© MAR 2026 | IRE Journals | Volume 9 Issue 9 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I9-1720341

Enterprise Risk Management in U.S. Financial Institutions: Building Resilience in an Increasingly Complex Risk Environment

ABDOULIE K DARBOE
School: Illinois Institute of Technology

Abstract- ***The U.S. financial sector currently faces a wide range of unprecedented risks, including credit, market, liquidity, cybersecurity, and algorithmic decision-making challenges, all worsened by an expanding regulatory environment. The 2008 crisis and ensuing reforms have elevated standards for risk management. Nonetheless, many institutions still struggle to develop comprehensive Enterprise Risk Management (ERM) systems that operate smoothly across departments, leverage technology effectively, and withstand multiple shocks (Lawati et al., 2025). This paper examines the current ERM landscape among U.S. financial institutions, highlights gaps in existing frameworks, and proposes an integrated model to boost resilience, compliance, and stakeholder value simultaneously rather than separately. This qualitative, applied approach systematically reviews academic literature, regulatory documents, and industry reports, primarily from peer-reviewed sources from 2015 to 2025. It also includes materials from federal banking agencies and industry bodies. A clear pattern emerges: institutions with more advanced ERM implementation tend to perform better financially and adapt more effectively to disruptions (Gao, Hsu, and Liu, 2025). Nonetheless, this maturity level varies widely; smaller banks often struggle to adopt the technology and analytics that larger institutions readily implement. Cybersecurity has become the fastest-evolving risk category, surpassing others. The swift adoption of artificial intelligence and machine learning boosts capabilities but also introduces new risks not seen a decade ago (Ma, 2025). Overall, the evidence points to key priorities: develop an integrated ERM framework with a focus on risk governance, utilize predictive analytics, enhance cybersecurity, invest in employee training, and view regulatory engagement as an ongoing relationship rather than a mere checklist. Success hinges on genuine board ownership and embedding a risk culture into daily operations, beyond policy documents.***

Keywords: ***Enterprise Risk Management, Banking, Compliance, Operational Risk, Governance, Risk Appetite, Risk Culture, Technology Integration, Regulatory Compliance, Financial Stability***

I. INTRODUCTION

The US financial services sector is one of the most vital worldwide, comprising banks, investment firms, insurers, and other financial intermediaries that handle trillions in assets. The complexity and interconnected nature of modern financial operations have heightened the importance of advanced risk management (Sang, 2024). Today, institutions face risks beyond traditional banking, including cyber threats, climate-related challenges, and ongoing technological innovation.

The 2008 global financial crisis marked a pivotal point for risk management in financial services, revealing major flaws in how institutions identified, evaluated, and handled systemic risks. It led to widespread regulatory changes, including the Dodd-Frank Act, stricter capital requirements under Basel III, and improved supervisory structures. These reforms collectively transformed risk management expectations by encouraging firms to move away from isolated, fragmented approaches toward integrated systems that offer a comprehensive view of organizational risk exposure (Nkansa, Barr-Pulliam, and Walker, 2025).

Despite investing in risk infrastructure and facing increased regulatory scrutiny, U.S. financial institutions still encounter significant challenges in achieving fully integrated ERM. In addition to traditional credit and market risks, modern banks must address operational complexities, cybersecurity threats, digital transformation, regulatory changes, and stakeholder demands for strong governance and

the integration of sustainability. Larger institutions have made greater progress, while smaller and medium-sized ones often lack the necessary resources, expertise, and technology to implement comprehensive risk management (Stasse, Hilhorst, and Rouwelaar, 2025). Rapid technological advances, including digital banking, fintech disruptions, and sophisticated cyber threats, have created new risks that legacy frameworks cannot effectively address. Furthermore, a persistent gap exists between board-level governance and frontline risk practices: strategic policies are not always implemented operationally (Sringam & Wuttidittachotti, 2026). The shortage of skilled risk professionals and the difficulty in integrating advanced analytics into existing frameworks further hinder effective risk management.

This study explores the current landscape of enterprise risk management within U.S. financial institutions. It highlights key success factors and implementation challenges, while proposing a practical ERM framework aligned with today's risk environment. The research aims to connect theoretical risk management ideas with real-world practices by integrating academic insights, regulatory advice, and industry experience. Specifically, it intends to analyze the types of risks faced by these institutions and their interrelationships, evaluate the relevance of existing frameworks such as COSO, Basel, and ISO 31000 to modern issues, examine how technology including AI and machine learning can enhance risk management, investigate how ERM implementation influences organizational performance, create a customized ERM framework for U.S. financial firms, and offer practical recommendations to improve risk governance and resilience.

