QUBAHAN ACADEMIC JOURNAL
VOL. 6, NO. 1, January 2026
https://doi.org/10.48161/qaj.v6n1a2067

Policy Implications for Improving Operational Risk Management of Commercial Banks: A Case Study in Vietnam

Phan Dien Vy [1] and Phan Thanh Tam [2*]

[1] Faculty of Postgraduate Studies, Ho Chi Minh University of Banking (HUB), Ho Chi Minh City 84, Vietnam;
[2] Faculty of Postgraduate Studies, Lac Hong University (LHU), Dong Nai Province 84, Vietnam.

* **Corresponding author:** tampt@lhu.edu.vn.

ABSTRACT: This study investigates the impact of organizational factors and digital transformation on operational risk management (ORM) in Vietnamese commercial banks. Employing a mixed-methods approach, qualitative interviews with 25 senior risk experts helped refine measurement scales, followed by a large-scale quantitative survey with 958 valid responses. Structural equation modeling (SEM) reveals that the internal environment is the most influential driver of ORM, while the awareness and operation of the ERM framework (AOF) play a critical mediating role. Results emphasize that effective ORM requires a strong risk-aware culture, integrated digital systems, and clear risk communication. The study contributes theoretically by demonstrating a dual-channel mechanism, direct and mediated, through which organizational and technological factors shape ORM effectiveness. Practically, the findings highlight that sustainable ORM requires fostering a risk-aware culture, enhancing communication, aligning technology with ERM frameworks, and integrating risk management into strategic objectives. Policy recommendations emphasize the importance of leadership commitment, ethical governance, and systematic training to strengthen the internal environment and institutionalize ERM maturity, thereby enabling Vietnamese banks to build resilience and competitiveness in an increasingly digitalized financial landscape. Finally, enhancing leadership accountability, strengthening risk culture, and embedding ERM into daily operations and strategy.

Keywords: risk management, technology, digital transformation, policy, management sciences.

I. INTRODUCTION

In the field of commercial banking, credit activities are always the core and main activities. Although this activity generates significant profits for the bank, it also poses very high potential risks. Risks often go hand in hand with benefits; the higher the risk, the greater the expected profit for the bank [1, 2]. Therefore, banks need to evaluate business opportunities based on the risk-benefit relationship to identify opportunities that yield benefits commensurate with the accepted level of risk. Risk management in commercial banks is a crucial activity that enables the timely detection, prevention, and resolution of risks, thereby limiting losses and ensuring the efficiency and safety of commercial bank operations. To effectively implement risk management activities, Vietnam has issued legal documents that regulate the credit activities of banks. In addition, Basel II standards, the second version of the Basel Accord issued by the Basel Committee, regulate the credit risk framework, determine capital standards to limit business risks for banks, and enhance the financial system's resilience. These standards are also applied by commercial banks in Vietnam under the control and guidance of Vietnamese law. However, in the context of the current volatile and difficult-to-control economy, the instability of exchange rates and interest rates necessitates that we adapt and innovate our business methods, propose timely solutions to mitigate risks, and ensure stable development for commercial banks.

Over the past decade, operational risk has shifted from the periphery to the core of bank risk management agendas. Global shocks (pandemics, cyber incidents, large-scale internal fraud, technology outages, and supply–chain ruptures) have repeatedly demonstrated that losses no longer arise solely from credit and market exposures. They are equally, and sometimes more severely, triggered by failures of processes, people, systems, or external events [1-3]. In parallel, the regulatory discourse has evolved from a narrow focus on capital charges for operational risk (Basel II/III) to a broader emphasis on operational resilience, internal control culture, and enterprise-wide risk governance. In commercial banking, credit activities remain central, generating significant returns but also exposing institutions to substantial risks. Traditionally, risk management research and practice in Vietnam have focused on credit risk and regulatory compliance, particularly in relation to Basel II and III. However, recent global shocks ranging from cyber incidents and internal fraud to supply-chain disruptions have revealed that operational risks can be equally, if not more, damaging. These risks, stemming from people, processes, systems, or external events, now sit at the core of bank governance agendas worldwide.

A central construct in this study is Awareness and Operation of ERM (AOF), which reflects the extent to which employees and managers understand, internalize, and implement ERM principles in practice. We posit that AOF functions as a transmission mechanism, channeling organizational inputs, such as strategy, control activities, communication, monitoring, and digital initiatives, into tangible ORM outcomes. Without this mediating function, even substantial investments in technology or monitoring may fail to yield improved risk resilience. The level of compliance with Basel II standards varies among banks, and empirical evidence evaluating its actual impact on risk reduction and financial stability remains limited [3, 4]. Furthermore, the effect of macroeconomic factors, including exchange rate volatility, interest rate fluctuations, and global economic uncertainties, on credit risk management in commercial banks has not been thoroughly examined. Most research lacks a systematic approach to linking external shocks with the performance of risk management strategies.

Another gap lies in the integration of advanced technologies, such as artificial intelligence, machine learning, and big data, into credit risk assessment and early-warning systems. These innovations are increasingly important but underexplored in the Vietnamese context. Addressing these gaps would provide valuable insights into improving the resilience and sustainable development of commercial banks. Despite a growing body of international work on ORM and ERM, three significant gaps persist in the Vietnamese context: fragmented perspectives, where many studies analyze single levers of ORM, such as internal controls, governance, or technology, without simultaneously modeling how these levers interact and flow through ERM awareness and practice to shape ORM outcomes [4, 5].

Under-theorized role of digital transformation: Banks in emerging markets invest aggressively in analytics, automation, and Artificial Intelligence (AI). Nevertheless, empirical evidence often shows weak or inconsistent direct effects of digital transformation on ORM, unless digital transformation is integrated into an ERM architecture supported by a sound internal environment and effective communication. The Vietnamese literature has only begun to test this conditionality. Limited, large-sample, structural tests: There is a dearth of comprehensive SEM-based studies that (i) deploy a validated multi-construct measurement model, (ii) explicitly treat ERM awareness and operation (AOF) as a mediator, and (iii) are built on broad, multi-bank samples to capture the heterogeneity of practices in Vietnam.

Against this backdrop, the present study proposes and empirically validates a hybrid qualitative - quantitative framework that integrates six organizational antecedents - Internal environment (IE), strategic objectives (SO), control activities (CA), information and communication (IC), monitoring activities (MA), and digital transformation (DT) and examines both their direct impacts on operational risk management (ORM) and their indirect effects through AOF. Conceptual anchor, ERM as the transmission belt. A central proposition of this research is that AOF - awareness and level of operation of the ERM framework functions as the transmission belt that converts organizational inputs (i.e., SO, CA, IC, MA, DT) into tangible ORM performance. This proposition is theoretically rooted in ERM and BCBS principles: risk management cannot be a siloed compliance function; it must be strategically aligned, culturally embedded, and operationally routine. The empirical evidence we report later strongly supports this view: the internal environment is the

dominant driver of both AOF and ORM, while the direct effects of the other five factors on ORM, though positive, are modest without the ERM bridge.

The overarching objective of this paper is to quantify and explain how organizational factors and digital transformation capabilities shape operational risk management in Vietnamese commercial banks, and through what mechanisms (direct vs. mediated by AOF) they do so. To achieve this, the study addresses the following research questions (RQs):

- RQ1: To what extent do IE, SO, CA, IC, MA, and DT directly affect ORM in Vietnamese commercial banks?
- RQ2: Does AOF (ERM awareness and operation) mediate the relationships between these six antecedents and ORM? If so, which antecedents rely more heavily on this mediation channel?
- RQ3: Which factor(s) emerge as the most influential for improving ORM, and what does this imply for prioritizing managerial actions and policy interventions?
- RQ4: How robust are these structural relationships when validated through bootstrapping and standard psychometric quality tests (reliability, convergent, and discriminant validity)?

The study follows a two-phase research design: a qualitative phase based on scale development and refinement. We conducted in-depth interviews with 25 risk management experts from 25 commercial banks to elicit context-specific indicators, validate conceptual definitions, and ensure that measurement items reflect the realities of Vietnamese regulatory, cultural, and digital environments. This phase yielded the formalized measurement scales for each construct. Quantitative phase (Large-sample SEM): A structured survey produced 1.000 responses, of which 958 were valid and used for analysis. We employed Cronbach's Alpha, EFA, CFA, and SEM, alongside bootstrapping with 5.000 resamples, to test (i) the measurement model by reliability and validity, (ii) the structural model (direct and indirect paths), and (iii) the stability of path estimates.

This article is confined to operational risk, as defined by Basel, which encompasses losses stemming from people, processes, systems, or external events. It does not explicitly model other risk classes, such as credit, liquidity, and market risk, although their interplay with operational risk is acknowledged. Our analysis focuses on Vietnamese commercial banks, which may limit generalizability to other jurisdictions with different regulatory, technological, or cultural settings. Furthermore, the quantitative analysis is based on perceptual measures, which, although robust and validated, should be triangulated in future work with objective ORM datasets, such as, loss event databases, key risk indicators, KRIs.

This study presents a comprehensive, empirically validated perspective on how Vietnamese banks can enhance operational risk management during a period marked by digital acceleration, regulatory tightening, and systemic uncertainty. It shows that the center of gravity for ORM success lies in the internal environment and the lived reality of ERM, that is, what people know, believe, and do every day about risk, rather than in any isolated toolkit, policy manual, or technology stack. By quantifying these relationships with a large, multi-bank dataset and a rigorous SEM architecture, the paper offers both scholarly insight and actionable guidance for boards, CROs, supervisors, and policymakers committed to building resilient, transparent, and digitally ready banking institutions. This article examines the critical factors influencing ORM in Vietnamese commercial banks, evaluates empirical findings from recent studies, and discusses strategic implications for building stronger and more resilient banking systems.

The remainder of the paper is organized as follows: Section I reviews the theoretical foundations of operational risk, ERM, digital transformation, and the six organizational pillars examined herein, and develops the research hypotheses. Section II elaborates on the methodology, including research design, instrument development, sampling, and analytical strategies (EFA, CFA, SEM, and bootstrapping). Section III presents the empirical results, including descriptive statistics, reliability and validity diagnostics, SEM path coefficients, mediation tests, and robustness checks. Section IV presents a discussion of the findings, linking the results to theory and practice, and articulating a prioritized risk governance agenda for banks and regulators. Section V presents policy recommendations, explicitly structured according to the relative strength of the standardized estimates derived from the model. Section VI discusses limitations and directions for future research.

II. LITERATURE EMPIRICAL REVIEW AND HYPOTHESIS DEVELOPMENT

1. OPERATIONAL RISK MANAGEMENT (ORM)

Operational risk is defined by the Basel Committee on Banking Supervision (BCBS) as "the risk of loss resulting from inadequate or failed internal processes, people, systems, or from external events" [5, 6]. ORM has become an integral part of banking risk governance due to the increased complexity of operations, heightened regulatory scrutiny, and rising digital threats. Effective ORM frameworks integrate organizational culture, control activities, information systems, and monitoring mechanisms to anticipate, mitigate, and respond to operational risks [7, 8]. Empirical research has demonstrated that the effectiveness of ORM is closely tied to the internal environment and the maturity of enterprise risk management (ERM) systems [8]. Moreover, ORM practices have evolved beyond traditional control checklists to include real-time data analytics, proactive risk culture, and enterprise-wide risk communication [9, 10].

2. AWARENESS AND LEVEL OF OPERATION OF ERM (AOF)

Awareness and level of operation of the enterprise risk management framework (AOF) refers to the extent to which employees and management understand, internalize, and implement ERM principles in daily operations. A high level of ERM awareness ensures that risk management becomes an integral part of decision-making processes, rather than a compliance-driven activity [10, 11]. The ERM awareness fosters a proactive risk culture where potential operational risks are identified, assessed, and mitigated in a structured and timely manner [12]. Empirical studies have emphasized that AOF acts as a critical mediator between organizational factors such as internal environment, control activities, and information and communication and operational risk management outcomes [13, 14]. When employees are well-informed about ERM practices, the organization can leverage its strategic objectives and digital transformation efforts more effectively [15].

3. INTERNAL ENVIRONMENT (IE)

The internal environment forms the foundation of any effective operational risk management (ORM) framework. It encompasses the corporate culture, ethical values, leadership tone, and organizational structure that shape risk awareness and behavior [14, 16]. A strong internal environment ensures that risk management is not merely a compliance exercise but an integral part of daily operations and strategic decision-making. The tone set by senior leadership, often referred to as the "tone at the top," is critical for embedding risk responsibility throughout the organization. Empirical studies underscore the significance of IE [11, 17]. The study finds that banks with proactive risk cultures and leadership commitment are better positioned to manage operational risks effectively. Furthermore, it is suggested that IE has a direct influence on ERM implementation, which in turn affects overall risk mitigation. In Vietnamese banking, where cultural and hierarchical structures strongly influence organizational behavior, IE can either enhance or hinder ORM depending on the level of employee empowerment and ethical governance [13, 18, 19]. The study indicates a relatively high reliability for the internal environment, suggesting some variability across banks. This highlights the need to improve leadership accountability, risk culture training, and internal ethics [20]. Strengthening IE should be the top priority for both managers and regulators, as it creates the conditions for other factors, such as controls, communication, and technology, to function effectively. Thus, the authors gave hypotheses H1 and H2 in Figure 1 below.

