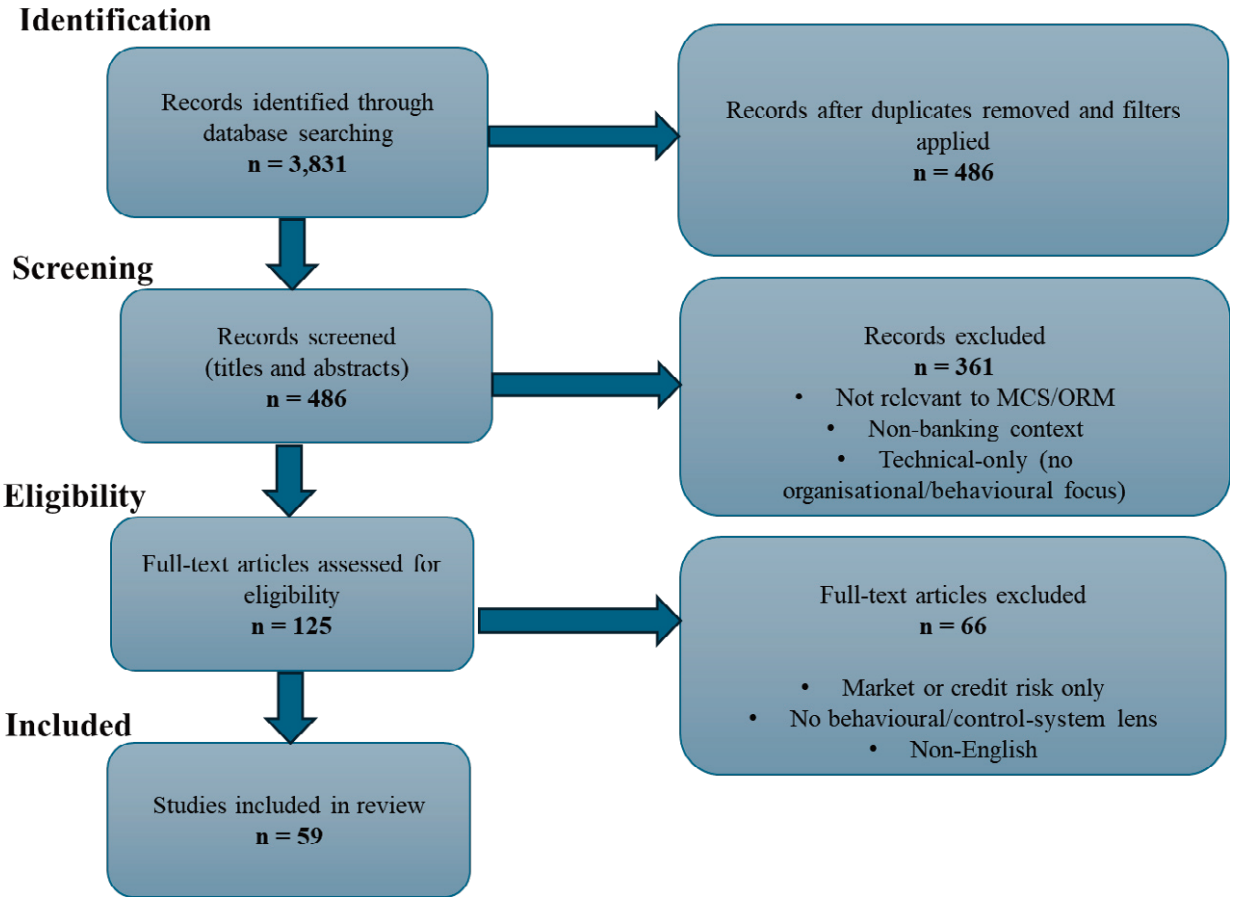
Table 2: Search Strategy

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 bankingOperational 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**

Note: The search strings, documented in Table 2, were iteratively developed to capture conceptual overlaps between MCS and ORM and refined during searches to balance sensitivity and specificity.

Source: Authors' own.

Figure 1: PRISMA-style flow diagram of the literature selection process



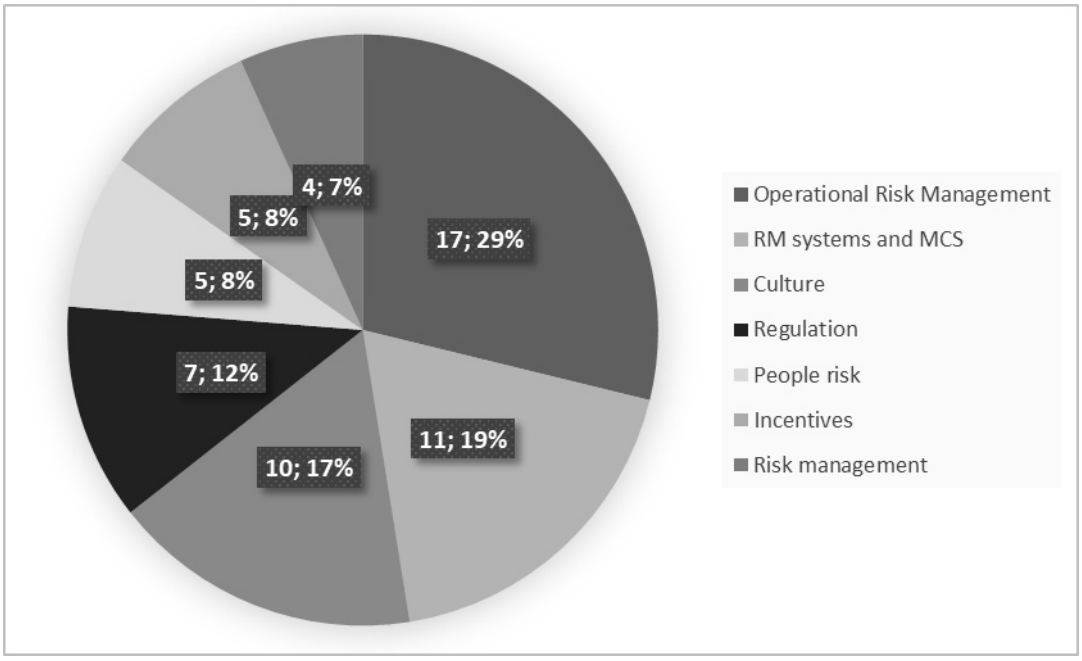
Source: Authors' own.

3.3 Data Analysis and Synthesis

All retained studies were coded manually using a structured analytical framework adapted from the OOC framework with coding outcomes summarized in Table 1. Each publication was examined to identify (1) the element of ORM addressed (design, use, or context), (2) the control object involved (rules, structure, incentives, or culture), (3) the control problem mechanism (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 (Mikes, 2009; Arena et al., 2010; Soin & Collier, 2013) and refined iteratively as patterns emerged across the reviewed studies. To enhance coding consistency, both authors applied the same coding logic and jointly discussed ambiguous or borderline cases (e.g., studies addressing both control design and enacted use) until consensus was reached. This iterative comparison helped ensure consistent interpretation of coding categories across the dataset.

Among the 59 papers retained for analysis, 17 focus specifically on ORM and 4 address risk management in general; 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 behavioural risk, and 5 analyse incentives-related risk (Figure 2).

Figure 2: Distribution of main topics in the retained records (n= 59)



Source: Authors' own.

A qualitative thematic synthesis approach was used to integrate findings across studies, focusing on how MCS design and use influence ORM performance and risk outcomes. Five overarching analytical dimensions guided the synthesis and presentation of findings:

- Design & Use – how control structures and system architectures are configured and how are they enacted or interacted with 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

Analytical attention centred on recurrent control problems that contribute to operational risk exposure such as information silos, compliance-driven rigidity, and incentive misalignment (Power, 2009; Butler & Brooks, 2024). 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 illustrates how recurring management control problems are associated with operational risk exposure in banking organizations.

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

4 FINDINGS

Our synthesis shows that although ORM systems are originally intended and formally designed to manage uncertainty, they are often enacted in ways that suppress discretion, judgement, and feedback from operational practice, resulting in detachment from their purpose and diminished effectiveness. The following subsections trace this dynamic by examining how design–use misalignment emerges (4.1), how it is expressed through rules and procedures (4.2), and how it becomes institutionalised and normalised through organisational structure (4.3), incentives (4.4), and culture (4.5).