These objectives lead to six key research questions: what are the essential elements of effective ERM in U.S. financial institutions; how do technological advancements influence risk identification, assessment, and mitigation; what challenges do institutions encounter when implementing comprehensive ERM systems; how does ERM adoption impact organizational performance and resilience; what governance structures and cultural factors promote effective risk management; and how should ERM frameworks adapt to emerging risks like cybersecurity and climate change?

This research advances both academic understanding and practical application. It reviews current literature on banking risk management, highlights gaps, and sets the stage for future studies on ERM effectiveness (Sang, 2024). In practice, the framework guides institutions in enhancing their risk management practices, while regulators and policymakers can better understand the factors that influence effective risk governance. Since U.S. financial institutions are crucial to economic stability, improving enterprise risk management has broader implications for financial-system resilience, consumer protection, and economic growth, helping institutions decrease fraud, reduce operational disruptions, ensure regulatory compliance, and boost public confidence in the financial system.

This study examines ERM practices among U.S.-based financial institutions, including commercial banks, savings institutions, and bank holding companies, covering 2015 to 2025. It tracks developments from major post-crisis regulatory reforms to emerging challenges today. While drawing on international research and frameworks, its recommendations are specifically tailored to the U.S. regulatory and competitive landscape. The main limitations stem from its qualitative, literature-based approach: reliance on publicly available sources might not fully reflect proprietary risk management practices. Although this approach is suitable for analyzing complex organizational phenomena, it limits the broader applicability of its findings. Given the fast-changing nature of cybersecurity and technology risks, some insights will need ongoing updates as the risk environment evolves.

II. LITERATURE REVIEW

Enterprise Risk Management marks a shift from isolated, department-specific risk handling to a comprehensive, organization-wide approach. It is best characterized as an ongoing, integrated process for managing both conventional and strategic risks to support business goals (Stasse, Hilhorst, and

Rouwelaar, 2025). Previously, financial institutions handled risk through separate, specialized functions: credit officers managed lending, treasury managed market exposure, operations focused on operational risks, and compliance focused on regulatory issues. This siloed approach, practiced for many years, created gaps and limited understanding of how different risk categories interconnect. Unlike isolated risk functions, ERM offers a framework for understanding risk interactions, collectively identifying threats and opportunities, and aligning risk management with strategic objectives.

Research shows that ERM has grown beyond merely ensuring compliance to become a key strategic asset that boosts competitive edge and organizational success (Lawati et al., 2025). Studies across various industries link ERM adoption with better financial results, less operational volatility, and higher-quality reports (Gao, Hsu, and Liu, 2025). Modern frameworks, especially the COSO Enterprise Risk Management Integrated Framework and ISO 31000, offer structured approaches for identifying, assessing, managing, and monitoring risks across organizations. They increasingly view risk management as intertwined with strategy, culture, governance, and performance metrics. Growing environmental, social, and governance pressures drive this expanded scope. Companies that incorporate risk assessment into their sustainability efforts tend to be more resilient and achieve better outcomes, with transparent risk identification and reporting fostering long-term success (Anton, Baba, and Bucșoiu, 2025).

Major categories of banking risk include credit risk, which remains the most critical for traditional banking. It refers to the potential for loss due to borrower default or a decline in credit quality. Research shows that credit risk adversely affects financial stability, underscoring the need for robust credit risk management (Ismail & Ahmed, 2023). Managing credit risk requires advanced evaluation of borrowers' creditworthiness, portfolio diversification, collateral requirements, and continuous monitoring. Recent advancements in machine learning significantly enhance this process: studies comparing deep learning techniques with traditional econometric models for estimating default probabilities reveal that neural network approaches achieve better calibration and can cut portfolio losses by about 12-13 percent (Ch et al., 2026), enabling earlier detection of potential defaults.

Operational risk involves the potential for losses arising from internal failures, such as flawed processes, employee errors, or system issues, as well as external shocks. Its importance has grown as institutions rely more on complex, interconnected technology. While they do not always directly threaten macrofinancial stability, individual failures can cause serious problems for specific institutions and indirectly affect overall market stability (Ismail & Ahmed, 2023). This risk encompasses fraud, process failures, system outages, compliance violations, reputational harm, and business disruptions. A study of Kenyan commercial banks showed a significant positive link between operational risk management practices and financial performance ($p = 0.05$). Although this has limited direct relevance to the U.S. market, it supports broader research (Kagima & Munene, 2025). Managing operational risk effectively requires comprehensive controls, strong business continuity plans, and quick incident response. Evidence indicates that good governance, including internal controls and audit oversight, can significantly reduce financial risks and promote overall stability (Surana, 2025).