- H1: The Internal environment has a positive effect on operational risk management.
- H2: The Internal environment has a positive effect on awareness and the level of ERM operation.

4. STRATEGIC OBJECTIVES (SO)

Strategic objectives represent the goals and priorities of an organization, and their alignment with risk management principles is vital for sustainable performance. When strategic objectives explicitly incorporate risk considerations, banks are better equipped to anticipate and mitigate potential threats that could disrupt their operations [6, 12, 21]. The study emphasizes that aligning strategy and risk management ensures that

operational risks are assessed within the context of the bank's broader mission and risk appetite [22]. The authors suggest that strategic alignment with risk factors significantly enhances ERM adoption and ORM performance [22]. Similarly, the study finds that organizations with clearly defined risk-adjusted strategies are more resilient to operational disruptions. In emerging markets like Vietnam, banks frequently face challenges due to rapid market changes, necessitating strategic plans that strike a balance between growth ambitions and robust risk management frameworks [23]. This suggests that while strategic objectives provide direction, their effectiveness depends on how well they are operationalized and communicated across departments. For banks, incorporating ORM into strategic scorecards, conducting scenario analyses, and linking executive KPIs to risk outcomes are critical measures to enhance the strategic integration of risk management [24, 25]. Thus, the authors gave hypotheses H3 and H4 in Figure 1 below.

- H3: Strategic objectives have a positive effect on operational risk management.
- H4: Strategic objectives have a positive impact on awareness and the level of ERM operation.

5. CONTROL ACTIVITIES (CA)

Control activities include policies, procedures, and mechanisms designed to mitigate risks and ensure that operations are conducted within defined parameters. They form the second line of defense in ORM frameworks and are essential for preventing errors, fraud, and system failures [17, 26]. Practical control activities often involve a combination of manual procedures and automated tools, ensuring that risk controls are both robust and efficient. Studies demonstrate that well-designed internal controls reduce both the frequency and severity of operational losses [27]. The study highlights that controls are most effective when integrated with ERM systems and aligned with the organization's risk appetite. In Vietnamese banks, control activities are evolving as institutions adopt digital solutions and standard operating procedures to meet international risk management standards. The study confirms its importance as a foundational element of risk management [28, 29]. However, its influence is negligible compared to IE or AOF, suggesting that controls must be supported by a strong culture and effective communication to yield maximum benefits [30]. Continuous testing, updating control frameworks, and investing in advanced control technologies such as AI-based fraud detection are recommended to strengthen CA. Thus, the authors proposed hypotheses H5 and H6, as shown in Figure 1 below.

- H5: Control activities have a positive effect on operational risk management.
- H6: Control activities have a positive effect on awareness and the level of operation of ERM.

6. INFORMATION AND COMMUNICATION (IC)

Information and communication (IC) ensure that risk data, incident alerts, and operational metrics are effectively disseminated across all levels of the organization [31]. Effective communication is crucial for making timely decisions, as operational risks often escalate due to information gaps or delays. In ORM, IC encompasses both the quality of information, including accuracy and completeness, as well as the communication channels, such as real-time dashboards and reporting systems [32, 33]. Empirical studies highlight IC as a key determinant of risk awareness and responsiveness. The study found that banks with robust risk communication systems respond more quickly to operational threats and mitigate the severity of losses. The study indicates systemic weaknesses in bank communication frameworks. This suggests that improvements in IC, such as better reporting mechanisms, cross-department collaboration, and transparent communication, can significantly enhance ORM outcomes [34, 35]. To improve IC, banks should develop centralized risk dashboards, integrate communication systems with real-time analytics, and establish clear escalation protocols for operational incidents. Thus, the authors gave hypotheses H7 and H8 in Figure 1 below.

- H7: Information and communication have a positive effect on operational risk management.
- H8: Information and communication have a positive effect on awareness and level of operation of ERM.

7. MONITORING ACTIVITIES (MA)

Monitoring activities (MA) involves continuous evaluation of risk management processes to ensure they remain effective and aligned with organizational objectives. These activities include internal audits,

compliance checks, and independent risk assessments [36]. Continuous monitoring of the study enables the identification of weaknesses early, allowing organizations to implement corrective actions before risks materialize into losses [37]. Empirical studies emphasize that MA is a critical enabler of ORM, particularly when combined with advanced analytics and automated monitoring tools [38, 39]. The effectiveness of monitoring depends on the quality of data collected, the independence of the monitoring function, and its integration with ERM frameworks. Strengthening MA requires investments in real-time anomaly detection, linking audit results to key performance indicators (KPIs), and adopting a continuous monitoring mindset rather than periodic reviews [40]. Thus, the authors gave hypotheses H9 and H6 in Figure 1 below.

- H9: Monitoring activities have a positive effect on operational risk management.
- H10: Monitoring activities have a positive effect on awareness and level of operation of ERM.

8. DIGITAL TRANSFORMATION (DT)

Digital transformation (DT) refers to the integration of digital technologies into banking processes, including AI, big data analytics, and blockchain. In the context of ORM, DT enhances the ability to detect, predict, and mitigate risks through automation and advanced data analysis [40, 41]. However, research shows that technology alone is insufficient for effective ORM; it must be complemented by a risk-aware culture and integrated ERM processes [42]. The study indicates that while DT supports risk management, its influence is secondary compared to cultural and organizational factors, such as IE. This may be due to gaps in staff training or incomplete integration of technology with existing risk management systems. To enhance the role of DT in ORM, banks must focus on aligning technology initiatives with ERM objectives, investing in digital literacy among employees, and conducting regular cyber risk assessments. Thus, the authors gave hypotheses H11 and H12 in Figure 1 below.

- H11: Digital transformation has a positive effect on operational risk management.
- H12: Digital transformation has a positive effect on awareness and level of operation of ERM.

9. AWARENESS AND LEVEL OF OPERATION OF ERM (AOF)

AOF captures the extent to which an organization understands, implements, and operationalizes the ERM framework. High ERM awareness ensures that risk management is embedded in strategic and operational decision-making [43]. AOF serves as a mediator, translating organizational capabilities into effective ORM outcomes [44]. The study confirms its mediating role. This suggests that factors such as IE, SO, and DT improve ORM primarily through their impact on AOF. In practice, banks with high ERM awareness tend to have integrated risk reporting, cross-departmental risk committees, and proactive incident management. Improving AOF requires ERM training programs, embedding risk considerations into performance evaluations, and developing ERM maturity models that guide continuous improvement.

- H13: AOF positively influences ORM.

The proposed research model aims to investigate the factors influencing operational risk management (ORM) in Vietnamese commercial banks, emphasizing both direct effects and indirect effects via a mediating variable: awareness and level of operation of the ERM framework (AOF). Building on the COSO-ERM framework (2017) and prior empirical findings, the model integrates six key independent variables: Internal environment (IE), strategic objectives (SO), control activities (CA), information and communication (IC), monitoring activities (MA), and digital transformation (DT). By employing a structural equation modeling (SEM) approach, this research model not only quantifies the relationships among constructs but also identifies the most influential drivers of ORM. The results will provide actionable insights for banks and regulators seeking to enhance operational risk governance in a rapidly digitalizing environment.

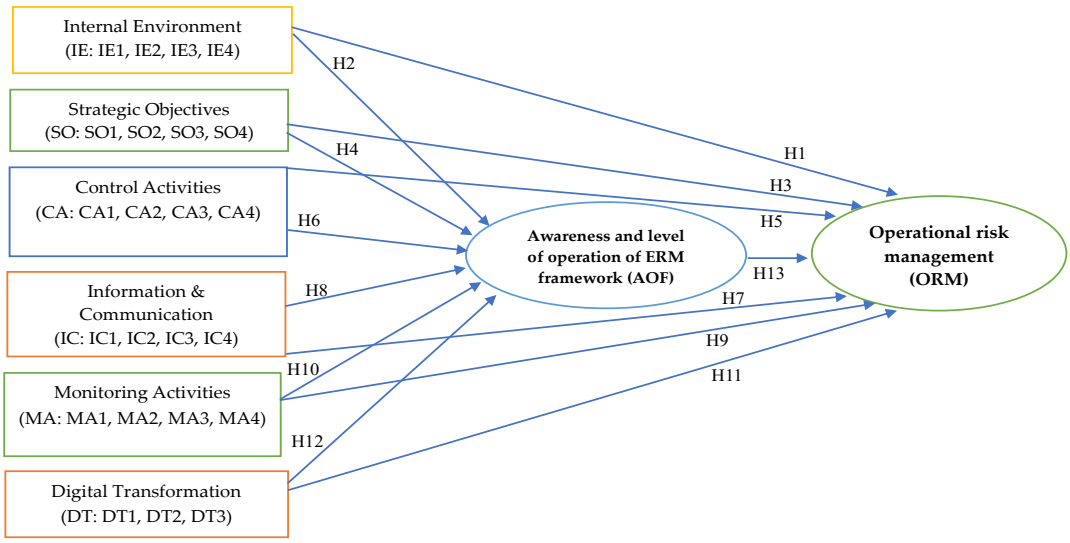


FIGURE 1. A research model for critical factors affecting operational risk management.

Figure 1 illustrates the proposed research model, which shows the relationships between six organizational factors and Operational Risk Management (ORM), with Awareness and level of operation of the ERM framework (AOF) serving as a mediating variable. The independent variables: Internal environment (IE), strategic objectives (SO), control activities (CA), information and communication (IC), monitoring activities (MA), and digital transformation (DT) are hypothesized to influence ORM both directly and indirectly through AOF. IE establishes the foundation for risk culture and governance, while SO ensures that risk management is aligned with strategic goals. CA represents the operational mechanisms that mitigate risk, and IC facilitates the adequate flow of risk-related information. MA provides continuous oversight, whereas DT enables advanced tools and data-driven approaches to enhance ORM. The model, depicted through hypotheses H1–H13, underscores AOF's pivotal role in translating organizational capabilities into effective ORM outcomes. This integrated approach supports the development of a robust operational risk framework.

III. METHODS OF RESEARCH

1. RESEARCH DESIGN

This research consists of two phases: (1) conducting qualitative research, and (2) conducting formal quantitative research. Qualitative research is conducted through in-depth interviews to establish the scales and research hypotheses outlined below.

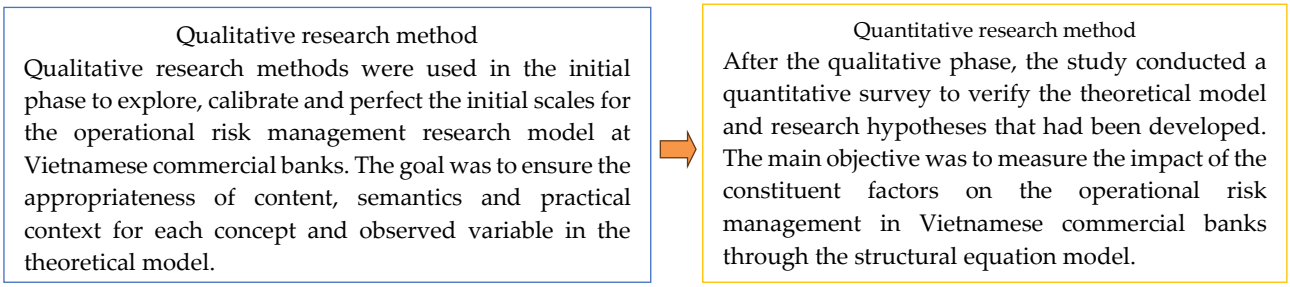


FIGURE 2. A research process for critical factors affecting operational risk management.

Phase one involves qualitative research and phase two involves quantitative study. Qualitative research is conducted through in-depth interviews to develop the scales and test the hypotheses shown in Figure 1. After obtaining thorough information about the research objectives, methodology, and potential implications, all participants provided their informed consent to participate in this study prior to data collection. Permission to participate was obtained in writing. The participants' written consent was obtained by signing a letter describing the study's goals, their rights, and the guarantees of confidentiality [45]. All participants agreed to participate and completed the study questionnaire, as shown in Table A1. This study integrates qualitative and quantitative methodologies in a structured mixed-methods approach to investigate key factors influencing operational risk management (ORM). Figure 2 illustrates the two-stage method that can corroborate empirical findings through quantitative analysis and ensure conceptual depth through qualitative insights, as discussed above.