4.1 Design and Use Misalignment

The reviewed literature consistently shows that problems in ORM originate not from a lack of control structures, but from a misalignment between how control systems are designed and how they are used in practice. In the context of ORM, *design* refers to the formal configuration of rules, procedures, reporting routines, and oversight arrangements that determine how operational risks are identified, measured, and mitigated (Mikes, 2009; Ferreira & Otley, 2009). Design issues concern the adequacy, integration, and coherence of systems governing risk identification, internal controls, and oversight structures (Soin & Collier, 2013; Arena et al., 2010). 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* of ORM systems refers to how controls are enacted in day-to-day operations (Ahrens & Chapman, 2007), including whether they stimulate dialogue and learning or function primarily as instruments of monitoring and compliance (i.e. are used interactively or diagnostically; Simons, 1995).

Across 21 identified studies examining the design and use of RMS (including ORM), the dominant pattern is that ORM in banking is *designed* under strong regulatory and institutional pressures that prioritize documentation, formal accountability, standardization and quantification (Power, 2005). In response to Basel-driven requirements, banks have developed extensive control architectures that translate regulatory expectations into detailed procedures, documentation practices, and risk reporting frameworks (Berger et al, 2022). While such designs enhance transparency and external legitimacy, they frequently embed a compliance-oriented logic that prioritizes procedural completeness over managerial judgement and adaptive learning (Power, 2005; Mikes, 2009, 2011). Preventive controls typically dominate (e.g., authorization procedures, segregation of duties), whereas detection and corrective design features are often underdeveloped. This imbalance reduces responsiveness to control failures, delays risk mitigation (Abdul Rahim et al., 2018; Chernobai et al, 2022), and may, paradoxically, weaken risk-awareness.

This design orientation shapes how controls are *used* in practice. Rather than functioning as interactive mechanisms that support sensemaking about emerging operational threats, ORM systems are predominantly applied diagnostically, to demonstrate adherence to predefined standards and indicators (e.g. Deschamps, 2019; Ringgaard et al., 2025). Risk management thus becomes a reporting obligation rather than an integral part of operational decision-making. Power (2009) describes this shift as a transformation of ORM into a "ritual of verification," where documentation substitutes for reflection and substantive engagement with risk. Empirical studies show that risk information in such settings is collected, analysed, and audited, but only weakly connected to managerial action (Lim et al., 2017; Ringgaard et al., 2025; Slapničar et al., 2025).

At the same time, the literature indicates that the way ORM systems are used can either amplify or mitigate design weaknesses. Where used narrowly and diagnostically, ORM design flaws such as rigidity and fragmentation tend to be reinforced (e.g. Ringgaard et al., 2025; Slapničar et al., 2025). By contrast, when managers use controls interactively, control systems can partially compensate for design limitations (Marc, Arena, & Peljhan, 2023; Ringgaard et al., 2025) because interactive use facilitates integrating risk data into strategic and operational decision-making.

The literature therefore converges on the *design–use misalignment* as a central explanation for ineffective ORM. Although ORM systems are formally designed to manage uncertainty and support resilience, they are used in ways that suppress discretion, judgement, and feedback from operational practice. Designs oriented primarily toward external assurance tend to crowd out the interactive and interpretive uses necessary for learning, sensemaking, and adaptation. As summarized in table 3, this misalignment manifests through fragmented ORM designs (Molamohamadi et al., 2024; Soin & Collier, 2013; Hall et al., 2015), weak integration of risk information into managerial decision-making (Göstl & Schwaiger, 2016; Soin & Collier, 2013), and limited feedback loops (Muermann & Oktem, 2002), which collectively limit learning and undermine adaptive capacity of ORM. Several authors further note that incidents are documented ex post but rarely translated into changes in processes or behaviours (e.g.

Rad, 2016; Florio & Leoni, 2017), allowing operational risk to persist when technical and procedural designs fail to align with human factors, incentives, and behavioural reliability (Xu et al, 2017).

Overall, the findings indicate that ORM effectiveness depends less on the technical sophistication of control system design than on the alignment between design and use. In highly regulated banking environments, formal control architectures remain necessary to ensure legitimacy and accountability. However, when these systems are enacted primarily as compliance devices, they may lose their adaptive capacity and become sources of rigidity (e.g. Muermann & Oktem, 2002; Slapničar et al., 2025). From an ex ante perspective, design–use misalignments weaken the ORM preventive role when controls are applied rigidly or symbolically. For example, procedures that are designed to guide judgement become checklists and training intended to enhance risk awareness becomes a formal requirement. In such cases, controls may not meaningfully alter behaviour and therefore fail to reduce the likelihood of operational risk events (Florio & Leoni, 2017). From an ex post perspective, misalignments undermine the mitigating capacity by limiting feedback and learning (Muermann & Oktem, 2002). For example, incident reporting systems and loss databases are designed to capture failures and support remediation, yet when used primarily for audit or regulatory purposes, they tend to discourage openness and suppress reflection. Instead of enabling timely response and organisational learning, controls become mere instruments of verification, delaying escalation and reducing the organisation's ability to contain losses or prevent recurrence (Soin & Collier, 2013).

These findings do not suggest that ORM control elements lack value or lose relevance because their objectives are ill-defined; rather, they show that such outcomes arise when their use becomes detached from their underlying purpose. When ORM is enacted primarily to satisfy formal requirements, its preventive and mitigating functions are displaced by symbolic assurance.

4.2 Rule and Procedure Problems

Rules and procedures represent the most visible and formalised component of ORM systems. In this context, they are primarily introduced as preventive controls, intended to reduce the likelihood of risk events by standardising processes, constraining unsafe behaviour, and guiding employee judgement (Chapelle et al., 2008; Dahen & Dionne, 2010). To a lesser extent, procedural frameworks are also expected to support mitigating functions by, for example, enabling timely escalation, documentation of incidents, and learning from failures (Xu et al., 2020). Across 13 reviewed studies, however, the literature indicates that both objectives may be undermined when procedural controls prioritise formal compliance over behavioural effectiveness, as summarized in Table 4.

A clear pattern emerging across these studies is the progressive *over-formalization* of rules and procedures in response to regulatory pressure. As banks translate regulatory frameworks into increasingly detailed internal procedures, checklists, and documentation routines, procedural systems often become detached from operational realities. Several

Table 3: Design and Use Issues

Design & Use Issues	
Misalignment pattern • *Compliance-oriented control design and diagnostic use* • *Fragmented risk systems and parallel control structures* • *Limited feedback and learning mechanisms*	**Consequences for ORM** • *Symbolic assurance replaces behavioural risk control* • *Risk information weakly embedded in managerial decision-making and action* • *Reduced adaptability and responsiveness to emerging risks*
Example studies: Power (2005); Mikes (2009, 2011); Soin & Collier (2013); Rad (2016); Abdul Rahim et al. (2018); Florio & Leoni (2017); Göstl & Schwaiger (2016); Lim et al. (2017); Slapničar et al. (2025); Marc, Arena & Peljhan (2023); Ringgaard et al. (2025)	

Source: Authors' own.

studies observed that while formalization of risk procedures can improve accountability and standardization, excessive reliance on prescriptive rules shifts the function of procedures from guiding action to *showing compliance* (e.g. Florio & Leoni, 2017; Mabwe et al, 2022; Bardoscia & Bellotti, 2012; Lim et al, 2017). This dynamic is particularly pronounced during crises, when procedural redesign aimed at restoring order and legitimacy initially improves coordination but gradually reinforces rigidity and overregulation (Rikhardsson et al., 2021).

As a result, adherence to rules becomes an end to itself and procedural controls become symbolic representations of control rather than mechanisms that meaningfully influence behaviour or reduce operational risk exposure (Power, 2009; Soin & Collier, 2013). At the behavioural level, this over-formalisation displaces professional judgement and situational awareness. Empirical studies show that employees and managers often focus on completing prescribed steps and producing required documentation, rather than engaging with the underlying risk logic that procedures are meant to address (e.g. Lim et al., 2019; Ringgaards et al., 2025). Preventive controls therefore lose their capacity to influence behaviour ex ante, as procedures are followed mechanically rather than reflexively, limiting their effectiveness in reducing the likelihood of operational failures (Moosa, 2017). The mitigating function of ORM is also weakend when procedures like incident reporting and escalation protocols are used primarily for audit or regulatory purposes. The reviewed studies document two reasons for this substitution of effective ORM with mere rule-following: i) avoiding perceived excessive administrative burden (Lim et al., 2019; Ringgaards et al., 2025; Moosa, 2017; Power, 2005) and ii) avoiding blame due to fear from punishment (Mabwe et al., 2022; Gurd & Helliar, 2017). In these cases, procedures do not facilitate containment or learning but instead contribute to delayed responses, suppressed reporting, and limited learning from failures.