Liquidity risk, the threat that an institution cannot fulfill its obligations or liquidate assets without substantial losses, does not always immediately threaten financial stability. However, it remains a crucial part of overall risk management (Ismail & Ahmed, 2023). The 2008 crisis demonstrated how rapidly liquidity problems can turn into solvency issues, leading Basel III to introduce stricter liquidity standards for systemically important institutions. Effective liquidity risk management includes maintaining enough liquid assets, diversifying funding sources, conducting stress tests on liquidity positions, and preparing contingency plans. Basel III codifies this with two key measures: the Liquidity Coverage Ratio (LCR), which requires institutions to hold sufficient high-quality liquid assets to cover net cash outflows over a 30-day stress period, and the

© MAR 2026 | IRE Journals | Volume 9 Issue 9 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I9-1720341

Net Stable Funding Ratio (NSFR), which requires a stable funding structure over a one-year horizon.

Cybersecurity risks are among the fastest-growing challenges for financial institutions, with threats becoming more complex and frequent. The sector faces a broad spectrum of dangers, from phishing and malware to advanced persistent threats and insider breaches (Shahzadi et al., 2025). The sensitivity of financial data amplifies these risks, along with the critical need for system availability and the risk of contagion across interconnected networks. Institutions deal with both simulated, training-focused threats and real attacks, including DDoS, ransomware, and sophisticated social engineering (Shahzadi et al., 2025). Effective defense requires multiple layers of security, combining technology, staff training, compliance, and incident response. While AI enhances threat detection, it also raises new concerns about algorithm stability and adversarial attacks (Shahzadi et al., 2025).

Compliance and regulatory risk refers to the risk of legal action, financial loss, or reputational damage resulting from non-compliance with laws, regulations, or internal policies. This risk has grown significantly in the post-crisis regulatory landscape, posing challenges due to increased regulatory complexity, enforcement uncertainties, and resource demands (Shahzadi et al., 2025). Regulatory Technology (RegTech) has become vital, as research shows that RegTech solutions enhance compliance oversight and risk management. They also help regulators increase supervisory agility, transparency, and real-time monitoring (Bagherifam et al., 2025). However, issues such as cybersecurity threats, a lack of algorithmic transparency, and fragmented regulations still limit the full automation of compliance processes.

Market risk potential loss arising from changes in interest rates, foreign exchange rates, equity prices, or commodity prices requires sophisticated measurement, including Value-at-Risk models, stress testing, and scenario analysis, given the complexity of modern trading portfolios and derivative exposures. Evidence on market valuation is mixed: some studies find a negative association between derivative-asset accumulation and market value, potentially reflecting suboptimal hedging or earnings volatility (Miloș & Miloș, 2022). Machine learning has improved market-risk modeling by capturing non-linear dynamics that traditional models miss; research on predictive modeling of market volatility reports meaningful gains in accuracy, providing more actionable input for dynamic risk management during periods of turbulence (Wang & Wu, 2025).