2. QUALITATIVE PHASE

Qualitative research methods were employed in the initial phase to explore, calibrate, and refine the initial scales for the operational risk management research model at Vietnamese commercial banks. The goal was to ensure the appropriateness of content, semantics, and practical context for each concept and observed variable in the theoretical model. Specifically, the research team conducted an expert survey using semi-structured interviews with 25 experts with experience in the field of banking risk management. These experts work at 25 typical commercial banks, including state-owned banks, joint-stock commercial banks, joint-venture banks, and foreign-invested banks. Those selected to participate in the survey have 10 years or more of experience in the field of risk management and hold positions such as Director of Risk Management, Head of Internal Audit, Head of Compliance and Internal Control, or are senior consultants in the fields of finance and banking. Semi-structured interviews are designed with a system of open-ended questions, focusing on main contents such as:

- Awareness and level of operation of the enterprise risk management (ERM) framework,
- Applying digital technology in operational risk management,
- Actual situation of control, supervision, and internal communication in risk management,
- Linkage between banking strategy and risk control objectives.

Interviews were conducted face-to-face and/or online, with an average duration of 30 to 60 minutes. Data were audio-recorded (with consent), and notes were taken and coded using content analysis. Data processing focused on identifying recurring themes, classifying groups of opinions, and extracting key elements from expert perspectives.

Qualitative research results are used to:

- Adjust the observed variables to suit the Vietnamese banking context.
- Remove or merge unnecessary indicators.
- Add measurement variables not covered in previous studies.

Therefore, the study has completed the official scale, which consists of 6 independent factor groups (Internal environment, strategic objectives, control activities, information and communication, monitoring activities, and digital transformation), 1 intermediate variable (Awareness and level of operation of ERM framework - AOF), and 1 dependent variable (Operational risk management - ORM). Each variable group has between 3 and 5 clearly defined indicators.

Overall, the qualitative phase played a crucial role in ensuring the content validity, localization, and practical relevance of the research model in the Vietnamese banking sector. This also serves as a necessary basis for conducting quantitative research in the next phase. Moreover, the reliability of the qualitative results was ensured through methodological triangulation, member checking with selected participants, and expert validation of the coding scheme by two independent reviewers. These procedures enhanced the credibility and dependability of the qualitative findings.

3. QUANTITATIVE PHASE

The authors employed a non-probability purposive sampling technique. Initial quantitative research was conducted from May 1, 2025, to May 6, 2025, in Hanoi, Ho Chi Minh City, Da Nang, Hai Phong, and Can

Tho to evaluate the modified scale. The sample size consisted of 1.000 questionnaires, which were distributed in person and online. As a result, 958 valid questionnaires were collected (validity rate reached 95.8%) and processed and analyzed based on research questionnaires, with only 958 votes processed [45].

Following the qualitative phase, the study conducted a quantitative survey to verify the theoretical model and research hypotheses that had been developed. The primary objective was to assess the impact of constituent factors on the effectiveness of operational risk management in Vietnamese commercial banks using the structural equation model (SEM).

Survey subjects and scope: The survey subjects were officers and employees working in departments related to risk management at 25 commercial banks, including:

- Risk management department,
- Internal audit,
- Internal control,
- Planning – strategy,
- Information technology,
- Legal and compliance.

These are groups of personnel who have knowledge and a direct role in operating the bank's operational risk management system. The survey was conducted in five major cities, representing key economic regions of Vietnam: Hanoi, Ho Chi Minh City, Da Nang, Hai Phong, and Can Tho. These are places with many bank branches and are highly representative of the national financial system. A total of 1.000 questionnaires were distributed in person and online. As a result, 958 valid questionnaires were collected (validity rate reached 95.8%) and processed and analyzed.

Data processing tools and processes in this study, data processing and analysis were conducted systematically to test the reliability, validity, and hypotheses in the theoretical model. Data from 958 valid survey forms were analyzed in 5 specific steps as follows: Descriptive statistical analysis: The objective of this step is to describe the demographic and behavioral characteristics of the survey sample, including the criteria: gender, age, education level, job position, and work experience in the banking sector. This description helps assess the diversity, representativeness, and balance of the research sample, thereby strengthening the generalizability of the model.

4. . DATA ANALYSIS

The descriptive statistics are also used to check the validity and quality of data, specifically to detect unusual data, deviations, or outliers. Indicators such as the mean, standard deviation, skewness, and kurtosis are also analyzed to verify the normal distribution of the measured variables. These operations are performed using SPSS 20.0 software. Scale reliability analysis (Cronbach's Alpha): Before conducting an in-depth analysis, it is necessary to test the internal reliability of each scale. Cronbach's Alpha method is used to determine the level of consistency between observed variables within the same concept. If Cronbach's Alpha coefficient is ≥ 0.7, then the scale is considered acceptable. Observed variables with a Corrected Item Total Correlation coefficient below 0.3 will be eliminated.

In this study, eight scales were used: IE, SO, CA, IC, MA, DT, AOF, and ORM. This step serves as an initial screening step, ensuring that the indicators included in the subsequent analysis are highly reliable. Exploratory Factor Analysis (EFA): After assessing reliability, the study proceeded with EFA to determine the number of factors, test the latent structure, and group the observed variables. Factor extraction method: principal axis factoring, factor rotation: Promax Rotation (allows correlated factors), inspection conditions: KMO ≥ 0.6 (ensuring data adequacy), Bartlett's Test Sig. < 0.05 and factor loading ≥ 0.5 [45].

There is no cross-loading phenomenon, such as variable loading highly on many factors. The purpose of EFA is to verify the structure of the scales following the theory, eliminate non-standard observed variables, and thereby provide the basis for building a confirmatory factor analysis (CFA) model. Confirmatory Factor Analysis (CFA): CFA analysis is used to confirm the validity of the measurement model. CFA helps to test the relationship between observed variables and corresponding latent variables, thereby establishing evaluation criteria such as: Overall model fit (Model Fit): Chi-square/df < 3.0 or 5.0, CFI, TLI ≥ 0.90, RMSEA ≤ 0.08, SRMR ≤ 0.08, composite reliability (CR) ≥ 0.7, average variance extracted (AVE) ≥ 0.5 and convergence:

Factor loading ≥ 0.5. Discriminability: Compare AVE with the squared correlation coefficient between concepts. If CFA gives good results, the measurement model is considered eligible for SEM structural model testing. Structural Equation Modeling (SEM): The SEM model is used to test the causal relationships among independent variables (IE, SO, CA, IC, MA, DT), the mediating variable (AOF), and the dependent variable (ORM). This analysis enables evaluation of direct interaction between concepts (via path coefficients), indirect effects (through the intermediate variable AOF), and total effects [45].

SEM was performed using the Maximum Likelihood estimation method on AMOS 20.0 software. In addition, to test the mediating role of AOF, the study used the Bootstrapping technique with 5.000 replicate samples to calculate the standard deviation, confidence interval, and p-value for the indirect paths. The use of SEM not only allows for a comprehensive assessment of the research model but also enables the testing of each hypothesis (H1–H13) specifically. The SEM model provides empirical evidence on the influencing mechanism of each factor on the effectiveness of operational risk management in the context of Vietnamese banks, especially the mediating role of awareness and the level of ERM framework (AOF) operation.

Finally, the model tests led the authors to offer governance implications. Initially, the authors created a study model to test the reliability and validity of the expected scale. Subsequently, the authors obtained official data to test their hypothesis and model, and suggested policy changes to improve operational risk management. The sequential application of EFA, CFA, and SEM allowed the study to comprehensively address all research objectives from exploring the underlying structure of operational risk constructs to empirically validating the proposed causal relationships among them.

VI. RESULTS AND DISCUSSION

1. ASSESSING THE CURRENT STATUS OF OPERATIONAL RISK MANAGEMENT AT VIETNAMESE COMMERCIAL BANKS IN THE PERIOD 2023-2024

In the context of the volatile global economy and finance in the period of 2023-2024, the Vietnamese banking industry faces many serious challenges related to operational risks, requiring credit institutions, especially commercial banks (CBs), to quickly innovate and strengthen their risk management systems. Operational risks such as system errors, fraud, violations of internal procedures, IT incidents, or impacts from the legal environment... are no longer "hidden" risks but have directly affected the efficiency and reputation of the entire industry. The year 2023 is marked by many significant fluctuations within the banking system. Although the economy continues to experience positive growth, credit growth tends to slow down, reflecting the caution of credit institutions in the face of pressure from bad debt and macroeconomic risks. Many banks have recorded bad debt ratios exceeding the safe level of 3%, especially in the context of the gradual end of post-COVID-19 support credit packages, creating a gap in credit risk management and thereby pressure on operational risk control. One notable event was the State Bank of Vietnam (SBV) providing exceptional support to SCB, a bank that was once among the largest in terms of assets. The support package of more than 24 billion USD (nearly 600.000 billion VND) granted to SCB in the period of 2023-2024 is a clear sign that systemic risks are at an alarming level. This event is not only a lesson in credit risk management but also highlights weaknesses in internal supervision, operational control, and the early detection of operational risks.

In fact, most Vietnamese commercial banks during this period have made positive progress in building and operating an operational risk management framework in line with international standards, especially Basel II and Basel III. Processes such as operational risk analysis, the internal assessment, the three lines of defense model, and periodic risk reporting have gradually become standard practices in many large banks, including Vietcombank, Techcombank, MB, BIDV, and VPBank. However, it must also be recognized that many small and medium-sized banks still formally implement operational risk management, lacking depth, or not yet integrated with the bank's overall development strategy. A notable highlight in the 2023-2024 period is the strong development of digital transformation in the Vietnamese banking system, especially in terms of risk management support. High-tech solutions, including behavioral monitoring systems, big data analytics, and artificial intelligence (AI) applications, are being widely deployed to detect fraud and manage operational incidents. Many banks have developed real-time operational risk dashboards, providing early

warnings of risks associated with processes, personnel, customers, and technology. In particular, in the context of digitizing business processes, many activities that were previously performed manually have now been automated, thereby helping to minimize risks associated with operational errors or internal fraud.

However, the gap between banks in terms of technology application remains large. Small-scale banks, with limited capital, a lack of unified data platforms, or inadequate specialized IT personnel, have struggled to effectively apply digital tools in risk management. This results in a "two-speed" phenomenon in operational risk management capacity between large and small banks. In terms of organizational structure, most commercial banks have established independent risk management departments and upgraded their internal audit and compliance control systems. However, the performance of these departments is not really uniform. Some banks have recorded that risk warnings are not handled properly, or that incidents continue to recur due to a lack of cross-monitoring and internal coordination. The “information barrier” between the operations department and the risk department still exists, leading to the three-line-of-defense model not being fully effective.

In particular, the integrated enterprise risk management (ERM) framework has only been implemented at a basic level in most banks. Some units have built an ERM on paper, but the actual operation has not been synchronized. The concept of "risk culture" has not been fully internalized among the banking staff, resulting in operational risks persisting due to personal errors, inadequate skills in identifying and handling risks, or violations of business processes. Training and capacity building for staff working on operational risk management have not yet received adequate investment. In many cases, staff from the credit or accounting departments are assigned to perform risk control, leading to a lack of in-depth professional background and an inability to analyze data or forecast risk trends. Recent studies have also shown that the role of human resources is a key factor in effective risk management, but it is a common weakness in many domestic commercial banks. From the perspective of the management agency, the State Bank has issued numerous documents to guide and supervise commercial banks in implementing risk control standards properly. Regular and irregular inspections and audits have been increased, especially after major incidents such as SCB or Van Thinh Phat. This has led banks to comprehensively review their internal management systems. However, to achieve long-term effectiveness, a preventive monitoring mechanism is needed rather than just post-audit processing.

In summary, it can be said that the current state of operational risk management at Vietnamese commercial banks from 2023 to 2024 is one of strong transition. Improvements in awareness, investment in technology, the establishment of an independent monitoring apparatus, and adherence to international standards are clear steps forward. At the same time, shortcomings related to human resource quality, risk culture, the level of ERM integration, and internal coordination capabilities continue to be significant barriers. To improve the effectiveness of operational risk management in the coming period, banks need to prioritize: (1) promoting digitalization of control processes; (2) providing in-depth training for risk management officers; (3) building an early warning and rapid response system; (4) promoting an organizational risk culture; and (5) integrating risk management into banking strategy. Only when these factors are ensured can the banking system develop sustainably, improve crisis response capacity, and better meet the requirements of international financial integration.

2. ANALYSIS OF DESCRIPTIVE STATISTICS AND CRONBACH’S ALPHA FOR FACTORS AFFECTING THE OPERATIONAL RISK MANAGEMENT

Table 1. Testing descriptive statistics and Cronbach's alpha for critical factors influencing operational risk management.