The literature further highlights that procedural problems are often amplified by *fragmentation and inconsistency in procedural requirements across organisational levels*. Centrally designed rules are frequently misaligned with local operational realities, leading to over-formalization and conflicting requirements (Rad, 2016, Sabanova and Kudinska, 2022) that weaken feedback loops essential for risk mitigation. Front-line employees must navigate multiple, overlapping rule systems that are difficult to reconcile with the pace and complexity of operational work, which increases cognitive load and error probability, while simultaneously reducing the perceived relevance of procedural controls (Sabanova and Kudinska, 2022). As a consequence, rules intended to reduce risk may paradoxically increase it by diverting attention away from critical judgement and situational awareness.

Some studies emphasise that procedural problems are not inherent to formalisation per se, but to how procedures are used and interpreted by employees. Where managers encourage dialogue around rules, allow for discretion, and treat procedures as evolving guides rather than fixed constraints, procedural controls can function as enabling mechanisms that support learning and responsiveness (Gurd and Helliar, 2017). Conversely, when *procedures are enforced rigidly*, they reinforce superficial compliance-oriented behaviour and suppress substantive understanding of risk (Mabwe et al., 2022). Procedural controls thus do not fail because rules exist (Ranjan, 2025), but because their use becomes detached from preventive and mitigating purposes.

Overall, rule and procedure problems form a pathway through which design-use misalignments undermine ORM. Over-formalization leads to rigidity and detachment from practice, turning preventive controls into compliance rituals and weakening mitigating by limiting timely reporting and learning.

4.3 Structural and Organizational Problems

Across 16 studies in our review, structural and organizational arrangements are identified as shaping how ORM systems function in practice (summarized in Table 5). When ORM is embedded in organisational structures that fragment responsibilities, constrain communication, or distance decision-making from operational processes, even well-designed control mechanisms lose their preventive and mitigating effectiveness (Cornwell et al., 2023; Soin & Collier, 2013; Mabwe et al., 2022). Moreover, the reviewed literature implies that

Table 4: Rules and Procedure Issues

Rules and Procedures Issues	
Patterns • *Over-formalization of rules and procedures; prescriptive procedural design* • *Compliance-oriented design and evaluation of procedures* • *Rigid enforcement of rules* • *Fragmentation, inconsistency, and overload or procedural requirements*	**Consequences for ORM** • *Symbolic ORM control and weakened risk prevention* • *Displacement of professional judgement* • *Increased error probability* • *Delayed response, limited learning, and weakened risk mitigation*
Example studies: Power (2005); Mikes (2009, 2011); Soin & Collier (2013); Rad (2016); Abdul Rahim et al. (2018); Florio & Leoni (2017); Göstl & Schwaiger (2016); Lim et al. (2017); Slapničar et al. (2025); Marc, Arena & Peljhan (2023); Ringgaard et al. (2025)	

Source: Authors' own.

structural problems do not merely coexist with procedural over-formalisation, but actively stabilise existing design–use misalignments.

The dominant identified pattern is *excessive functional fragmentation*. ORM, compliance, internal audit, and business units are frequently organised as parallel systems with distinct mandates, reporting lines, and performance criteria (Soin and Collier, 2013). While such separation is intended to enhance independence and accountability, it often results in siloed information flows and limited cross-functional learning (e.g. Al-Amri & Davydov, 2016; Butler & Brooks, 2024), even in organisations that have invested in modernisation efforts (Cornwell et al., 2023). The main issue is that risk information is generated and processed within specialised units but remains weakly integrated into operational decision-making. As a consequence, control systems operate alongside, rather than within, core business processes, reducing their capacity to influence behaviour ex ante or to support timely response ex post. In this sense, the issue is not risk ownership *per se*, which is widely regarded as good practice, but the lack of structural and informational integration that prevents risk frameworks from functioning as an effective, organization-wide control mechanism. Closely related to fragmentation is *ambiguity in responsibility and escalation*, particularly in the implementation of formal governance models such as the Three Lines of Defence (3LoD). Empirical evidence shows that, despite conceptual clarity, these structures often generate overlapping mandates, poorly coordinated interfaces, and uncertainty regarding risk ownership in practice (Lim et al., 2017; Mabwe et al., 2022). This also leads to duplication of controls in some areas and gaps in others, weakening accountability and delaying escalation, which in turn undermine both the preventive and mitigating purposes of ORM systems.

The literature further highlights *excessive centralisation* as a recurrent structural problem. Centralised risk functions are designed to ensure consistency, standardisation, and regulatory alignment across large banking organisations, yet when decision authority and control design are concentrated at the centre, local operational knowledge is marginalised (Rad, 2016). Front-line managers and employees often perceive centrally imposed risk frameworks as disconnected from operational realities, reducing engagement and responsiveness (Rad, 2016; Sabanova & Kudinska, 2022). This structural distance limits the organisation's ability to detect weak signals and emerging risks at their source and slows response when incidents occur (Rad, 2016). Similar consequences also emerge from the *weak vertical integration* between ORM and governance structures. Several studies show that ORM is frequently positioned at intermediate organisational levels (Hartmann & Slapničar, 2007; Ringgaard et al., 2025), with limited influence on strategic decision-making or board-level discussions (e.g. Siaw Ofori et al, 2025; Gontarek, 2016; Cerasi & Oliviero, 2015). As a result, risk information is filtered, aggregated, or reframed as it moves upward, reducing its relevance for strategic choices and resource allocation. This reinforces the perception of ORM as a compliance function rather than a strategic MCS.

Finally, structural arrangements *interact* closely with cultural and behavioural dynamics. Hierarchical reporting lines, rigid communication structures, and performance pressures can discourage upward communication about errors and near misses (Cohn et al., 2014; Gurd & Helliar, 2017), leading employees to manage impressions rather than risks. Structural rigidity can therefore reinforce behaviours that limit learning and adaptation, turning organisational design features into persistent sources of operational vulnerability (e.g. Yokoi-Arai, 2023; Wright, 2018).

Fragmentation, centralisation, and weak vertical integration do not merely constrain information flows, they strengthen compliance-oriented use of ORM and suppress learning. As a result, ORM systems may become structurally insulated from operational practice, reducing their capacity to prevent risk events and to mitigate their consequences. Improving ORM therefore requires not only well-designed control elements (e.g. rules and frameworks), but also organisational structures that enable integration, dialogue, and shared accountability across functional and hierarchical boundaries.

4.4 Incentive-Related Control Problems

Incentive systems represent a critical touching point between organisational MCS design and individual action. From a risk management perspective, incentive mechanisms are expected to align employee behaviour with the organisation's risk appetite by reinforcing prudent conduct, accurate reporting, and long-term resilience. The reviewed literature (12 studies) shows, however, that incentive-related control problems often undermine these objectives by translating structural and procedural misalignments into behavioural distortions that increase operational risk exposure. We identified four types of patterns (summarized in Table 6): 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 *misalignments between performance incentives and risk management objectives* increase banks' exposure to operational and reputational risks (e.g. Faugère & Stul, 2021; Butler & Brooks, 2024; Caretta et al, 2024; Cerasi & Oliviero, 2015). Incentive systems in banking continue to emphasise short-term financial outcomes (e.g. revenue growth, efficiency, or cost reduction) while operational risk considerations are weakly integrated into performance evaluation and reward structures. When rewards are tied primarily to financial metrics, risk-related controls become less influential in guiding behaviour and decision-making. Empirical evidence shows that incentive misalignments not only encourage moral hazard, short-termism, and manipulation, resulting in excessive

Table 5: Organisational and Structural Issues

Organisational and Structural Issues	
Patterns • *Functional fragmentation (siloed departments)* • *Unclear and overlapping responsibilities* • *Excessive centralization of risk function* • *ORM positioned at intermediate organizational levels, weakly connected to board-level decision-making* • *Interaction of structure with cultural and incentive pressures (rigid hierarchical communication and reporting lines)*	**Consequences for ORM** • *Siloed risk information, control gaps and limited cross-functional learning* • *Delayed escalation, weak integration of risk information into operational decision-making* • *Marginalisation of local knowledge, weakened identification of emerging risk* • *ORM perceived as compliance function, with limited strategic influence* • *Limited upward communication about errors and people-risks, reduced organisational learning*
Example studies: Power (2005); Mikes (2009, 2011); Soin & Collier (2013); Rad (2016); Abdul Rahim et al. (2018); Florio & Leoni (2017); Göstl & Schwaiger (2016); Lim et al. (2017); Slapničar et al. (2025); Marc, Arena & Peljhan (2023); Ringgaard et al. (2025)	

Source: Authors' own.

risk-taking, but also distort information flows and weaken ethical norms (Acrey et al., 2011; Cohn et al., 2014; Murphy, 2001). In this way, incentive misalignments weaken the preventive function of ORM by promoting risk-taking behaviours that controls are intended to constrain. Moreover, several studies indicate that banking organisational culture itself can amplify the effects of misaligned incentives (e.g. Faugère & Stul, 2021; Posch, 2020; Caretta et al, 2024) by reinforcing performance-oriented norms and professional identities (Cohn et al., 2014), leading to "ethical blindness" (Palazzo et al., 2012).