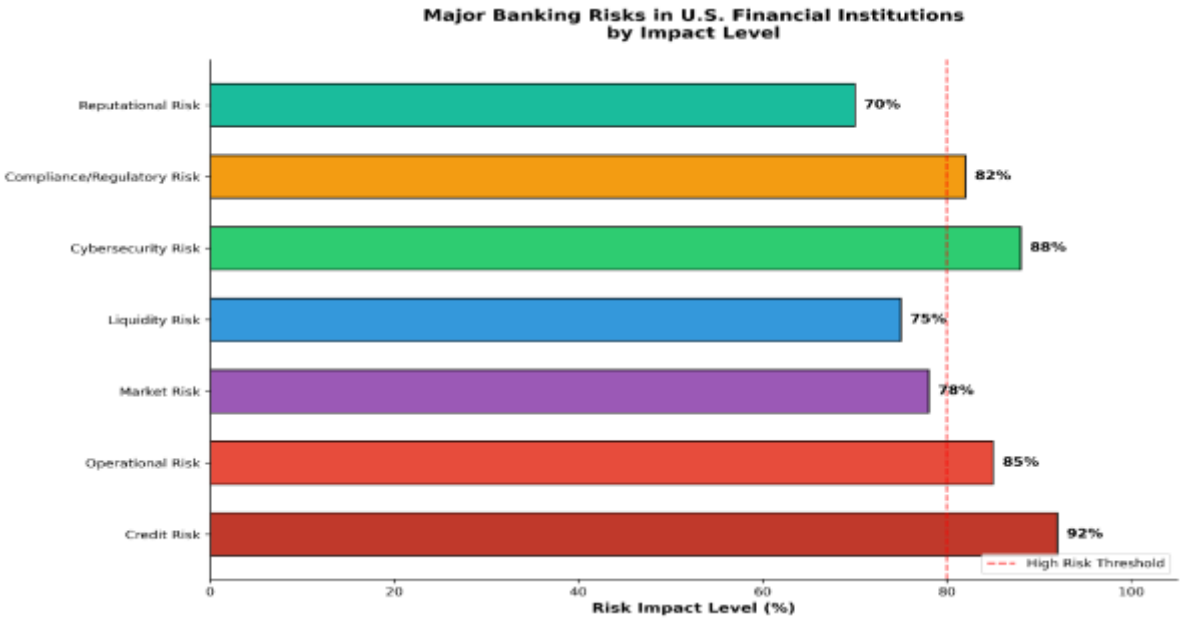

Figure 1. Perceived impact level of major banking risk categories in U.S. financial institutions, synthesized from the reviewed literature. Percentages are illustrative severity ratings drawn from qualitative synthesis rather than a single empirical source, and should be read as indicative rather than as a precise measurement.

Established ERM frameworks, with the COSO Enterprise Risk Management framework being the most recognized standard, focus on enterprise risk governance, identification, assessment, response, and monitoring. Factor analysis supports its continued relevance, revealing a strong two-factor structure that covers core and strategic ERM aspects and aligns with the 2017 COSO ERM framework (Stasse, Hilhorst, and Rouwelaar, 2025). The framework includes five interconnected components: Governance & Culture, Strategy & Objective-Setting, Performance, Review & Revision, and Information, Communication & Reporting, supported by twenty operational principles. It distinguishes ERM from traditional internal controls by incorporating risk appetite, risk tolerance, and strategic alignment to create, preserve, and maximize organizational value (COSO, 2020). Additionally, it has played a key role in shaping the internal audit function within ERM: based on COSO, research indicates that internal auditors' expertise aids in risk identification and assessment, although management is ultimately responsible for risk management and controls (Nkansa, Barr-Pulliam, and Walker, 2025). Successful compliance and ethics programs built on this foundation require clear governance principles such as board risk oversight, well-defined operational frameworks, a clearly articulated culture, and adherence to core values, along with a structured process for identifying compliance risks, evaluating their severity, prioritizing, and responding appropriately. Continuous improvement is vital for effectiveness, and regulators increasingly acknowledge genuine efforts to improve by reducing penalties and settlements. The most effective programs combine objective measurement of compliance metrics, risk assessment that considers both likelihood and impact, stakeholder-specific communication strategies, and technology that enables rapid detection and response to emerging issues.

Component	Principles	Key Focus Areas
Governance & Culture	5	Board oversight; operating structures; desired culture; core values; talent acquisition
Strategy & Objective-Setting	3	Business context; risk appetite; strategy evaluation; business objectives
Performance	5	Risk identification; severity assessment; risk prioritization; response design; portfolio view
Review & Revision	3	Substantial change assessment; risk & performance review; program improvement
Information, Communication & Reporting	4	Data & technology; risk communication; risk reporting

Table 1. The five components of the COSO ERM framework and their twenty supporting principles. Source: COSO ERM Framework (COSO, 2020).