Items of operational risk management	Cronbach's alpha	Mean	Std. Deviation
1. Internal environment (IE: IE1, IE2, IE3, IE4)	0.934	3.019	1.002
2. Strategic objectives (SO: SO1, SO2, SO3, SO4)	0.944	3.044	0.972
3. Control activities (CA: CA1, CA2, CA3, CA4)	0.938	3.049	1.004

4. Information and communication (IC: IC1, IC2, IC3, IC4)	0.879	2.421	0.674
5. Monitoring activities (MA: MA1, MA2, MA3, MA4)	0.860	3.409	0.940
6. Digital transformation (DT: DT1, DT2, DT3)	0.909	3.303	0.982
7. Awareness and level of operation of ERM framework (AOF: AOF1, AOF2, AOF3)	0.893	3.310	0.979
8. Operational risk management (ORM: ORM1, ORM2, ORM3)	0.832	2.365	0.656

Source: Processed by SPSS 20.0

Table 1 presents the reliability analysis (Cronbach's alpha) and descriptive statistics (mean and standard deviation) for eight constructs that are considered critical factors influencing operational risk management (ORM). These constructs include: Internal environment (IE), strategic objectives (SO), control activities (CA), information and communication (IC), monitoring activities (MA), digital transformation (DT), awareness and level of operation of ERM framework (AOF), and the dependent variable operational risk management (ORM). The results demonstrate that all eight constructs exhibit high internal consistency reliability, with Cronbach's alpha coefficients ranging from 0.832 to 0.944, which exceeds the widely accepted threshold of 0.70 for social science research (Nunnally & Bernstein, 1994). This indicates that the survey items used to measure these constructs are reliable and can be confidently utilized in subsequent factor analysis (EFA and CFA) and SEM testing. Table 1 tests for analysis of descriptive statistics and Cronbach's alpha for operational risk management factors, following:

- Internal environment (IE): having Cronbach's alpha: 0.934, Mean: 3.019, Std. Deviation: 1.002. The internal environment (IE) construct demonstrates excellent internal consistency (α = 0.934), reflecting that the four measurement items (IE1–IE4) are closely related and measure the same underlying concept. The mean score of 3.019 (on a 5-point Likert scale) suggests that respondents perceive the internal environment of banks encompassing leadership commitment, risk culture, and internal policies as moderate. The relatively high standard deviation (1.002) suggests that opinions among employees vary somewhat. While some banks have established a solid risk management culture, others may still lack clear risk governance frameworks.
- Strategic objectives (SO): having Cronbach's alpha: 0.944, Mean: 3.044, Std. Deviation: 0.972. The strategic objectives (SO) dimension exhibits the highest Cronbach's alpha (0.944), indicating strong coherence among the four items (SO1–SO4). The mean value of 3.044 suggests that the integration of risk management into strategic goals is recognized to some extent, but not fully optimized across all banks. A standard deviation of 0.972 implies moderate variability in responses, indicating that some banks have well-defined risk-oriented strategic objectives, whereas others may treat risk management as a secondary consideration rather than an integral component of strategy.
- Control activities (CA): having Cronbach's alpha: 0.938, Mean: 3.049, Std. Deviation: 1.004. The control activities (CA) factor also achieves high reliability (α = 0.938). With a mean score of 3.049, respondents perceive internal control measures as being moderately effective. These activities, including standard operating procedures, compliance protocols, and corrective mechanisms, are crucial for minimizing operational risk. The relatively high standard deviation (1.004) suggests that the effectiveness of control activities varies among banks, possibly due to differences in resources, technology, and staff training.
- Information and communication (IC): having Cronbach's alpha: 0.879, Mean: 2.421, Std. Deviation: 0.674. Among all factors, information and communication (IC) exhibits the lowest mean value (2.421), indicating that respondents perceive this area as the weakest link in the ORM framework. Despite having an acceptable reliability score (α = 0.879), the low mean highlights a significant challenge: the flow of information regarding risks, incidents, and control measures within banks is insufficient. The relatively small standard deviation (0.674) indicates that this perception is consistent across respondents, suggesting a systemic issue within the industry. Poor communication and lack of transparency in risk information can significantly undermine timely decision-making and the effectiveness of operational risk management.
- Monitoring activities (MA): having Cronbach's alpha: 0.860, Mean: 3.409, Std. Deviation: 0.940. Monitoring activities (MA) has a Cronbach's alpha of 0.860, which is good, and a relatively high mean score of 3.409, making it the highest-rated construct in Table 1. This result suggests that most banks have put significant effort into monitoring and auditing processes, including periodic checks, performance reviews, and

independent assessments. The standard deviation of 0.940 shows a moderate spread of responses, but overall, respondents agree that monitoring is among the stronger aspects of ORM in their institutions.

- Digital transformation (DT): having Cronbach's alpha: 0.909, Mean: 3.303, Std. Deviation: 0.982. Digital Transformation (DT) shows strong reliability (α = 0.909) and a mean score of 3.303, indicating a positive perception of banks' efforts in adopting digital technologies for risk management. The high reliability reflects that the three measurement items (DT1–DT3) effectively capture the dimension of technological innovation and digital integration. However, the standard deviation (0.982) implies that while some banks are leading in digital initiatives (e.g., AI-based fraud detection, real-time monitoring dashboards), others are still in the early stages of digital adoption.
- Awareness and level of operation of ERM framework (AOF): having Cronbach's alpha: 0.893, Mean: 3.310, Std. Deviation: 0.979. AOF, representing awareness and implementation of the enterprise risk management (ERM) framework, has a high reliability (α = 0.893) and a mean value of 3.310. This result indicates that respondents acknowledge a reasonably good level of awareness and application of ERM principles within their banks. A standard deviation of 0.979 suggests that ERM maturity varies, with some banks integrating ERM into their core decision-making processes, while others implement ERM only superficially.
- Operational risk management (ORM): having Cronbach's alpha: 0.832, Mean: 2.365, Std. Deviation: 0.656. The dependent variable ORM shows the lowest reliability among all constructs (α = 0.832), but it still surpasses the acceptable threshold of 0.7. The mean score of 2.365 is the lowest overall, reflecting respondents' perception that current operational risk management practices are below expectations or only moderately effective. The low standard deviation (0.656) indicates that this opinion is widely held among employees across various banks. This finding suggests that, despite progress in some areas, such as monitoring and digital transformation, the overall ORM framework still faces significant gaps.

A comparison of the constructs reveals a notable mismatch between inputs and outcomes. For example, monitoring activities (MA) and digital transformation (DT) are rated relatively high (means > 3.3), and awareness of ERM (AOF) is also above 3.3, yet the overall ORM score is only 2.365. This gap suggests that although banks have invested in monitoring and technology, these efforts have not yet translated into substantial improvements in risk outcomes. One possible explanation is that weak Information and Communication (IC) (mean = 2.421) undermine the effectiveness of other factors, as poor information flow can render monitoring and digital systems less impactful.

Managerial implications: The results of Table 1 highlight several important managerial implications:

Strengthen information and communication (IC): Given its low mean score, banks need to prioritize enhancing internal communication channels, transparency of risk reports, and information sharing across departments. Additionally, leveraging monitoring and digital transformation are essential, although MA and DT are relatively strong. Banks should ensure that these systems are fully integrated with the ERM framework to maximize their impact on ORM outcomes. Improve internal environment and strategic alignment: IE, SO, and CA are rated around the neutral midpoint (3.0), indicating the need to embed risk awareness into the bank's culture, strategic planning, and daily operations. Focus on ERM maturity (AOF): With an AOF score of 3.310, banks are on the right track but must continue to strengthen ERM adoption, ensuring that risk management is not just a compliance exercise but a strategic advantage.

In summary, Table 1 highlights the crucial role of well-designed and reliable constructs in assessing operational risk management. While the reliability scores confirm that the measurement scales are valid and consistent, the descriptive statistics reveal key strengths, such as monitoring activities and digital transformation, as well as weaknesses, including information and communication, and overall ORM effectiveness. The findings suggest that banks should not only invest in digital tools and monitoring systems but also foster a culture of transparent communication and strategic alignment to achieve meaningful improvements in operational risk outcomes.

Table 2. Testing critical factors affecting the operational risk management.

Hypothesis	Relationships			Standardized estimate	S. E	C. R	P value	Supported
H10	MA	→	AOF	0.149	0.027	5.043	***	Yes
H12	DT	→	AOF	0.056	0.029	2.771	0.006	Yes
H2	IE	→	AOF	0.568	0.029	17.402	***	Yes
H4	SO	→	AOF	0.091	0.024	3.233	0.001	Yes
H6	CA	→	AOF	0.110	0.022	3.905	***	Yes
H8	IC	→	AOF	0.076	0.047	2.692	0.007	Yes
H1	IE	→	ORM	0.337	0.022	8.689	***	Yes
H3	SO	→	ORM	0.103	0.016	3.429	***	Yes
H5	CA	→	ORM	0.090	0.015	3.058	0.002	Yes
H7	IC	→	ORM	0.140	0.032	4.646	***	Yes
H9	MA	→	ORM	0.110	0.018	3.600	***	Yes
H11	DT	→	ORM	0.057	0.020	2.681	0.007	Yes
H13	AOF	→	ORM	0.317	0.026	7.901	***	Yes

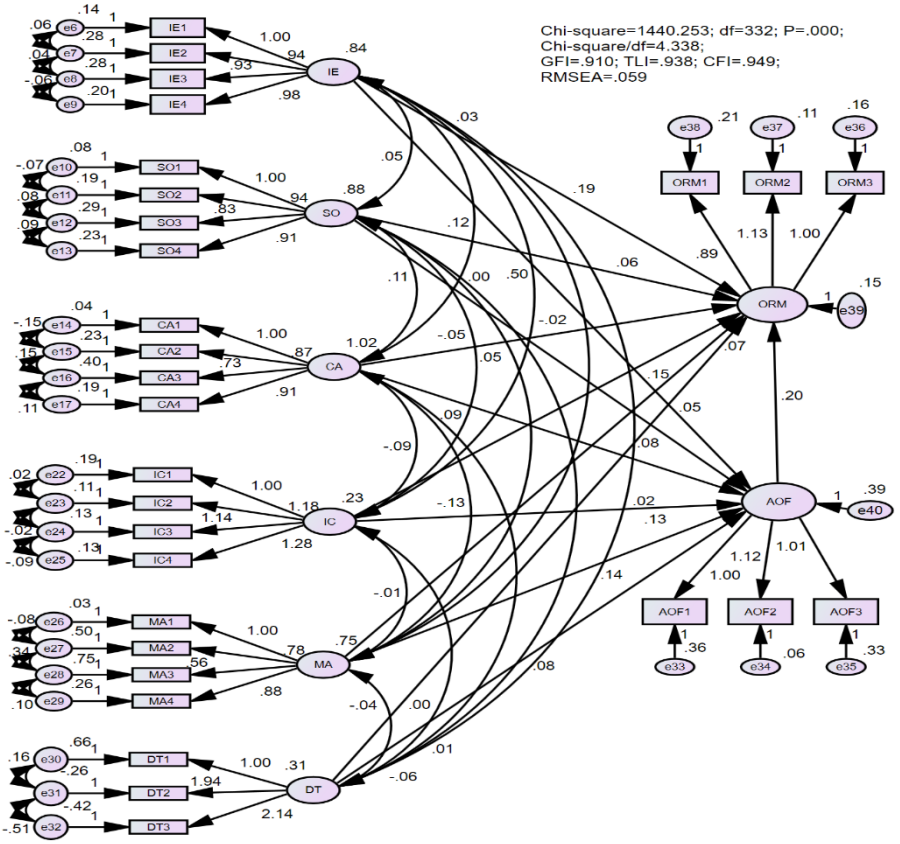
Source: Processed by SPSS 20.0, Amos; *** is significant with 1%.

Table 2 presents the results of hypothesis testing for the structural model, which evaluates the direct and indirect effects of six independent variables: Internal environment (IE), strategic objectives (SO), control activities (CA), information and communication (IC), monitoring activities (MA), and digital transformation (DT) on the mediator Awareness and level of operation of ERM framework (AOF) and the dependent variable operational risk management (ORM). The table also provides key statistical indicators such as standardized estimates (β), standard errors (S.E.), critical ratios (C.R.), and p-values, which collectively determine whether the proposed hypotheses (H1–H13) are accepted or rejected.