A third recurring pattern concerns *subjective performance evaluation* in incentive-based management control because it influences fairness perceptions and subsequent behavioural compliance. When risk-related behaviours are assessed inconsistently or opaquely, employees may perceive evaluation processes as arbitrary or biased, leading to reduced motivation for compliance and more opportunistic behaviour (Tran et al., 2021). This undermines both main objectives of ORM by weakening incentives to report issues accurately, escalate problems, or invest effort in risk-reducing actions. Finally, some studies show that *regulatory-driven formalization* of ORM can obscure incentive-driven misconduct (Moosa, 2017; Power, 2009). When bank managers focus on measurable compliance indicators and diagnostic control, incentives may become detached from actual risk outcomes (e.g. Liang et al, 2024; Ringgaard et al., 2025) as individuals are rewarded for demonstrating compliance rather than for actively reducing risk or mitigating the consequences of failures. As a result, such incentive systems reinforce symbolic assurance rather than substantive risk management.

Misaligned incentives, amplified by cultural and regulatory pressures, may lead to excessive risk-taking, blurred ethical boundaries, and opportunistic behaviour, undermining both the preventive and mitigating purposes of ORM. The findings collectively indicate that operational risk cannot be effectively managed without addressing the behavioural responses induced by incentive systems that conflict with risk management objectives.

4.5 Cultural-based Problems

The reviewed literature highlights organisational culture as a deeper layer through which management control problems become embedded and normalised over time. Culture-based problems shape how ORM mechanisms are interpreted and enacted in practice, influencing whether formal controls reinforce learning and accountability or gradually lose behavioural influence. While rules, structures, and incentives define the formal architecture of ORM systems, organisational culture determines how these mechanisms are understood, applied, and ultimately sustained in practice. Across 19 reviewed studies, the literature consistently shows that when cultural norms become misaligned

Table 6: Incentive-related Issues

Incentive-Related Issues	
Patterns • *Misalignment between financial performance incentives and risk objectives* • *Ethical distortion reinforced by banking culture and professional identity* • *Subjective or opaque performance evaluation* • *Regulatory-driven incentive evaluation focused in compliance*	**Consequences for ORM** • *Moral hazard, short-termism, manipulation, leading to increased operational risk exposure* • *Excessive risk-taking, normalisation of unethical behaviour, and undermined preventive controls* • *Opportunistic behaviour, weakened motivation for risk prevention and mitigation* • *Symbolic compliance, detachment of incentives from actual risk outcomes*
Example studies: Acrey et al. (2011); Cohn et al. (2014); Murphy (2001); Huston & James (1995); Tran et al. (2021); Moosa (2017); Power (2009); Ringgaard et al. (2025)	

Source: Authors' own.

with the preventive and mitigating purposes of ORM, formal controls lose behavioural influence and risk-related failures become normalised (e.g. Channon et al, 2025; Edwards & Wolfe, 2004; Ashraf et al, 2016; Caretta et al, 2024). Several studies find that a strong control culture promotes integrity, learning, and accountability, whereas weak or misaligned culture may normalise deviance, erode ethical standards, and reproduce control failures (Cohn et al, 2014; Lui, 2015; Mikes, 2009; Power, 2009; Gurd & Helliar, 2017; Sabanova & Kudinska, 2023). Cultural dynamics often stabilise existing design–use misalignments by embedding compliance-oriented practices into everyday routines (Kunz & Heitz, 2021; Faugère & Stul, 2021). Table 7 summarizes the cultural factors identified as contributing to persistent operational risk exposure, including leadership style (tone at the top), specific banking identity and competitive culture, and a cultural fear of mistakes.

The first recurring pattern concerns *leadership framing and tone-at-the-top. S*everal studies show that leadership behaviour strongly shapes how employees interpret risk controls and risk responsibilities (e.g. Butler & Brooks, 2024; Carpenter et al, 2021; Kunz & Heitz, 2021). Where senior management communicates risk management primarily as a compliance requirement, risk policy is interpreted as a bureaucratic formality rather than a shared responsibility, and has a weak motivational impact (Brauman et al, 2020). Conversely, where managers interactively engage employees in open discussions of risk issues and failures, they foster cultural norms supporting collective vigilance and learning that make risk culture stronger (Kunz & Heitz, 2021) and reduce operational exposure (Gurd & Helliar, 2017). Leadership communication therefore functions as a critical cultural control mediating the formal systems' influence on behaviour, and can either reinforce or undermine ORM effectiveness.

Several studies also point to a second pattern relating to *banking identity and competitive performance culture*. Misconduct is not merely an individual failure but may be a product of the institutionalized behavioral expectations within the banking culture (e.g. Holland, 2019; Faugère & Stul, 2021; Laguecir & Leca, 2022). Empirical evidence shows that strong professional identification with banking roles can increase tolerance for opportunistic behaviour in incentivized tasks compared to control groups (Cohn et al., 2014), while competitive performance cultures may normalise greed, recklessness, and dishonesty across hierarchical levels, sometimes even escalating into systemic misconduct (Lui, 2015). In such environments, cultural norms reinforce incentive-driven behaviour, increasing the likelihood that small deviations escalate into significant operational risk events.

Another pattern identified in the literature concerns *fear-based cultures* leading to defensive routines (e.g. Faugère & Stul, 2021; Frese & Keith, 2015; Carretta et al, 2024). When risk management is associated with blame or negative (career) consequences, employees may avoid reporting problems or experimenting with learning-oriented practices (Mikes, 2009; Power, 2009). These cultural patterns suppress feedback loops and limit adaptive learning due to the stigma attached to mistakes (Sabanova & Kudinska, 2023, 2024). Instead of surfacing emerging risks, ORM controls may thus inadvertently encourage silence and impression management, weakening both preventive and mitigating capacities.

We can thus conclude that dysfunctional cultures, driven by leadership framing, excessive competitive identity, or fear-based control environments, may convert temporary control weaknesses into enduring organisational traits. Culture thus also represents a pathway through which management control problems become stabilised and normalised over time, undermining both the preventive and mitigating purposes of ORM systems.

4.6 Summary of findings

Across the five analytical dimensions, our findings explain how MCS used for ORM may themselves become sources of risk. Rather than representing isolated problem areas, issues related to design and use, rules, structure, incentives, and culture form an interrelated sequence through which control effectiveness gradually deteriorates. We conceptualise this process as a two-stage dynamic linking control misalignment to persistent operational risk exposure (illustrated in Figure 3). The first stage explains how management control problems emerge through misalignment between the

Table 7: Culture-based Issues

Culture-based Issues	
Patterns • *Compliance-oriented leadership framing and weak tone at the top* • *Banking identity and competitive performance culture* • *Fear-based culture and stigma around mistakes*	**Consequences for ORM** • *ORM enacted primarily as a bureaucratic or symbolic formality* • *Normalization of misconduct, escalation into systemic failures* • *Limited feedback, limited adaptive learning, reduced risk prevention and mitigation capacity*
Example studies: Cohn et al. (2014); Lui (2015); Mikes (2009); Power (2009); Gurd & Helliar (2017); Sabanova & Kudinska (2023); Kunz & Heitz (2021), Brauman et al. (2020); Sabanova & Kudinska (2024)	

Source: Authors' own.

design and use of ORM systems, thereby addressing RQ1, while the second stage captures the organisational and behavioural mechanisms through which these problems undermine the purpose of ORM in banking institutions, thereby addressing RQ2.