© MAR 2026 | IRE Journals | Volume 9 Issue 9 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I9-1720341

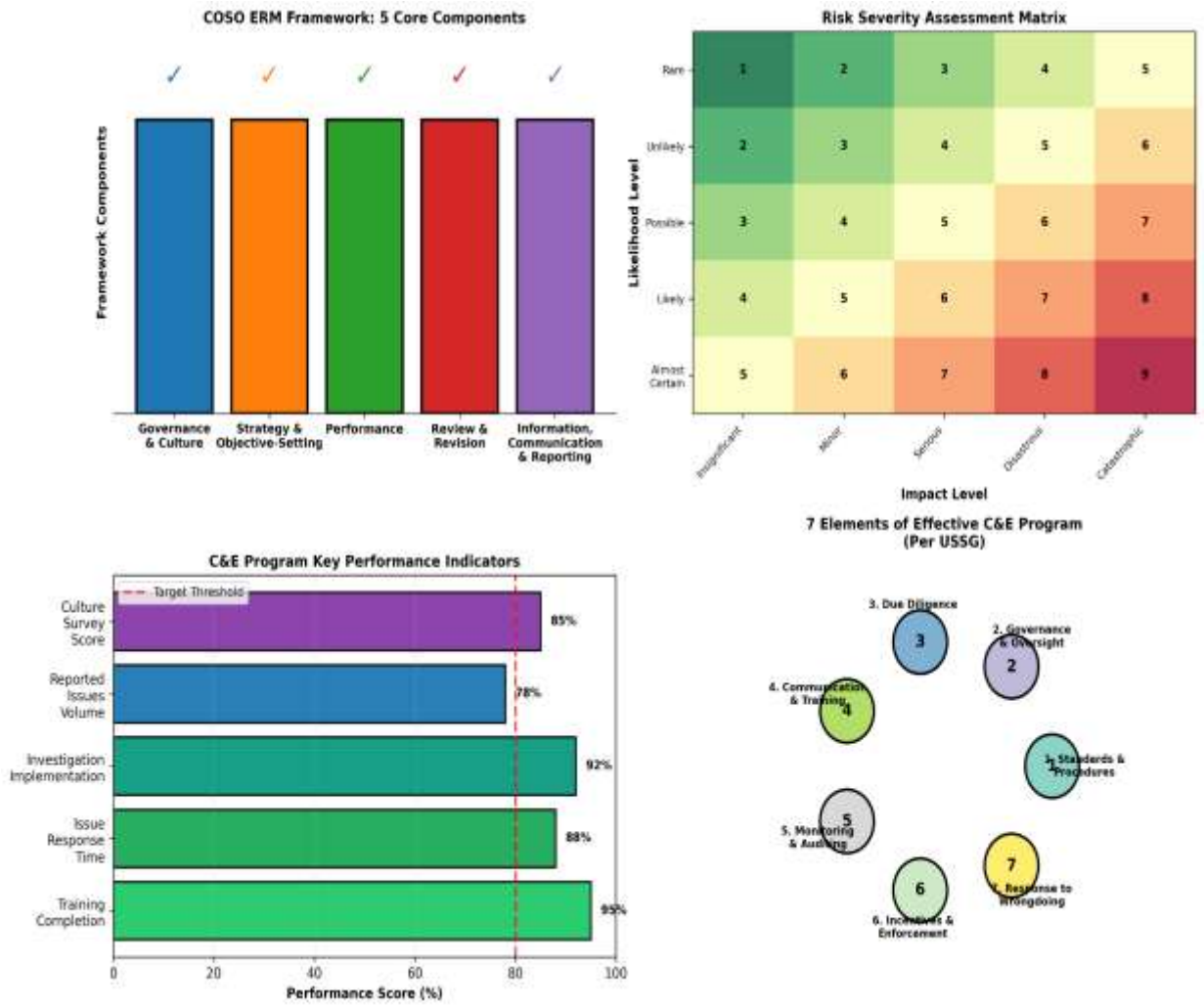

Figure 2. The five components of the COSO ERM framework, a risk severity (likelihood × impact) assessment matrix, the seven elements of an effective compliance and ethics program under the U.S. Federal Sentencing Guidelines, and representative categories of key performance indicators for compliance programs. Sources: COSO ERM Framework; U.S. Federal Sentencing Guidelines (COSO, 2020).

#	Element	Key Components	Primary Responsibility
1	Standards & Procedures	Code of conduct; policies; ethics standards	Compliance & management
2	Governance & Oversight	Board oversight; compliance function authority; operating structure	Board & senior leadership
3	Due Diligence in Delegation	Background checks; third-party vetting; ongoing monitoring	HR & management
4	Communication & Training	Code training; role-specific training; leadership communication	Compliance & management

© MAR 2026 | IRE Journals | Volume 9 Issue 9 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I9-1720341

#	Element	Key Components	Primary Responsibility
5	Monitoring, Auditing & Reporting	Risk-based auditing; data analytics; regular assessments	Compliance & internal audit
6	Incentives & Enforcement	Performance metrics; discipline consistency; financial incentives	Management & HR
7	Response to Wrongdoing	Investigation procedures; remediation; documentation	Compliance & legal

Table 2. The seven elements of an effective compliance and ethics program under the U.S. Federal Sentencing Guidelines (USSG), with typical organizational ownership.