- Overview of results shows: All 13 hypotheses (H1–H13) have been accepted at a significance level of $p < 0.01$, with most relationships significant at $p < 0.001$. This outcome demonstrates the robustness of the proposed model and validates the conceptual framework, where both direct and mediated effects play a critical role in shaping operational risk management outcomes. The standardized estimates (β) range from 0.056 (DT → AOF) to 0.568 (IE → AOF), showing that the strength of influence varies notably across factors. Among these, Internal Environment (IE) emerges as the dominant driver, exerting a substantial direct effect on both AOF (β = 0.568) and ORM (β = 0.337). Other factors, such as SO, CA, IC, MA, and DT, have positive but comparatively moderate effects on AOF and ORM.
- Effects on the mediator (AOF) showed: H2: IE → AOF (β = 0.568, C.R = 17.402, $p < 0.001$): The internal environment has the most decisive influence on AOF. A standardized coefficient of 0.568 indicates that a well-structured internal environment, characterized by strong leadership, a risk-aware culture, and robust internal policies, significantly enhances the awareness and operationalization of the ERM framework. This aligns with the literature, which emphasizes that a strong internal risk culture forms the foundation of effective risk governance (COSO, 2017). H4: SO → AOF (β = 0.091, C.R = 3.233, p = 0.001): Strategic objectives also have a positive impact on AOF but with a more negligible effect (β = 0.091). This implies that while aligning risk management with strategic goals is essential, it may not be as critical as organizational culture (IE) in fostering ERM awareness. H6: CA → AOF (β = 0.110, C.R = 3.905, $p < 0.001$): Control activities (e.g., standard operating procedures, internal audits) positively contribute to AOF (β = 0.110). This suggests that adequate controls help embed ERM practices into daily operations. H8: IC → AOF (β = 0.076, C.R = 2.692, p = 0.007): Information and Communication (IC) exert a relatively small positive effect on AOF (β = 0.076). This reflects a possible weakness in internal communication flows, which aligns with the descriptive results in Table 1, where IC had the lowest mean score (2.421). H10: MA → AOF (β = 0.149, C.R = 5.043, $p < 0.001$): Monitoring activities have a moderate influence on AOF (β = 0.149), indicating that continuous monitoring and feedback loops help increase ERM awareness and operationalization. H3: DT → AOF (β = 0.056, C.R =

2.771, p = 0.006): Digital transformation has the weakest direct effect on AOF (β = 0.056). This suggests that while technology is a necessary enabler, it does not automatically enhance ERM awareness unless accompanied by cultural and procedural improvements.

- Direct effects on ORM showed: H1: IE → ORM (β = 0.337, C.R = 8.689, p < 0.001): Internal environment also has a substantial direct effect on ORM (β = 0.337), making it the most significant predictor of operational risk management outcomes. This reinforces the view that a risk-oriented culture and leadership commitment have a direct influence on the effectiveness of risk mitigation. H3: SO → ORM (β = 0.103, C.R = 3.429, p < 0.001): Strategic objectives show a positive impact (β = 0.103), which suggests that banks with well-defined and risk-aware strategic goals are better at managing operational risk. H5: CA → ORM (β = 0.090, C.R = 3.058, p = 0.002): Control activities have a relatively small yet significant effect (β = 0.090). While controls are essential, they are most effective when integrated with other key elements, such as ERM awareness and digital systems. H7: IC → ORM (β = 0.140, C.R = 4.646, p < 0.001): Information and Communication has a moderate impact on ORM (β = 0.140), highlighting the importance of transparent and efficient communication in detecting and mitigating operational risks. H9: MA → ORM (β = 0.110, C.R = 3.600, p < 0.001): Monitoring activities influence ORM (β = 0.110), confirming that continuous oversight is a key mechanism for controlling operational risk events. H11: DT → ORM (β = 0.057, C.R = 2.681, p = 0.007): Digital transformation has the weakest direct effect on ORM (β = 0.057). This suggests that while technology improves efficiency, its direct impact on risk management outcomes is limited unless fully integrated into the ERM framework.
- Mediating role of AOF showed: H13: AOF → ORM (β = 0.317, C.R = 7.901, p < 0.001): AOF significantly influences ORM (β = 0.317), demonstrating its role as a key mediator. This indicates that factors such as internal environment, monitoring, and digital transformation indirectly improve ORM through their positive impact on AOF. The strong path from AOF to ORM suggests that ERM awareness and implementation amplify the effectiveness of other factors.
- Key insights: Dominance of internal environment (IE): IE stands out as the most influential factor, impacting both AOF and ORM more strongly than any other variable. A well-structured risk culture, management support, and ethical standards directly enhance ORM effectiveness. Moderate Roles of SO, CA, IC, and MA: These factors provide meaningful but secondary contributions to both AOF and ORM. For example, IC and CA show smaller coefficients, suggesting room for improvement in communication practices and the consistency of control measures. Technology as an Enabler, not a Driver: DT's weak direct effects (β = 0.056 on AOF, β = 0.057 on ORM) indicate that digital transformation alone is not sufficient to drive ORM. Its value is realized only when integrated into broader ERM practices and supported by a strong internal environment. Critical Role of ERM Awareness (AOF): The path AOF → ORM (β = 0.317) confirms that ERM functions as a bridge, translating the efforts in internal controls, monitoring, and strategy into tangible improvements in risk management outcomes.
- Managerial implications: Focus on culture and leadership as IE is the strongest predictor; banks should prioritize developing a risk-aware culture and ensure top management actively promotes ERM practices. Enhancing information and communication, based on the relatively low influence of IC, highlights the need to improve transparency, reporting systems, and cross-departmental communication. Align risk with strategic objectives by integrating risk management into banks' strategic planning processes, ensuring that ORM is not an isolated function. Leveraging technology through digital initiatives within the ERM framework should be embedded to maximize the benefits of risk mitigation.



Source: Processed by SPSS 20.0, Amos

FIGURE 3. Testing for critical factors affecting operational risk management.

Figure 3 illustrates the SEM diagram, which shows the structural model evaluating factors affecting operational risk management (ORM) through the mediating variable AOF - Awareness and the level of operation of the ERM framework. The model fit indices (Chi-square/df = 4.338, GFI = 0.910, TLI = 0.938, CFI = 0.949, RMSEA = 0.059) indicate that the model demonstrates a good overall fit.

The internal environment (IE) exhibits the highest standardized loading (0.84) and has the most decisive influence on both ORM (0.33) and AOF (0.50), confirming that risk culture and internal governance serve as foundational elements of effective risk management. Control Activities (CA) and Strategic Objectives (SO) also have positive but more minor effects (approximately 0.11–0.12). Information and communication (IC) influences ORM indirectly through AOF (0.13), highlighting the importance of transparent information flow. Monitoring activities (MA) and digital transformation (DT) contribute positively, albeit with relatively low coefficients (0.08 and 0.02), indicating that technology and monitoring mechanisms require deeper integration with the ERM framework.

Notably, the path AOF → ORM (0.20) highlights the critical mediating role of ERM awareness and implementation, suggesting that internal factors, strategic objectives, control measures, and digital initiatives enhance ORM effectiveness only when systematically embedded within the ERM framework. Figure 3 confirms that all six independent variables have a positive influence on ORM, either directly or indirectly through AOF. Internal environment emerges as the most significant factor, while digital transformation plays a supporting role. The strong mediating effect of AOF highlights the importance of ERM awareness and operationalization as a central pillar of modern risk management. These results suggest that Vietnamese

commercial banks need a balanced approach that combines strong leadership, strategic alignment, robust controls, and integrated digital systems, all channeled through a mature ERM framework.

Table 3. Testing average variance extracted for factors affecting operational risk management.

Code	CR	AVE	MSV	Results
AOF	0.896	0.743	0.343	Good
IE	0.935	0.784	0.343	Good
SO	0.944	0.808	0.025	Good
CA	0.937	0.789	0.034	Good
IC	0.881	0.651	0.025	Good
MA	0.857	0.607	0.029	Good
DT	0.914	0.781	0.015	Good
ORM	0.833	0.627	0.319	Good

Source: Author's own work

Table 3 presents the results of testing the reliability and validity of the constructs affecting operational risk management (ORM). All constructs exhibit strong composite reliability (CR) values, ranging from 0.833 (ORM) to 0.944 (SO), which are well above the recommended threshold of 0.70, indicating strong internal consistency. The average variance extracted (AVE) values for all constructs are greater than 0.60, with the highest being 0.808 (SO) and the lowest 0.607 (MA), indicating strong convergent validity and that the majority of the variance in the indicators is explained by the latent constructs. Moreover, the maximum shared variance (MSV) for all constructs is lower than their corresponding AVE, demonstrating good discriminant validity and ensuring that each construct is distinct from the others. Overall, these results confirm that the measurement model is both reliable and valid, providing a solid foundation for the subsequent SEM analysis and hypothesis testing.

Table 4. Testing Bootstrap 5.000 samples for factors affecting operational risk management.

Parameter			SE	SE-SE	Mean	Bias	SE-Bias	Result
MA	→	AOF	0.033	0.000	0.136	0.002	0.002	1.00
DT	→	AOF	0.034	0.000	0.077	0.003	0.003	1.00
IE	→	AOF	0.037	0.000	0.496	0.002	0.002	1.00
SO	→	AOF	0.025	0.000	0.072	0.007	0.004	1.75
CA	→	AOF	0.023	0.000	0.082	0.006	0.005	1.20
IC	→	AOF	0.081	0.001	0.100	0.006	0.004	1.50
IE	→	ORM	0.023	0.000	0.186	0.004	0.003	1.33
SO	→	ORM	0.023	0.000	0.055	0.001	0.002	0.50
CA	→	ORM	0.022	0.000	0.039	0.002	0.002	1.00
IC	→	ORM	0.067	0.001	0.119	0.002	0.002	1.00
MA	→	ORM	0.018	0.000	0.060	0.005	0.003	1.67
DT	→	ORM	0.024	0.000	0.044	0.003	0.002	1.50
AOF	→	ORM	0.029	0.000	0.209	0.003	0.002	1.50

Source: Processed by SPSS 20.0, Amos

Table 4 reports the results of the bootstrap method (5.000 samples) to evaluate the stability and reliability of parameter estimates in the SEM model. The key columns - SE (standard error), Bias, and SE-Bias help

assess the precision of the estimates and the potential bias due to sampling variability with confidence level 95%.

The results show that all standard errors (SEs) are minor (ranging from 0.018 to 0.081), indicating that the parameter estimates are highly stable across the resampled datasets. For example, the path IE → AOF has SE = 0.037, with a mean estimate of 0.496 and minimal bias (0.002), suggesting a robust and consistent influence of Internal Environment on AOF. Similarly, the path AOF → ORM (SE = 0.029, Mean = 0.209) confirms the mediating role of AOF with high reliability. Moreover, Bias and SE-Bias values are negligible across all parameters, indicating that no significant systematic bias exists in the bootstrapped estimates. The "Result" column (values close to 1.00 or slightly above) shows that the bootstrap confidence intervals are consistent with the significance of the paths observed in the original SEM results.

Overall, the bootstrap analysis validates the robustness of the SEM model, confirming that all key relationships, particularly IE → AOF, MA → AOF, and AOF → ORM, remain stable and statistically significant under resampling conditions.

3. DISCUSSIONS OF FINDINGS

This study set out to examine how six organizational antecedents: Internal environment (IE), strategic objectives (SO), control activities (CA), information and communication (IC), monitoring activities (MA), and digital transformation (DT) shape operational risk management (ORM) in Vietnamese commercial banks, both directly and indirectly through the mediator awareness and level of operation of the ERM framework (AOF). Using a two-stage design (qualitative scale development with 25 experts and quantitative SEM on 958 valid surveys), the paper presents a multi-layered picture of the maturity and effectiveness of ORM in the post-pandemic, high-uncertainty period (2023–2024). Below, we discuss the significant empirical insights, their theoretical implications, and managerial and policy implications.

- Measurement quality: a solid platform to read the structure based on the psychometric properties reported in Table 1 and Table 3 confirms that the constructs are measured reliably and validly. Cronbach's alpha values range from 0.832 to 0.944, indicating strong internal consistency across all scales. Composite Reliability (CR) values (0.833–0.944) and Average Variance Extracted (AVE) (0.607–0.808) surpass conventional thresholds, while MSV < AVE for every construct confirms discriminant validity [14, 15, 46, 47]. This gives confidence that the structural paths uncovered by SEM can be interpreted substantively rather than as artifacts of measurement error. A striking descriptive insight is that Information and Communication (IC) and ORM post the lowest mean scores (2.421 and 2.365, respectively), while Monitoring Activities (MA) and Digital Transformation (DT) are perceived as notably higher (3.409 and 3.303). In other words, although banks have invested in monitoring mechanisms and digital tools, employees still do not perceive ORM outcomes to be strong, and they rate risk information flows as weak. This "input–output" misalignment foreshadows the structural findings: without embedded ERM consciousness (AOF) and transparent, timely communication, technology and monitoring alone will not translate into superior ORM outcomes.
- Structural model: Internal environment is the anchor; ERM awareness is the bridge. Table 2 and the SEM diagram jointly indicate that all 13 hypothesized paths are statistically significant, demonstrating that each antecedent contributes incremental explanatory power to AOF and/or ORM. Yet, the magnitude of impacts is uneven, delivering several nuanced stories. The Internal Environment (IE) is the dominant driver: IE → AOF ($\beta = 0.568$, $p < 0.001$) is the strongest path leading to ERM awareness and operation. IE → ORM ($\beta = 0.337$, $p < 0.001$) is also the strongest direct determinant of ORM [18, 19, 48, 49]. This finding underscores that risk culture, tone at the top, clearly assigned responsibilities, and a coherent internal control philosophy are preconditions for both understanding ERM and delivering ORM performance. It aligns with the COSO-ERM and BCBS principles, which stress leadership commitment and a pervasive risk culture as the nucleus of a sound risk framework.
- ERM awareness and operation (AOF) matters and mediates: AOF → ORM ($\beta = 0.317$, $p < 0.001$) is sizeable, confirming AOF as a material mediator. While several antecedents (e.g., IE, SO, CA, IC, MA, DT) show direct positive effects on ORM, the indirect route via AOF is also critical [21, 23, 50, 51]. This means banks cannot rely solely on isolated functions, e.g., enhanced controls or increased monitoring; they must institutionalize

ERM, train their staff, and ensure that ERM is systematically integrated into planning, decision-making, and day-to-day execution. Strategic Objectives (SO), Control Activities (CA), Information and Communication (IC), and Monitoring Activities (MA) all positively influence AOF and ORM, but with smaller coefficients than IE: Their effects on AOF (β ranging from 0.076 to 0.149) indicate that they help operationalize ERM, albeit more modestly than IE. Their direct effects on ORM (β = 0.090–0.140) are statistically significant but not dominant. These patterns suggest complementarity: well-crafted objectives, robust controls, credible monitoring, and effective communication strengthen ERM awareness, which in turn transmits benefits to ORM. However, without a strong internal environment to orchestrate and internalize these functions, their effects risk becoming fragmented. Digital Transformation (DT) is essential but not sufficient: DT → AOF (β = 0.056, p = 0.006) and DT → ORM (β = 0.057, p = 0.007) are the weakest positive paths. Interpretation: technology is an enabler, not a guarantor. Banks may invest heavily in AI, big data, and real-time dashboards, but unless these technologies are aligned with ERM processes, risk culture, and decision rights, their impact on ORM remains muted. This helps explain the paradox from the descriptive statistics: high perceived DT, yet low ORM outcomes.