First, the misalignment between ORM system design and use leads to a displacement of the original control purpose. Although ORM systems are formally intended to reduce the probability of operational risk events and mitigate their consequences, the reviewed literature shows that regulatory and institutional pressures often orient their design toward auditability, standardisation, and external verification (e.g. Power, 2005, 2009; Lim et al., 2017). Such design encourages a diagnostic and compliance-oriented use (e.g. Ringgaard et al., 2025), translating the preventive and mitigating risk intentions into procedural requirements, checklists, and reporting routines that gradually produce rigidity (e.g. Slapničar et al., 2025). As a result, ORM may become largely symbolic, losing its capacity to influence behaviour and prevent risk ex ante, as well as to support timely learning and risk mitigation ex post.

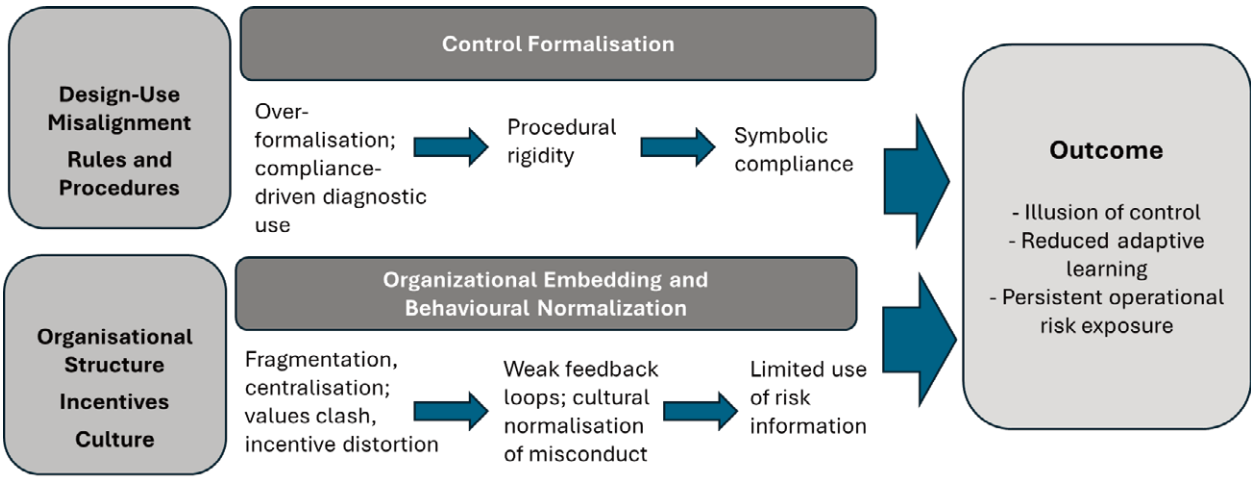
Over time, this rigidity may become institutionalised and self-reinforcing through organisational structure, incentive systems, and cultural norms, giving rise to additional sources of operational risk. Fragmented or overly centralised structures weaken horizontal and vertical feedback loops, thereby hindering managers from effectively using risk information (e.g. Sabanova & Kudinska, 2022) and creating coordination gaps that may generate further risks (e.g. Rad, 2016). Incentive schemes prioritising short-term performance over risk considerations typically reinforce opportunistic behaviour and symbolic compliance (Acrey et al., 2011; Cohn et al., 2014), while cultural patterns characterised by performance pressure, fear of mistakes, and strong professional identities to a certain extent normalise silence, error concealment, and procedural conformity (e.g. Sabanova and Kudinska, 2023). Together, these mechanisms may stabilise the displacement of the original control purpose, leading to a situation in which assurance substitutes for adaptive learning about risk.

The combined effect is a systemic outcome in which ORM systems continue to operate as visible assurances of governance and compliance, creating an illusion of control while underlying behavioural and organisational vulnerabilities may persist and accumulate. By linking procedural rigidity to its structural, motivational, and cultural reinforcements, the synthesis clarifies why management control failures persist despite increasingly sophisticated risk management architectures. Operational risk may thus emerge not only from insufficient control, but also from control systems that have become detached from their preventive and mitigating purposes.

5 DISCUSSION

Our review advances knowledge at the intersection of MCS and ORM by explaining how control architectures shape operational risk outcomes through a two-stage behavioural-institutional mechanism. Prior research has examined dysfunctional control behaviour within the MCS literature and governance challenges within ORM literature largely

Figure 3: Two-stage mechanism linking management control problems to operational risk



Source: Authors' own.

as separate domains (e.g. Merchant & Van der Stede, 2017; Power, 2005; Soin & Collier, 2013). While earlier studies have connected MCS to risk management more broadly (e.g., Bhimani, 2009; Soin & Collier, 2013; Braumann et al., 2024; Hiebl, 2024), they have focused primarily on enterprise or organisational risk management rather than operational risk specifically. This review is, to the best of our knowledge, the first attempt to synthesise these streams and shift the analytical focus from the presence or integration of controls toward the behavioural management control problems associated with ORM systems operating in practice.

5.1 Theoretical implications

Our study advances MCS theory by conceptualising control problems not as isolated dysfunctional outcomes, but as a dynamic process through which control effectiveness evolves over time. Existing work often treats control problems as behavioural deviations such as gaming, rigidity, or manipulation (Merchant & Van der Stede, 2017). By integrating findings across design-use misalignment, rules, structure, incentives, and culture, we develop a two-stage mechanism that explains how such outcomes emerge and persist. Design–use misalignment initially displaces the original purpose of control by translating preventive and mitigating intentions into compliance-oriented routines. Subsequently, organisational structures, incentives, and cultural norms stabilise and reproduce these effects, embedding behavioural responses within everyday practice. This processual view complements established distinctions between diagnostic and interactive control use (Simons, 1995) by demonstrating how regulatory environments systematically bias risk controls toward diagnostic enactment, thereby limiting dialogue, interpretation, and learning.

Building on this process perspective and drawing on Merchant & Van der Stede (2017), we further show that operational risk arises less from missing controls than from misalignment across interconnected control domains. Within this processual framework, rules and procedures translate institutional expectations into formalised practices that may prioritise visible compliance over substantive risk management, echoing prior work on "rituals of verification" (Power, 2005, 2009; Lim et al., 2017). Structural arrangements shape the flow of risk information, where fragmented governance and isolated functions hinder coordination and accountability (Soin & Collier, 2013; Cornwell et al., 2023; Mabwe et al., 2022). Incentive systems reinforce short-term performance pressures that distort judgement and normalise opportunistic behaviour (Acrey et al., 2011; Cohn et al., 2014; Tran et al., 2021). Finally, in the cultural domain, fear, blame, or excessive com-

petition undermine reporting integrity, whereas interactive uses of control that encourage dialogue strengthen trust and collective learning (Mikes, 2009; Kunz & Heitz, 2021; Marc et al., 2023). Taken together, these insights extend OOC-based theorising beyond a classification of control objects toward an explanation of how control configurations interact over time to influence operational risk outcomes.

Our study further contributes by integrating behavioural insights from MCS research with institutional pressures emphasised in banking and risk governance studies. We develop a framework that connects design choices with organisational responses and specifies the process through which design-use misalignments become stabilised under institutional pressure. The two-stage mechanism identified in this study clarifies that balancing compliance and learning is not a mere trade-off but a self-reinforcing dynamic in which institutional pressures shape how controls are interpreted, enacted, and reproduced. In this way, the study advances behavioural management control theory by showing how control effectiveness evolves over time within highly regulated environments.

In addition, we contribute to the ORM and risk governance literature by reframing operational risk as a behavioural-institutional manifestation of management control dynamics. Much of the existing ORM research emphasises governance structures, risk measurement, or risk culture (Power, 2007; Mikes, 2009; Soin & Collier, 2013), often assuming that more formalised control architectures strengthen resilience. Our findings suggest a more nuanced interpretation. Regulatory-driven control designs enhance transparency and accountability, yet they may also encourage symbolic compliance and procedural rigidity (Power, 2005, 2009; Lim et al., 2017). Operational risk therefore persists not despite formal control systems, but partly because institutionalised assurance practices reinforce behavioural responses that detach controls from their preventive and mitigating purposes. Within the developed two-stage mechanism, institutional pressures, such as regulatory expectations, auditability demands, and internal assurance routines reinforce and stabilise behavioural responses to control design, such as workarounds, diffusion of accountability, or normalised deviations over time. In this way, increasing formalisation can strengthen regulatory legitimacy while simultaneously narrowing the interpretive space needed for organisational learning and adaptation.