- Robustness: Bootstrap confirms the stability of the architecture. Table 4 (Bootstrap with 5.000 samples) confirms the stability of the structural paths. Standard errors are minor, biases are negligible, and SE-bias values approach zero, showing that the sample-based estimates are not inflated by sampling idiosyncrasies [29, 45, 47, 52, 53]. Importantly, the most significant effects in the original SEM—IE → AOF and AOF → ORM retain their magnitudes and remain significant in the bootstrap distribution, consolidating the conclusion that ERM awareness mediates the strongest organizational driver (IE) into ORM performance.
- Theoretical contributions: First, the study empirically verifies a dual-channel mechanism (direct + mediated) through which organizational predictors shape ORM, establishing Internal Environment as the core lever and AOF/ERM as the transmission belt [27, 33, 54, 55, 56]. This extends classical BCBS and COSO propositions with a quantified mediation structure, offering fine-grained evidence from an emerging market context. Second, by explicitly including Digital Transformation as a separate antecedent, the study adds to nascent literature that questions the "technology = better risk management" assumption. The results suggest that technology's payoff is conditional; it generates meaningful improvements only when absorbed into a mature ERM architecture and supported by a strong culture and leadership. Third, the finding that IC scores low on perception (mean = 2.421) but still shows statistically significant structural paths places risk information governance at the heart of ORM execution. This links the behavioral and communicative dimension of risk management (often overlooked) with hard outcomes, pushing future ORM research to better integrate communication and organizational learning theories.

The findings converge on a clear message: culture first, ERM next, then technology and communication throughout. Vietnamese commercial banks have begun to assemble the necessary components, including monitoring, digital tools, and control procedures. Still, true ORM excellence emerges only when these pieces are orchestrated by a strong internal environment and are coherently embedded within a living ERM framework. In a period marked by systemic stresses, this integrated route is not merely desirable; it is mission-critical for resilience, trust, and sustainable growth.

Moreover, the findings of this study provide several actionable implications for banking practitioners and policymakers. First, the strong effect of the internal environment on operational risk management (ORM) underscores the need for Vietnamese banks to cultivate a risk-aware culture. This requires leadership commitment to ethical governance, transparent decision-making, and accountability mechanisms that promote integrity throughout the organization. Second, the mediating role of Awareness and Operation of ERM (AOF) highlights that policies and technological initiatives only improve ORM when employees understand and apply them in daily operations. For example, training programs that empower frontline staff to recognize irregular transactions, or communication campaigns that encourage open reporting of near-miss incidents, can transform compliance from a formality into a living practice. Third, the relatively weak direct impact of digital transformation indicates that technology must be aligned with human capabilities and risk frameworks. Banks investing in AI-based fraud detection, big data analytics, or core banking upgrades should complement these with systematic ERM awareness initiatives. Without this alignment, technological investments risk underperforming. Finally, for regulators, the results suggest that compliance with Basel

II/III should not be treated as a box-ticking exercise. Instead, supervisory authorities should encourage banks to institutionalize risk culture through mandatory ERM training, integrated reporting mechanisms, and incentives for effective risk practices. Such measures will not only strengthen individual banks but also enhance the resilience and competitiveness of Vietnam's financial system in a digital era.

V. CONCLUSIONS AND POLICY RECOMMENDATIONS

1. CONCLUSIONS

This research investigated the critical factors influencing operational risk management (ORM) in Vietnamese commercial banks during the period of 2023–2024, focusing on the interplay between six independent variables - Internal environment (IE), strategic objectives (SO), control activities (CA), information and communication (IC), monitoring activities (MA), and digital transformation (DT) and the mediator awareness and level of operation of the ERM framework (AOF). By adopting a hybrid methodology that combines qualitative expert interviews with 25 senior risk management professionals and quantitative SEM analysis on 958 valid responses, the study provides comprehensive insights into the drivers, mechanisms, and outcomes of ORM within the banking sector. The research confirms that all proposed constructs exhibit high reliability and validity. The measurement model, evaluated through Cronbach's Alpha, composite reliability, average variance extracted, and discriminant validity tests, shows that the survey instruments are robust and suitable for hypothesis testing. The SEM results and bootstrap analysis further validate the structural relationships, confirming the significance of all 13 hypotheses (H1–H13). The study's findings resonate strongly in the current context of Vietnam's banking sector, which is undergoing rapid digitalization and heightened regulatory scrutiny. To thrive in this environment, banks must cultivate a risk-aware culture, enhance ERM maturity, improve communication, and smartly leverage technology. Only by combining these elements can banks achieve sustainable, resilient, and effective ORM, ensuring not only regulatory compliance but also long-term stability and trustworthiness.

2. POLICY RECOMMENDATIONS

The research results highlight the structural relationships between organizational factors (IE, SO, CA, IC, MA, DT) and the mediating variable, as well as operational risk management. The results show that the internal environment has the most decisive influence, while AOF acts as a critical mediator that channels the effects of other factors into ORM performance. Based on these findings, several policy recommendations are proposed for regulators, banking associations, and financial institutions. The authors provided policy recommendations based on the impact of factors, as shown in the standardized estimates below.

- The internal environment (IE) has the highest standardized estimate (IE → AOF = 0.568; IE → ORM = 0.337), making it the top priority for policy intervention. A strong internal environment encompasses leadership commitment, ethical values, and a risk-aware corporate culture that aligns with both regulatory expectations and organizational goals. A weak internal environment can lead to a fragmented risk management structure, a lack of accountability, and increased exposure to operational failures.
  Policy recommendation: Regulators, such as the State Bank of Vietnam (SBV), should establish policies that promote the development of a strong risk culture across all commercial banks. This can be done by mandating annual risk culture assessments and requiring boards of directors to actively oversee ORM practices. Furthermore, corporate governance codes should emphasize the integration of operational risk considerations into all layers of management decision-making. Policies could also require banks to publicly disclose risk culture indicators, such as employee training rates on risk management or the presence of whistleblowing mechanisms. Leadership development is another crucial area. Senior managers and risk officers should undergo periodic leadership training with a focus on ethical decision-making, operational risk awareness, and crisis management. This will ensure that ORM is not viewed as a compliance obligation but as a strategic function critical to the long-term stability of the bank. Regarding legal regulations, banks must regularly update their knowledge of changes in legal regulations and international standards, while ensuring the effective implementation of procedures related to debt classification, provisioning, and credit management. Strengthen coordination with the State Bank to establish effective internal control

mechanisms, thereby minimizing risks associated with sudden policy changes. Build a specialized internal legal department, ensuring the monitoring and enforcement of regulations.

- The influence of strategic objectives is moderate (SO → AOF = 0.091; SO → ORM = 0.103), but still significant. When operational risk management is aligned with strategic objectives, banks are better positioned to anticipate risks associated with new product development, market expansion, or regulatory changes. Conversely, a lack of alignment can lead to strategic blind spots and operational vulnerabilities.
  Policy recommendation: SBV should require risk-adjusted strategic planning for all commercial banks. For example, before approving major strategic initiatives, e.g., entering new markets or launching digital products, banks should conduct operational risk assessments and scenario analyses to ensure informed decision-making. Stress testing requirements should be extended to include operational risk factors such as IT system outages, fraud events, and human errors. Furthermore, risk-based performance management systems should be encouraged. By integrating risk-related key performance indicators into senior management's strategic scorecards, banks can ensure that executives remain accountable for both financial outcomes and operational resilience. This alignment ensures ORM is treated as a strategic enabler rather than a reactive or siloed function. Regarding banking management policies, we should focus on refining risk management policies to ensure specificity, flexibility, and suitability in response to market fluctuations. Establish a periodic risk assessment system and a rapid response mechanism to address unexpected risks. Regularly evaluate the effectiveness of policy implementation, thereby adjusting and refining it based on actual outcomes.
- Control Activities have standardized estimates of CA → AOF = 0.110 and CA → ORM = 0.090, indicating that internal controls are critical but function as supporting mechanisms rather than primary drivers. Controls include policies, procedures, and automated systems designed to prevent, detect, or mitigate errors, fraud, or operational failures.
  Policy recommendation: Banks should be required to regularly review and update internal control frameworks, ensuring they remain relevant to emerging risks, such as cyberattacks or technology disruptions. SBV could issue guidelines on automated control systems, encouraging the adoption of real-time monitoring tools that minimize manual intervention and human errors. Periodic independent control audits should be mandated, with a focus on high-risk areas such as payment processing, credit approval, and IT security. Additionally, policies should incentivize banks to invest in advanced control technologies, including artificial intelligence and robotic process automation, to detect anomalies and automate routine control functions. Regarding the customer's ability, the bank must conduct a detailed financial analysis and review the customer's credit history before approving the loan. Develop a rigorous customer information verification process, encompassing credit history, financial capacity, and the intended purpose of capital utilization. Establish clear criteria to classify customers based on risk level, thereby applying appropriate credit policies. Organize programs to advise and support customers in using loans for the right purposes, while raising customers' sense of responsibility in fulfilling financial obligations.
- Although IC's standardized estimates are lower (IC → AOF = 0.076; IC → ORM = 0.140), its low mean score (2.421) from Table 1 highlights it as a critical weakness across banks. Effective communication ensures that risk information is distributed accurately and promptly to all relevant stakeholders.
  Policy recommendation: SBV should mandate centralized reporting systems for operational risk events, requiring banks to submit data on incidents, losses, and near-misses to a national database. This would promote industry-wide learning and risk benchmarking. Internally, banks must enhance their real-time risk dashboards to integrate key risk indicators (KRIs) and provide early-warning alerts for management. Training programs focusing on risk communication skills for employees should be encouraged, ensuring that potential issues are escalated promptly. Banks need to regularly organize training programs to enhance the skills and expertise of their employees in risk analysis, credit management, and financial forecasting. Recruit and develop a team of experienced experts in the field of risk management to enhance organizational capacity. Build a culture of self-awareness and responsibility, particularly in implementing effective risk management processes. Participate in conferences and specialized forums to update on new trends in risk management. Learn, research, and apply successful risk management models from developed countries.

Strengthen cooperation with credit institutions and regulatory agencies to improve risk management capacity.

- Monitoring activities have MA → AOF = 0.149 and MA → ORM = 0.110, indicating that continuous oversight is an essential factor in sustaining ORM performance. Monitoring includes internal audits, compliance checks, and performance reviews.
  Policy recommendation: Regulators should encourage banks to implement continuous monitoring systems that use advanced analytics to detect operational anomalies. Additionally, periodic independent reviews of ORM by third-party experts should be required to assess the effectiveness of monitoring frameworks. The SBV could also recommend linking monitoring outcomes to employee performance evaluations, ensuring accountability for risk management at all organizational levels. Regarding the banking information technology system, it is necessary to focus on investing heavily in integrated risk management systems, using technologies such as artificial intelligence (AI) and big data analysis to improve the ability to detect abnormalities in financial activities. Develop measures to protect information technology systems, ensuring the safety and security of customer data and internal operations. Apply technology to automate the credit assessment and risk analysis process to increase accuracy and minimize errors.
- Digital transformation (DT) has the lowest standardized estimates (DT → AOF = 0.056; DT → ORM = 0.057). While DT is often viewed as a driver of efficiency and innovation, its direct contribution to ORM is limited unless aligned with ERM frameworks.
  Policy recommendation: Banks should prioritize integrating digital tools into their risk management processes, ensuring that investments in AI, big data, and automation directly support risk detection, prevention, and response. The SBV can establish cybersecurity standards and digital risk guidelines, requiring banks to conduct regular cyber risk audits and stress tests of their digital infrastructure. Moreover, cross-bank collaborations should be encouraged through shared cybersecurity intelligence platforms, enabling banks to collectively defend against systemic digital threats. In terms of the economic environment, banks need to develop macroeconomic analysis and forecasting models to identify early risks associated with interest rates, exchange rates, and inflation. Have a flexible business strategy that adapts to unusual changes in the economic environment. Promote international cooperation to leverage capital and expertise from foreign financial institutions, while also enhancing competitiveness in the global market.
- The mediating role of AOF (AOF → ORM = 0.317) shows that ERM awareness and operation translate other factors, e.g., IE, MA, DT into effective ORM outcomes.