Finally, these findings also extend ERM research, which typically emphasises integration, proportionality, and risk-informed decision-making within governance structures. While ERM models assume that formal structures enable coordination and learning, our synthesis shows that behavioural and organisational misalignments frequently prevent these principles from materialising in practice. The mechanisms identified here therefore offer a behavioural–systems explanation for the persistent gap between ERM design ideals and operational risk outcomes, suggesting that effective risk governance depends not only on formal architectures but also on how management controls are enacted and sustained within organisational contexts.

5.2 Practical implications

The findings of this review indicate that addressing operational risk requires treating incentives as integral components of ORM systems rather than as peripheral motivational tools. While incentives are a core element of management control, they are often only implicitly addressed in ORM frameworks, limiting their ability to account for behavioural responses to risk controls. Effective ORM therefore depends on aligning formal control structures with supportive incentive and cultural mechanisms that promote ethical awareness, open communication, and continuous learning. Without such reinforcement, even sophisticated ORM frameworks risk becoming procedural shells that are symbolically compliant yet behaviourally fragile.

For banks, this implies e.g. embedding risk awareness directly into managerial incentives, decision routines, and training programmes rather than treating ORM as a specialised compliance function. Regulators and supervisory bodies may strengthen behavioural training and educational materials to help risk managers recognise design–use misalignment and symbolic compliance risks, while boards and senior management can incorporate risk-adjusted performance indicators into managerial evaluations and bonus schemes. Risk management

structures may also need to shift from documentation-driven reporting toward cross-functional dialogue around emerging risks and near misses. Strengthening ORM therefore requires not more control, but more reflexive control: systems designed and used in ways that enable learning, judgement, and adaptation rather than mere compliance.

From the governance perspective, the findings of this review have direct implications for strategic and ERM frameworks. Although the empirical focus of this study is ORM systems rather than ERM as a whole, the behavioural and control design dynamics identified here extend beyond ORM and can inform the design and use of broader ERM architectures in banking. While ERM models emphasise integration, proportionality, and risk-informed decision-making (Bromiley et al., 2015), our synthesis shows that these principles are difficult to realise when control systems are designed primarily for compliance and used diagnostically. Design–use misalignment, structural fragmentation, incentive distortion, and cultural fear undermine the enablers commonly associated with effective ERM, such as cross-functional coordination (Mikes, 2009), open risk communication (Sax & Torp, 2015), and organisational learning (Arena et al., 2010). From this perspective, ERM effectiveness depends not only on adopting formal frameworks or principles, but on aligning management control systems with behavioural and organisational realities.

Building on these implications, we develop principles translating the review's insights into concrete guidance for designing more resilient ORM systems, viewing management controls as an interdependent socio-technical system rather than a set of standalone compliance instruments. Table 8 summarises the principles alongside the specific control problems they address and illustrative organisational practices derived from the literature. The following paragraphs elaborate each principle.

Principle 1: Design controls for interpretative use, not only auditability. Risk control systems should enable dialogue, reflection, and interpretation rather than functioning solely as compliance verification tools. Studies on interactive control use (Mikes, 2011; Ringgaard et al., 2025) show that engaging managers in discussions around risk information strengthens early detection and organisational learning, whereas purely diagnostic use tends to reinforce procedural rigidity and symbolic compliance.

Principle 2: Maintain procedures as enabling guides rather than coercive constraints. Procedural controls remain essential for regulatory legitimacy, yet excessively prescriptive rules may displace professional judgement and situational awareness (Power, 2009; Mabwe et al., 2022). Allowing contextual interpretation, periodic review of procedures, and managerial discretion where appropriate can preserve the preventive function of rules while avoiding mechanical compliance.

Principle 3: Structure risk management around feedback loops and integration. Organisational arrangements should integrate ORM with operational decision-making rather than isolating risk functions in parallel hierarchies. Evidence from structural studies (Soin & Collier, 2013; Rad, 2016; Cornwell et al., 2023) suggests that cross-functional communication, clear escalation ownership, and stronger board engagement with operational risk information enhance responsiveness and reduce fragmentation.

Principle 4: Align incentive systems with risk-aware behaviour rather than compliance outputs. Reward systems should recognise behaviours that support risk identification, escalation, and learning. Incentives tied primarily to short-term financial outcomes or formal compliance indicators may encourage opportunistic behaviour and weaken ethical judgement (Acrey et al., 2011; Cohn et al., 2014; Tran et al., 2021). Aligning incentives with long-term resilience helps reinforce both preventive and mitigating functions of ORM. In practice, this may involve linking a portion of variable compensation to risk escalation quality, learning contributions, or cross-functional risk collaboration rather than solely to financial outputs.

Principle 5: Treat organisational culture as a core control layer. Leadership framing and psychological safety strongly influence how controls are interpreted in practice. Research on risk culture (Mikes, 2009; Kunz & Heitz, 2021; Sabanova & Kudinska, 2023) shows that open discussion of errors, learning from near misses, and constructive challenge strengthen reporting integrity and reduce fear-based behaviour.

Table 8: Design principles for resilient operational risk management systems

Design principle	Control problem addressed	Actionable recommendations
1. Design controls for interpretative use, not only auditability	Design–use misalignment; diagnostic overuse of controls; symbolic assurance	• Embed regular cross-functional risk dialogues around risk reports. • Complement compliance dashboards with interpretative discussion forums. • Require managers to explain risk implications, not only report indicators.
2. Maintain procedures as enabling guides rather than coercive constraints	Procedural rigidity; over-formalisation; mechanical rule-following	• Periodically review procedural complexity and eliminate redundant steps. • Introduce discretionary checkpoints where judgement is explicitly allowed. • Encourage post-incident learning reviews instead of checklist-driven responses.
3. Structure governance around feedback loops and integration	Structural fragmentation; weak vertical and horizontal information flow	• Create joint forums between risk, operations, and audit functions. • Assign clear escalation ownership. • Ensure operational risk reporting reaches board-level strategic discussions.
4. Align incentives with risk-aware behaviour rather than compliance outputs	Incentive distortion; ethical blindness; symbolic compliance	• Incorporate risk reporting quality and learning behaviours into performance evaluations. • Balance financial metrics with long-term risk indicators. • Avoid rewarding procedural completion without behavioural impact.
5. Treat organisational culture as a core control layer	Fear-based culture; normalisation of misconduct; suppressed feedback	• Encourage leadership framing of ORM as shared responsibility. • Establish psychologically safe channels for reporting near misses. • Recognise teams that surface risks early, not only those avoiding incidents.

Source: Authors own.

5.3 Limitations and Future Research Directions

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.

Beyond these scope-related constraints, several methodological limitations should also be considered. First, as a qualitative synthesis of a diverse and fragmented literature, the review relies on interpretative judgement in categorising studies and abstracting underlying mechanisms. To address this limitation, we adopted transparent inclusion and exclusion criteria, systematically coded studies across theoretically-grounded analytical dimensions, and focused on convergent patterns rather than isolated findings. Nevertheless, future research could complement this work with qualitative or mixed-method approaches to further validate and refine the mechanisms identified. For example, group-level research could examine how operational teams collectively interpret risk indicators and negotiate the use of control procedures in situations of uncertainty, and how these interactions reinforce or challenge design–use alignment over time.

Second, while the review spans multiple disciplines and methodological traditions, the evidence base remains skewed toward banking and highly regulated financial institutions. This focus is appropriate given the research questions, but it limits the generalisability of the findings beyond similar regulatory and institutional contexts. Comparative research across industries and institutional settings would help establish the boundary conditions of the proposed mechanisms. For example, it would be interesting to explore if similar patterns exist in healthcare, aviation, or other safety-critical sectors.

Third, although the review highlights behavioural dynamics and organisational processes, many of the underlying studies rely on cross-sectional designs or retrospective accounts, which constrain causal inference. While this review identifies the design–use misalignment as a foundational mechanism, further research is needed to understand how such misalignments emerge, persist, or are corrected over time. Longitudinal research could examine successful case studies of how organisations recalibrated risk-related controls in response to incidents, regulatory change, or performance pressure, and under what conditions control design–use alignment supports learning rather than procedural rigidity. When do design–use misalignments self-correct, and when do they instead evolve into persistent procedural rigidity? Further research could also explore whether these conditions are mainly organisational, individual or collective (cultural) in nature. Combining theoretical perspectives from MCS and organisational learning may be particularly fruitful in advancing this line of inquiry.

Beyond these limitations, our review points to several additional directions for future inquiry. The notion of behavioural and institutional coupling calls for multi-level studies that connect individual cognition and ethical judgement with institutional logics, offering opportunities for new contributions in particular to risk management literature. Such research could explore, for example, how professional norms and organizational cultures interact to shape the enactment of ORM practices, how leadership practices mediate the translation of institutional risk expectations into everyday control use, and under what conditions unethical norms spread and escalate into operational risk. Network-based analysis approaches to organisational analysis may be particularly useful in addressing these questions.

Finally, the growing digitalization of control systems opens new avenues for future research. Emerging technologies, such as data analytics and artificial intelligence are reshaping how operational risks are generated, identified, monitored, and governed. Future research could examine how employees interpret and respond to algorithmic risk indicators compared to traditional rule-based controls, and whether new technologies reproduce procedural rigidity and misalignments or whether they can be used to effectively bridge the design-use misalignments?

6 CONCLUSION

This systematic literature review examined how problems emerge within the design and use of MCS and how these problems shape ORM in the banking sector. By structuring the synthesis around the OOC framework, the review revealed that operational risk arises not merely from technical control failures but from the interaction between control design, use, and organizational behaviour over time.

The findings demonstrate that while regulatory-driven control architecture enhances formal accountability, it often creates 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 which 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.

Despite limitations associated with systematic literature reviews, our study brings several contributions. Most importantly, it develops a two-stage behavioural–institutional explanation that extends the OOC framework to operational risk management by showing how result, action, personnel, and cultural controls operate as interdependent mechanisms that both enable and constrain organisational behaviour. Rather than depicting ORM as ineffective, the synthesis demonstrates that regulatory-driven control architectures strengthen governance and accountability, yet operational risk emerges when these mechanisms become misaligned or behaviourally distorted in practice. By bridging management control and risk management literatures, the review reframes operational risk not merely as a stochastic or technical phenomenon but a behavioural outcome of control enactment. Practically, the findings highlight that banks should view ORM as a socio-technical system in which effective risk management depends not only on robust design but also on learning-oriented use. Managers can strengthen operational resilience by embedding open communication, cross-functional

coordination, and reflective learning into control processes, while regulators and boards should recognise that compliance effectiveness relies on behavioural engagement rather than procedural completeness alone. For researchers, the study outlines an agenda for longitudinal, multi-level, and cross-sectoral investigations that examine how management control configurations evolve alongside regulatory, technological, and cultural change, and how cognitive and social mechanisms mediate the relationship between control design and operational outcomes.

In conclusion, the effectiveness of ORM depends on balancing formal control assurance with behavioural adaptability. Banks managers who 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.

EXTENDED SUMMARY/IZVLEČEK

Članek obravnava, kako napake in problemi v sistemih managerske kontrole prispevajo k nastanku in obvladovanju operativnega tveganja v bančnem sektorju. Kljub zahtevnim regulatornim okvirjem, kot sta Basel II in III, ter razvoju sofisticiranih kontrolnih mehanizmov za obvladovanje tveganj, banke še vedno beležijo znatne izgube, ki izvirajo predvsem iz notranjih napak, pomanjkljivih postopkov in človeškega ravnanja. Ti primeri kažejo, da formalna popolnost kontrolnih sistemov sama po sebi še ne zagotavlja njihove dejanske učinkovitosti. Metodološko se članek opira na sistematični pregled literature, ki zajema obdobje med letoma 1995 in 2025. Analiza teoretično temelji na modelu *Object of Control* in zajema 59 empiričnih in konceptualnih študij, razvrščenih v pet analitičnih dimenzij: zasnova in uporaba kontrol, pravila in postopki, struktura, spodbude in kultura. Na podlagi primerjalne analize in konceptualne sinteze člankov članek pojasnjuje, kako konfiguracija in uporaba sistemov managerske kontrole vplivata na pojav operativnih tveganj ter učinkovitost njihovega obvladovanja v bankah. Ugotovitve kažejo, da operativno tveganje ne izvira zgolj iz tehničnih ali procesnih napak, temveč lahko tudi iz načina, kako so kontrole zasnovane in uporabljene v organizacijskem kontekstu. Kontrole, ki jih predpisuje regulatorni okvir in usmerjajo skladnost, sicer povečujejo odgovornost in sledljivost, a pogosto povzročajo neželene vedenjske učinke, kot so togost postopkov, silosno delovanje, izkrivljene spodbude in oslabitev kulture učenja. V članku razvijemo dvostopenjski model, ki pojasnjuje, kako se težave pri kontrolah prevedejo v trajno izpostavljenost operativnemu tveganju. Prvič, neskladje med zasnovo in načinom uporabe izriva preventivni in blažilni namen sistemov za obvladovanje operativnih tveganj ter kontrole preoblikuje v simbolno zagotavljanje skladnosti. Drugič, strukturna fragmentacija ali centralizacija, neustrezno usklajeni mehanizmi nagrajevanja ter kulturne norme to togost stabilizirajo z oslabitvijo povratnih zank in normalizacijo vedenja, ki zasleduje skladnost namesto obvladovanja tveganj. Posledično se zmanjšuje sposobnost organizacij, da pravočasno zaznajo in se odzovejo na nastajajoča tveganja, kar povečuje verjetnost operativnih tveganj in posledično izgub v bankah. Članek povezuje literaturo s področja managerske kontrole in obvladovanja tveganj ter pokaže, da operativno tveganje ni zgolj tehnična ali statistična kategorija, temveč je lahko tudi vedenjski rezultat disfunkcionalne kontrole. Teoretični prispevek predstavljata razširitev modela *Object of Control* na področje obvladovanja operativnih tveganj in razvoj dinamične razlage interakcij med različnimi tipi managerske kontrole, ki lahko vodi do pojava operativnih tveganj. Praktični prispevek vključuje priporočila za banke in regulatorje: večja učinkovitost obvladovanja operativnih tveganj zahteva uravnoteženje formalnih elementov kontrole s prožnostjo pri njihovi uporabi, upoštevanje vedenjskih posledic ter spodbujanje odprte komunikacije, interdisciplinarnega sodelovanja in organizacijskega učenja. Uspešnost sistemov za obvladovanje operativnega tveganja tako temelji na usklajenosti med zasnovo in uporabo kontrol ter na ravnotežju med skladnostjo in organizacijskim učenjem.

REFERENCES

References marked with an asterisk (*) indicate studies included in the systematic literature review corpus.

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.*

Abdul-Rahman, A., & Yazid, Z. (2015). Developing a framework of Islamic bank operational risk management: People risk. *Jurnal Pengurusan, 44*, 129–139.*

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.*

Ahrens, T., & Chapman, C. S. (2007). Management accounting as practice. *Accounting, Organizations and Society, 32*(1–2), 1–27.

Al-Amri, K., & Davydov, Y. (2016). Testing the effectiveness of enterprise risk management: Evidence from operational losses. *Journal of Economics and Business, 87*, 70–82.*

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2023). Operational and cyber risks in the financial sector. *International Journal of Central Banking, 19*(5), 341–402.

Anthony, R. N. (1965). *Planning and control systems: A framework for analysis*. Harvard University, Graduate School of Business Administration, Division of Research.

Arena, M., & Arnaboldi, M. (2014). Risk and performance management: Are they easy partners? *Management Research Review, 37*(2), 152–166.

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

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.*

Bardoscia, M., & Bellotti, R. (2012). A dynamical approach to operational risk measurement. *arXiv*. https://arxiv.org/abs/1202.2532 *

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

Basel Committee on Banking Supervision. (2006). *International convergence on capital measurement and capital standards: A revised framework (Comprehensive version).* Bank for International Settlements. https://www.bis.org/publ/bcbs128.htm

Basel Committee on Banking Supervision. (1998). *Framework for internal control systems in banking organisations*. Bank for International Settlements.*

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*, Article 106730.*

Braumann, E., Grabner, I., & Posch, A. (2020). *Tone from the top in risk management: A complementarity perspective on how control systems influence risk awareness* (Working Paper No. 03/2020). WU Vienna University of Economics and Business.*

Braumann, E. C., 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.

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. *Long Range Planning, 48*(4), 265–276.

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.*

Carpenter, N. C., Whitman, D. S., & Amrhein, R. (2021). Unit-level counterproductive work behavior: A conceptual review and quantitative summary. *Journal of Management, 47*(6), 1498–1527.*

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.*

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.*

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management: Integrating with strategy and performance*. COSO.