Policy recommendation: Regulators should promote ERM maturity models with clear benchmarks and require banks to publicly report their ERM level annually. Banks should conduct regular ERM workshops and integrate ERM principles into their operational strategy and decision-making processes. Based on the standardized estimates from Table 2, policy actions should prioritize IE and AOF, followed by IC and MA, while ensuring that SO and CA are strategically aligned. DT should not be overlooked but must be strategically integrated with ERM and supported by a strong internal environment. Overall assessment of business objectives and environment: Clearly define the bank's business objectives and deeply analyze the business environment to understand the factors that may affect the bank's operations. Develop a strategy based on risk tolerance: Set risk tolerance thresholds in line with the bank's business strategy and financial situation, ensuring that all investment and lending decisions comply with the defined risk framework.

Moreover, the findings contribute to the literature by highlighting AOF as a central transmission channel, thereby reinforcing the importance of risk culture, communication, and ERM maturity in ensuring effective ORM. The authors give more policy and managerial recommendations as follows: (1) Board-Level oversight: Regulators should require banks to establish ORM Key Performance Indicators (KPIs) monitored at the board level. Independent risk committees must regularly review ORM metrics to ensure accountability and facilitate timely corrective actions. (2) ERM awareness modules for managers: Banks should design structured training programs on ERM awareness tailored for mid-level managers, who translate strategy into daily operations. Such modules should include practical case studies of operational failures and recovery processes. (3) Integration of ORM into strategic objectives: ORM considerations should be embedded into annual business plans, credit expansion targets, and digital transformation strategies. This ensures risk management is proactive rather than reactive. (4) Technology human alignment: Digital transformation

initiatives, such as fraud detection systems, cybersecurity platforms, or core banking upgrades, must be paired with AOF-enhancing activities, including awareness workshops and simulation drills. This ensures that staff fully utilize technology in mitigating risks. (5) Regulatory support and supervision: The State Bank of Vietnam should complement Basel III implementation with policies encouraging a risk culture. This may include mandating annual ERM training, requiring disclosure of ORM incidents, and incentivizing banks that demonstrate improvements in ORM performance. (6) Internal communication channels: Banks should establish confidential, multi-channel systems for reporting near misses and operational anomalies. Such mechanisms help ensure that risks are identified early and addressed systematically.

3. LIMITATIONS AND FURTHER RESEARCH

The study's findings underscore the importance of a strong internal environment, effective ERM awareness, and transparency of information in driving operational risk management. However, there is still much to learn about how these factors interact with emerging challenges such as cybersecurity threats, digitalization, and regulatory shifts. Future studies should adopt a multi-method approach, combining longitudinal data, objective performance metrics, and qualitative insights to provide a comprehensive picture of ORM evolution. The banking sector in Vietnam, like many emerging markets, is undergoing rapid changes due to digital transformation, global integration, and regulatory reforms. As such, ORM frameworks must evolve beyond traditional control-based approaches to embrace data-driven, technology-enabled, and culture-centric strategies. Future research should thus focus not only on refining ORM theory but also on developing actionable models that enable banks to anticipate, mitigate, and recover from operational disruptions in an increasingly volatile environment. Finally, there are sampling bias, self-report bias, and cross-sectional limitation. Therefore, further studies should pay attention to overcoming the above three weaknesses.

Funding Statement

The authors acknowledge that specific funding was provided by Ho Chi Minh University of Banking (HUB) and Lac Hong University (LHU), as well as support for this study.

Ethical Approval

Ethical approval based on Lac Hong University, Number 961/QĐ-ĐHLH and Ho Chi Minh University of Banking (HUB).

Author Contribution

The authors made contributions to the development and planning of the study. The authors divided the tasks equally; Phan Dien Vy wrote the conception, method, and design, and conducted the data analysis. Phan Thanh Tam wrote the critical revisions of the intellectual content and approved the final version.

Conflict of Interest

The authors declare that they have no conflicts of interest.

Data Availability Statement

Data is available from the authors upon request.

Acknowledgments

The authors would like to acknowledge the assistance of the Editor and reviewers in preparing the article for publication.

REFERENCES

1. Abdulla, H., & Elshandidy, T. (**2023**). Do governance factors affect the effectiveness of risk management disclosure in UAE banks? *Cogent Business & Management*, *10*(2), 1–28.

2. Elshandidy, T., Elmassri, M., & Elsayed, M. (**2022**). Integrated reporting, textual risk disclosure and market value. *Corporate Governance the International Journal of Business in Society*, *22*(1), 173–193.
3. Bitar, M., Naceur, S. B., Ayadi, R., & Walker, T. (**2020**). Basel compliance and financial stability: Evidence from Islamic banks. *Journal of Financial Services Research*, *60*(1), 1–54.
4. Elamer, A. A., Ntim, C. G., & Abdou, H. A. (**2020**). Islamic governance, national governance, and bank risk management and disclosure in MENA countries. *Business & Society*, *59*(5), 914–955.
5. Elamer, A., Ntim, C. G., Abdou, H., Zalata, A., & Elmagrhi, M. (**2019**). The impact of multi-layer governance on bank risk disclosure in emerging markets: The case of Middle East and North Africa. *Accounting Forum*, *43*(2), 246–281.
6. Grassa, R., Moumen, N., & Hussainey, K. (**2021**). What drives risk disclosure in Islamic and conventional banks? An international comparison. *International Journal of Finance & Economics*, *26*(4), 6338–6361.
7. Ökmen, Ö., Leijten, M., Stratton, T., Bosch-Rekveldt, M., & Bakker, H. (**2024**). Employee perspectives on risk management in a construction company. *Journal of Risk Research*, *27*(3), 404–422.
8. Widjanarko, W., Manurung, A. H., & Machdar, N. M. (**2025**). Operational risk management in digital banks: Challenges and solutions. *Dinasti International Journal of Economics, Finance & Amp; Accounting*, *6*(1), 315–324.
9. Cornwell, N., Bilson, C., Gepp, A., Stern, S., & Vanstone, B. J. (**2022**). The role of data analytics within operational risk management: A systematic review from the financial services and energy sectors. *Journal of the Operational Research Society*, *74*(1), 374–402.
10. Araz, O. M., Choi, T. M., Olson, D. L., & Salman, F. S. (**2020**). Role of analytics for operational risk management in the era of big data. *Decision Sciences*, *51*(6), 1320–1346.
11. Bouveret, A. (**2019**). Estimation of losses due to cyber risk for financial institutions. *Journal of Operational Risk*, *14*(2), 1–20.
12. Dong, M., Nassif, A. B., & Li, B. (**2019**). A data-driven residential transformer overloading risk assessment method. *IEEE Transactions on Power Delivery*, *34*(1), 387–396.
13. Embrechts, P., Mizgier, K. J., & Chen, X. (**2018**). Modeling operational risk depending on covariates: An empirical investigation. *Journal of Operational Risk*, *13*(3), 17–46.
14. Groth, K. M., Denman, M. R., Darling, M. C., Jones, T. B., & Luger, G. F. (**2020**). Building and using dynamic risk-informed diagnosis procedures for complex system accidents. Proceedings of the Institution of Mechanical Engineers. *Journal of Risk and Reliability*, *234*(1), 193–207.
15. Lacković, I. D., Kovšca, V., & Vincek, Z. L. (**2020**). A review of selected aspects of big data usage in banks' risk management. *Journal of Information and Organizational Sciences*, *44*(2), 317–330.
16. Virglerova, Z., Panic, M., Voza, D., & Velickovic, M. (**2021**). Model of business risks and their impact on operational performance of SMEs. *Economic Research-Ekonomska Istraživanja*, *35*(1), 4047–4064.
17. Ferreira, S., & Dickason-Koekemoer, Z. (**2019**). A conceptual model of operational risk events in the banking sector. *Cogent Economics & Finance*, *7*(1), 1–18.
18. Hamed, R. (**2023**). The role of internal control systems in ensuring financial performance sustainability. *Sustainability*, *15*(13), 1–18.
19. Ellis, K. A. S., & Gené, J. M. (**2015**). Effect of internal controls on credit risk among listed Spanish banks. *Intangible Capital*, *13*(1), 25–50.
20. Horvey, S. S. (**2025**). Insurers risk-taking behaviour in an emerging economy: unpacking the linear and nonlinear effects of enterprise risk management and corporate governance. *Cogent Business & Management*, *12*(1), 1–23.
21. Stulz, R. M. (**2015**). Risk-taking and risk management by banks. *Journal of Applied Corporate Finance*, *27*(1), 8–18.
22. Silva, J. R., Silva, A. F. D., & Chan, B. L. (**2019**). Enterprise risk management and firm value: Evidence from Brazil. *Emerging Markets Finance and Trade*, *55*(3), 687–703.
23. Nocco, B. W., & Stulz, R. M. (**2022**). Enterprise risk management: Theory and practice. *Journal of Applied Corporate Finance*, *34*(1), 81–94.
24. Lundqvist, S. A., & Vilhelmsson, A. (**2018**). Enterprise risk management and default risk: Evidence from the banking industry. *Journal of Risk and Insurance*, *85*(1), 127–157.
25. Kalia, A., & Gill, S. (**2023**). Corporate governance and risk management: A systematic review and synthesis for future research. *Journal of Advances in Management Research*, *20*(3), 409–461.
26. Hunjra, A. I., Hanif, M., Mehmood, R., & Nguyen, L. V. (**2021**). Diversification, corporate governance, regulation and bank risk-taking. *Journal of Financial Reporting and Accounting*, *19*(1), 92–108.
27. Horvey, S. S., & Odei-Mensah, J. (**2023**). The measurements and performance of enterprise risk management: A comprehensive literature review. *Journal of Risk Research*, *26*(7), 778–800.

28. Abdullah, R., Ismail, Z., & Smith, M. (**2018**). Audit committees' involvement and the effects of quality in the internal audit function on corporate governance. *International Journal of Auditing*, *22*(3), 385–403.
29. Al-Dmour, A., Al-Dmour, R., & Rababeh, N. (**2021**). The impact of knowledge management practice on digital financial innovation: The role of bank managers. *VINE Journal of Information and Knowledge Management Systems*, *51*(3), 492–514.
30. Barr-Pulliam, D., Eulerich, M., & Ratzinger-Sakel, N. (**2024**). The effect of the internal audit function's perceived assurance versus advisory purpose on the external auditor's reliance decision. *Managerial Auditing Journal*, *39*(2), 138–165.
31. 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.
32. Elshandidy, T., Shrives, P. J., Bamber, M., & Abraham, S. (**2018**). Risk reporting: A review of the literature and implications for future research. *Journal of Accounting Literature*, *40*(1), 54–82.
33. Tarjo, T., Vidyantha, H. V., Anggono, A., Yuliana, R., & Musyarofah, S. (**2022**). The effect of enterprise risk management on prevention and detection fraud in Indonesia's local government. *Cogent Economics & Finance*, *10*(1), 1–19.
34. Cohen, J., Krishnamoorthy, G., & Wright, A. (**2016**). Enterprise risk management and the financial reporting process: the experiences of audit committee members, CFOs, and external auditors. *Contemporary Accounting Research*, *34*(2), 1178–1209.
35. Mcshane, M. (**2018**). Enterprise risk management: History and a design science proposal. *The Journal of Risk Finance*, *19*(2), 137–153
36. Saeidi, P., Saeidi, S. P., Gutierrez, L., Streimikiene, D., Alrasheedi, M., Saeidi, S. P., & Mardani, A. (**2020**). The influence of enterprise risk management on firm performance with the moderating effect of intellectual capital dimensions. *Economic Research-Ekonomska Istraživanja*, *34*(1), 122–151.
37. Farrell, M., & Gallagher, R. (**2015**). The valuation implications of enterprise risk management maturity. *Journal of Risk and Insurance*, *82*(3), 625–657.
38. García, V., Marqués, A. I., & Sánchez, J. S. (**2015**). An insight into the experimental design for credit risk and corporate bankruptcy prediction systems. *Journal of Intelligent Information Systems*, *44*(1), 159–189.
39. Siswanti, I., Riyadh, H. A., Nawangsari, L. C., Mohd Yusoff, Y., & Wibowo, M. W. (**2024**). The impact of digital transformation for sustainable business: the meditating role of corporate governance and financial performance. *Cogent Business & Management*, *11*(1), 1–16.
40. Jardak, M. K., & Ben Hamad, S. (**2022**). The effect of digital transformation on firm performance: Evidence from Swedish listed companies. *The Journal of Risk Finance*, *23*(4), 329–348.
41. Ahmed, S., Abd, A. N., Haque, R., Bin, S., Senathirajah, A. R., & Qazi, S. Z. (**2024**). Digital transformation in Malaysian manufacturing: a study of change sensing and seizing capabilities. *Cogent Business & Management*, *11*(1), 1–28.
42. Giovannoni, E., Quarchioni, S., & Riccaboni, A. (**2016**). The role of roles in risk management change: The case of an Italian bank. *European Accounting Review*, *25*(1), 109–129.
43. Oyewo, B. (**2022**). Enterprise risk management and sustainability of banks performance. *Journal of Accounting in Emerging Economies*, *12*(2), 318–344.
44. Gao, S., Hsu, H. T., & Liu, F. C. (**2025**). Enterprise risk management, financial reporting and firm operations. *Risks*, *13*(3), 1–28.
45. Hair, J., Anderson, R., Tatham, R., & Black, W. (**2018**). *Multivariate data analysis*. Prentice-Hall.
46. Akter, S., Michael, K., Uddin, M. R., McCarthy, G., & Rahman, M. (**2022**). Transforming business using digital innovations: The application of AI, blockchain, cloud and data analytics. *Annals of Operations Research*, *308*(2), 7–39.
47. Bojesson, C., & Fundin, A. (**2021**). Exploring microfoundations of dynamic capabilities – Challenges, barriers and enablers of organizational change. *Journal of Organizational Change Management*, *34*(1), 206–222.
48. Dixit, S., Singh, S., Dhir, S., & Dhir, S. (**2021**). Antecedents of strategic thinking and its impact on competitive advantage. *Journal of Indian Business Research*, *13*(4), 437–458.
49. Serkbayeva, Z., Zhumabayeva, M., Kassenova, G., Karimbayeva, G., Faizulayev, A., & Kulumbetova, D. (**2024**). Examining the impact of fintech and other factors on banking practices: QISMUT + 3 countries. *Cogent Business & Management*, *11*(1), 1–24.
50. Rakshit, B., & Bardhan, S. (**2019**). Bank competition and its determinants: Evidence from Indian banking. *International Journal of the Economics of Business*, *26*(2), 283–313.
51. Parmankulova, I., Issakhova, P., Zhanabayeva, Z., Faizulayev, A., & Orazymbetova, K. (**2022**). The drivers of financial vulnerability and profitability: Evidence from conventional and Islamic banks in Islamic finance-oriented countries. *Journal of Islamic Accounting and Business Research*, *13*(6), 902–919.
52. Meskovic, A., Kozarevic, E., & Avdukic, A. (**2024**). The influence of national and individual Islamic governance on Islamic banks' social performance. *Journal of Islamic Accounting and Business Research*, *15*(6), 911–941.

53. Kanapiyanova, K., Faizulayev, A., Ruzanov, R., Ejdys, J., Kulumbetova, D., & Elbadri, M. (**2022**). Does social and governmental responsibility matter for financial stability and bank profitability? Evidence from commercial and Islamic banks. *Journal of Islamic Accounting and Business Research*, *14*(3), 451–472.
54. Ally, O. J., Kulindwa, Y. J., & Mataba, L. (**2025**). Financial technology and credit risk management: the case of non-performing loans in Tanzanian banks. *Cogent Economics & Finance*, *13*(1), 1–19.
55. Wang, R., Liu, J., & Luo, H. R. (**2021**). Fintech development and bank risk taking in China. *The European Journal of Finance*, *27*(4-5), 397–418.
56. Zhang, A., Wang, S., Liu, B., & Liu, P. (**2022**). How fintech impacts pre-and post-loan risk in Chinese commercial banks. *International Journal of Finance & Economics*, *27*(2), 2514–2529.

Appendix

Table A1. Research questionnaires - Measurement Items

Items	Contents of items	Construct	Source(s)
IE1	The Board of Directors is strongly committed to building a risk management culture	Internal environment (IE)	[4, 14, 16]
IE2	The Bank has a clear policy regarding operational risk		
IE3	Internal processes are designed to control risks		
IE4	The organizational structure effectively supports operational risk management		
SO1	The bank's strategic objectives incorporate risk	Strategic objectives (SO)	[6, 12, 21]
SO2	Risk objectives are clearly communicated throughout the system		
SO3	Business decisions take into account the impact of operational risk		
SO4	The bank defines a clear risk tolerance for each activity		
CA1	The Bank has a clear and effective internal control system	Control activities (CA)	[5, 17, 26]
CA2	The control process is updated periodically to suit the reality		
CA3	Risk violations are detected and handled promptly		
CA4	Employees are trained to comply with the control process		
IC1	Risk information is collected and analyzed in a timely manner	Information and communication (IC)	[6, 32, 33]
IC2	The information system serves well for operational risk management		
IC3	The bank has an effective internal risk communication channel		
IC4	Employees are fully informed about risk events that arise		
MA1	The Bank has an independent and objective risk monitoring system	Monitoring activities (MA)	[9, 38, 39]
MA2	The results of risk monitoring are used to adjust control policies		
MA3	The internal audit/control board conducts periodic monitoring		
MA4	The findings from monitoring are handled promptly and thoroughly		
DT1	The bank has deployed digital technology in operational risk management	Digital transformation (DT)	[25, 40, 41]
DT2	Digital applications help reduce operational errors and enhance risk control		
DT3	Digital transformation is integrated into core business processes		
AOF1	Bank staff have a clear understanding of the ERM framework and its role	Awareness and level of operation of ERM (AOF)	[10, 11, 19]
AOF2	ERM is consistently implemented across functional departments		
AOF3	ERM is integrated into the risk assessment and decision-making process		
ORM1	The bank significantly reduces losses from operational risks	Operational risk management (ORM)	[5, 6, 21]
ORM2	QTRRHĐ helps improve the bank's operational performance		
ORM2	The ability to respond to risk events is significantly improved		

Table A2. Research questionnaires.

Code	Factors affecting operational risk management	5-point Likert scale				
		(1)	(2)	(3)	(4)	(5)
IE1	The Board of Directors is strongly committed to building a risk management culture	(1)	(2)	(3)	(4)	(5)
IE2	The Bank has a clear policy regarding operational risk	(1)	(2)	(3)	(4)	(5)
IE3	Internal processes are designed to control risks	(1)	(2)	(3)	(4)	(5)
IE4	The organizational structure effectively supports operational risk management	(1)	(2)	(3)	(4)	(5)
SO1	The bank's strategic objectives incorporate risk	(1)	(2)	(3)	(4)	(5)
SO2	Risk objectives are clearly communicated throughout the system	(1)	(2)	(3)	(4)	(5)
SO3	Business decisions take into account the impact of operational risk	(1)	(2)	(3)	(4)	(5)
SO4	The bank defines a clear risk tolerance for each activity	(1)	(2)	(3)	(4)	(5)
CA1	The Bank has a clear and effective internal control system	(1)	(2)	(3)	(4)	(5)
CA2	The control process is updated periodically to suit the reality	(1)	(2)	(3)	(4)	(5)
CA3	Risk violations are detected and handled promptly	(1)	(2)	(3)	(4)	(5)
CA4	Employees are trained to comply with the control process	(1)	(2)	(3)	(4)	(5)
IC1	Risk information is collected and analyzed in a timely manner	(1)	(2)	(3)	(4)	(5)
IC2	The information system serves well for operational risk management	(1)	(2)	(3)	(4)	(5)
IC3	The bank has an effective internal risk communication channel	(1)	(2)	(3)	(4)	(5)
IC4	Employees are fully informed about risk events that arise	(1)	(2)	(3)	(4)	(5)
MA1	The Bank has an independent and objective risk monitoring system	(1)	(2)	(3)	(4)	(5)
MA2	The results of risk monitoring are used to adjust control policies	(1)	(2)	(3)	(4)	(5)
MA3	The internal audit/control board conducts periodic monitoring	(1)	(2)	(3)	(4)	(5)
MA4	The findings from monitoring are handled promptly and thoroughly	(1)	(2)	(3)	(4)	(5)
DT1	The bank has deployed digital technology in operational risk management	(1)	(2)	(3)	(4)	(5)
DT2	Digital applications help reduce operational errors and enhance risk control	(1)	(2)	(3)	(4)	(5)
DT3	Digital transformation is integrated into core business processes	(1)	(2)	(3)	(4)	(5)
AOF1	Bank staff have a clear understanding of the ERM framework and its role	(1)	(2)	(3)	(4)	(5)
AOF2	ERM is consistently implemented across functional departments	(1)	(2)	(3)	(4)	(5)
AOF3	ERM is integrated into the risk assessment and decision-making process	(1)	(2)	(3)	(4)	(5)
ORM1	The bank significantly reduces losses from operational risks	(1)	(2)	(3)	(4)	(5)
ORM2	QTRRHĐ helps improve the bank's operational performance	(1)	(2)	(3)	(4)	(5)
ORM3	The ability to respond to risk events is significantly improved	(1)	(2)	(3)	(4)	(5)

Note: A 5-point Likert scale states the level of agreement in five points. The 5-point Likert scale consists of the below points – (1) Strongly Disagree; (2) Disagree; (3) Neither Agree nor Disagree; (4) Agree; (5) Strongly Agree.

Table A3. Research results for model type based on CFA (Measurement Model) and SEM (Structural Model).

Model Type	χ^2/df	GFI	TLI	CFI	RMSEA	SRMR	Interpretation
CFA (Measurement Model)	3.912	0.912	0.931	0.943	0.062	0.047	Acceptable fit
SEM (Structural Model)	4.338	0.91	0.938	0.949	0.059	–	Good fit

Table A4. Research results for diagnostic test normality, multicollinearity and common method bias.

Diagnostic Test	Method	Criterion	Result	Conclusion
Normality	Skewness and Kurtosis		Skewness, Kurtosis ∈ ±2.0	Normal distribution confirmed
Multicollinearity	VIF and Tolerance	VIF < 5.0; Tolerance > 0.30	VIF < 3.0	No multicollinearity
Common Method Bias	Harman's One-Factor Test	Variance < 50%	32.40%	No CMB issue

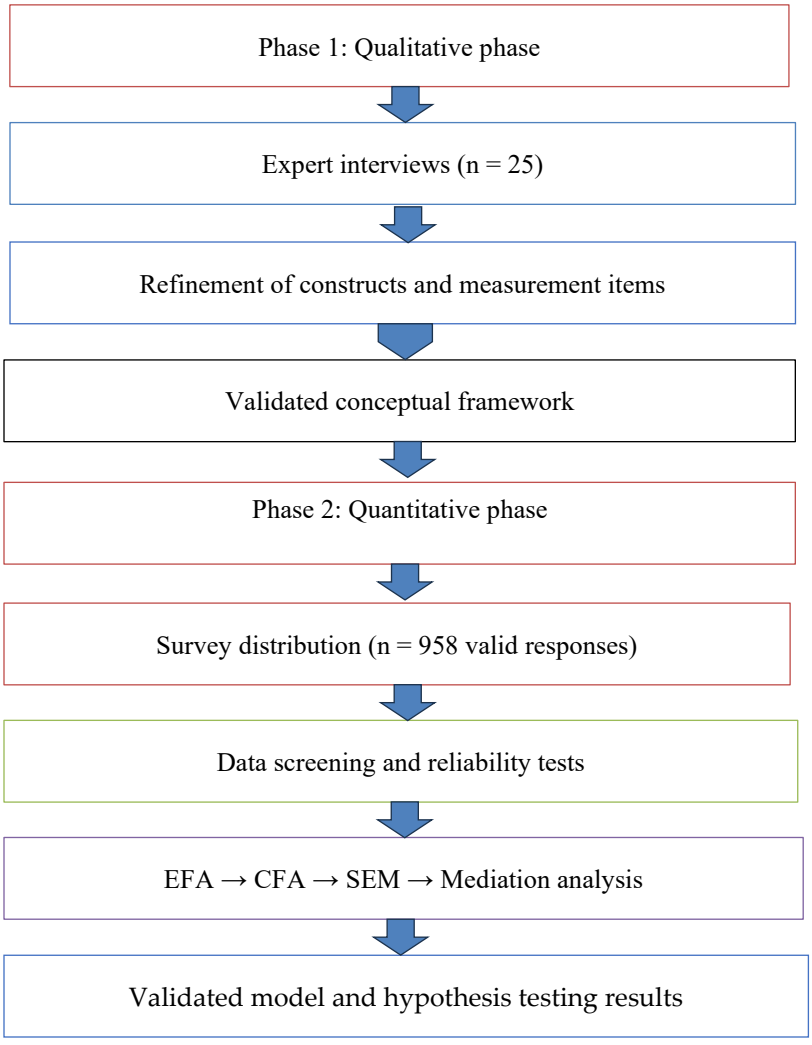


FIGURE A1. A research process for critical factors affecting operational risk management.