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*, Article e25.*

Chapelle, A., Crama, Y., Hübner, G., & Peters, J. P. (2004). *Basel II and operational risk: Implications for risk measurement and management in the financial sector* (Working Paper No. 51). National Bank of Belgium.

Chapelle, A., Crama, Y., Hübner, G., & Peters, J. P. (2008). Practical methods for measuring and managing operational risk in the financial sector: A clinical study. *Journal of Banking & Finance, 32*(6), 1049–1061.

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.*

Cohn, A., Fehr, E., & Maréchal, M. A. (2014). Business culture and dishonesty in the banking industry. *Nature, 516*(7529), 86–89.*

Cornalba, C., & Giudici, P. (2004). Statistical models for operational risk management. *Physica A: Statistical Mechanics and Its Applications, 338*(1–2), 166–172.

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*, Article 101906.*

Cruz, M., Coleman, R., & Salkin, G. (1998). Modeling and measuring operational risk. *Journal of Risk, 1*(1), 63–72.

Dahen, H., & Dionne, G. (2010). Scaling models for the severity and frequency of external operational loss data. *Journal of Banking & Finance, 34*(7), 1484–1496.

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.

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.*

Edwards, J., & Wolfe, S. (2004). The compliance function in banks. *Journal of Financial Regulation and Compliance, 12*(3), 216–224.*

European Banking Authority. (2023). *Operational risks and resilience report 2023*. https://www.eba.europa.eu/publications-and-media/publications/operational-risks-and-resilience-0

Faugère, C., & Stul, O. (2021). Harmful events and misconducts in financial organizations: Human biases and root causes. *Research in International Business and Finance, 56*, Article 101382.*

Ferreira, S., & Dickason-Koekemoer, Z. (2019). A conceptual model of operational risk events in the banking sector. *Cogent Economics & Finance, 7*(1).

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.

Financial Stability Board. (2014). *Guidance on supervisory interaction with financial institutions on risk culture: A framework for assessing risk culture*. Financial Stability Board.*

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

Fontnouvelle, P. D., Jordan, J., & Rosengren, E. (2005). *Implications of alternative operational risk modeling techniques*(Working Paper No. 04-9). Federal Reserve Bank of Boston.

Frese, M., & Keith, N. (2015). Action errors, error management, and learning in organizations. *Annual Review of Psychology, 66*, 661–687.*

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.*

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.*

Gurd, B., & Helliar, C. (2017). Looking for leaders: Balancing innovation, risk and management control systems. *The British Accounting Review, 49*(1), 91–102.*

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*, 241–257.*

Hartman, F., & Slapničar, S. (2007). *Corporate governance in banks: Characteristics of internal management control systems in Slovenian banks*. University of Ljubljana.*

Heimeriks, K. H., Schijven, M., & Gates, S. (2012). Manifestations of higher-order routines: The underlying mechanisms of deliberate learning in the context of postacquisition integration. *Academy of Management Journal, 55*(3), 703–726.

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

Holland, J. (2019). Bank top management teams, disclosure, learning, survival and failure: 1990–2017. *Qualitative Research in Financial Markets, 11*(1), 31–59.*

Houston, J. F., & James, C. (1995). CEO compensation and bank risk. *Journal of Monetary Economics, 36*(2), 405–431.*

Kunz, J., & Heitz, M. (2021). Banks' risk culture and management control systems: A systematic literature review. *Journal of Management Control, 32*(4), 439–493.*

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.*

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), Article 1196.*

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.*

Lueg, R., & Knapik, M. (2016). Risk management with management control systems: A pragmatic constructivist perspective. *Corporate Ownership and Control, 13*(3), 72–81.

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.*

Mabwe, K., Ring, P., & Webb, R. (2022). The status of people risk management in UK banks. *Journal of Operational Risk, 17*(2), 83–104.*

Malmi, T., & Brown, D. A. (2008). Management control systems as a package: Opportunities, challenges and research directions. *Management Accounting Research, 19*(4), 287–300.*

Marc, M., Arena, M., & Peljhan, D. (2023). The role of interactive style of use in improving risk management effectiveness. *Risk Management, 25*(2), Article 9.*

Merchant, K. A., & Otley, D. T. (2006). A review of the literature on control and accountability. In C. S. Chapman, A. G. Hopwood, & M. D. Shields (Eds.), *Handbook of management accounting research* (Vol. 1, pp. xx–xx). Elsevier. (page range missing in original source—verify)

Merchant, K. A., & Van der Stede, W. A. (2017). *Management control systems: Performance measurement, evaluation and incentives* (4th ed.). Pearson.

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

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

Molamohamadi, Z., Samani, M. A., & Karimi, M. (2024). Reviewing the historical milestones of risk management. *SN Business & Economics, 4*, Article 161.*

Moosa, I. A. (2007). The Basel Committee, Basel I and Basel II. In *Operational risk management* (pp. 26–41). Palgrave Macmillan.

Moosa, I. A. (2017). Good regulation versus bad regulation. *Journal of Banking Regulation, 19*(1), 55–63.*

Muermann, A., & Oktem, U. (2002). The near-miss management of operational risk. *Journal of Risk Finance, 3*(2), 25–36.*

ORX. (2024). *Top 5 losses May 2024: Human error events (Citi and Barclays).* https://orx.org/podcast/orx-news-top-5-losses-may-2024-human-error-events

ORX. (2024). *Top 5 operational risk losses Q4 2024: Mastercard case.* https://orx.org/blog/top-5-orx-news-losses-q4-2024

ORX. (2025). *Annual banking operational risk loss data report 2025*. Oxford Risk Exchange Consortium. https://orx.org/blog/global-banks-report-lowest-financial-losses-in-a-decade

Palazzo, G., Krings, F., & Hoffrage, U. (2012). Ethical blindness. *Journal of Business Ethics, 109*(3), 323–338.

Peljhan, D., Miloš Sprčić, D., & Marc, M. (2018). Strategy and organizational performance: The role of risk management system development. In M. J. Epstein, F. H. M. Verbeeten, & S. K. Widener (Eds.), *Performance measurement and management control: The relevance of performance measurement and management control research* (Vol. 33, pp. 65–91). Emerald Publishing.

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*, Article 101126.*

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ, 372*, n71.

Power, M. (2005). *The invention of operational risk* (Discussion Paper No. 16). ESRC Centre for Analysis of Risk and Regulation, London School of Economics and Political Science.*

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

Rad, A. (2016). Risk management–control system interplay: Case studies of two banks. *Journal of Accounting & Organizational Change, 12*(4), 522–546.*

Raghavan, R. S. (2003). Risk management in banks. *The Chartered Accountant*, 841–851.

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.*

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.*

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.* Advance online publication.*

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.*

Sabanova, J., & Kudinska, M. (2023). The reasons for human errors in banks and employees' mindsets. *Economy and Market Communication Review, 13*(2), 362–378.*

Sabanova, J., & Kudinska, M. (2024). Management response to human errors and key controls in banks. *Marketing and Management of Innovations, 15*(2), 89–99.*

Sax, J., & Torp, S. (2015). Speak up! Enhancing risk performance with enterprise risk management, leadership style, and employee voice. *Management Decision, 53*(7), 1452–1468.

Siaw Ofori, B., Padi, A., & Musah, A. (2025). Corporate governance effectiveness and operational risk of banks. *Discover Global Society, 3*, Article 23.*

Simons, R. (1995). *Levers of control: How managers use innovative control systems to drive strategic renewal*. Harvard Business School Press.

Slapničar, S., Axelsen, M., & Eulerich, M. (2025). Cyber risk management: An illusion of a risk-based approach. *Journal of Management Control.* Advance online publication.*

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

Soin, K., Varoutsa, E., & Taylor, L. (2020). Blurred lines. *Enterprise Risk*, 28–29.

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.*

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.

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* (Doctoral dissertation, University of Twente).

Wright, J. F. (2018). *Risk management: A behavioural perspective*. Oslo and Akershus University College of Applied Sciences.*

Xu, Y., Pinedo, M., & Xue, M. (2017). Operational risk in financial services: A review and new research opportunities. *SSRN Electronic Journal.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2823166 *

Xu, Y., Zhu, L., & Pinedo, M. (2020). Operational risk management: A stochastic control framework with preventive and corrective controls. *Operations Research, 68*(6), 1804–1825.

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.*