Figure 3. The compliance risk assessment lifecycle, the Three Lines Model, a typical allocation of compliance and ethics program investment across activity categories, and comparative effectiveness ratings for common risk-response mechanisms. Sources: COSO Risk Assessment Process; Three Lines Model.

Step	Description	Key Consideration
1. Identify compliance risks	Identify risks inherent to organizational activities and planned strategy	Consider internal and external environments, third parties
2. Map to internal controls	Link risks to existing preventive and detective controls	Include controls across all business units
3. Assess control effectiveness	Evaluate how well controls are designed and operating	Both design and operational effectiveness are critical
4. Assess likelihood & impact	Assess probability of occurrence and potential consequences	Use objective scoring and assessment criteria
5. Prioritize via scoring	Use matrices or heat maps to prioritize high-risk areas	Align with risk appetite and organizational resources
6. Design risk responses	Improve controls, training, policies, and technology as needed	Balance compliance and operational efficiency
7. Assign & monitor implementation	Establish clear accountability and follow-up evaluation	Track implementation and measure outcomes

Table 3. The seven-step COSO compliance risk assessment process.

Metric	Value
Total COSO ERM framework principles	20 principles
Components in the COSO ERM framework	5 major components
Elements of an effective C&E program (per USSG)	7 elements
Key performance indicator categories	8+ KPI categories
Risk assessment process steps	7 core steps
Lines of defense in the compliance model	3 lines (Management / Risk Oversight / Internal Audit)

Table 4. COSO and compliance framework quick-reference statistics. Sources: COSO ERM Framework; U.S. Federal Sentencing Guidelines; Three Lines Model.

The Basel regulatory framework, formulated by the Basel Committee on Banking Supervision, establishes minimum capital requirements and supervisory standards for banking institutions. Introduced after the 2008 crisis, Basel III significantly increased capital buffers, added new liquidity standards, and improved risk-weighted asset calculations, leading to notable enhancements in capital adequacy and liquidity across the banking sector. Its focus on risk-weighted capital has promoted more advanced risk assessment techniques and prompted regulatory arbitrage incentives; studies applying Basel measures to European banks have used these measures to identify systemically important banks and monitor vulnerabilities during crises (Ltaifa & Derbali, 2026). The framework is still evolving, with ongoing discussions on how to integrate climate-related financial risks and operational resilience.

An additional Basel III tool worth noting is the Leverage Ratio, a non-risk-weighted safeguard designed to prevent excessive leverage in banks. It works alongside risk-weighted capital rules and is calculated by dividing Tier 1 capital by total leverage exposure, expressed as a percentage. Total leverage

© MAR 2026 | IRE Journals | Volume 9 Issue 9 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I9-1720341

exposure includes four elements: on-balance-sheet exposures (excluding derivatives and SFTs), derivative exposures, SFT exposures, and off-balance-sheet items. Derivative exposure is determined by adding replacement cost and potential future exposure; SFT exposure is measured at gross value without netting; off-balance-sheet exposure is found by multiplying the notional amount by a credit conversion factor that varies by commitment type (Bank for International Settlements, n.d.). Banks must maintain at least a 3 percent Leverage Ratio at all times, calculated on a gross basis without considering collateral or credit risk mitigation, and report figures quarterly.

ISO 31000 provides internationally recognized, non-prescriptive guidelines for risk management that apply to organizations of all sizes, activities, or sectors. Instead of prescribing specific practices, it outlines principles and a general process that organizations can tailor to their unique context, highlighting the integration of risk management into governance, strategy, planning, and operations. This flexibility is useful for institutions developing a customized ERM framework but also demands careful judgment during implementation, which may lead to varied practices across organizations; consequently, the literature emphasizes integrating ISO 31000's principles with industry-specific requirements and regulatory standards. As shown schematically below, the standard organizes risk management into three interconnected elements: guiding principles, an organizational framework for embedding those principles, and an operational process for applying them.

Figure 4. Schematic overview of the ISO 31000:2018 structure: Principles, Framework, and Process, adapted for this review.

Current research and knowledge gaps: Over the past forty years, the academic literature on banking risk management has grown substantially. Bibliometric analysis indicates a steady increase in publications and citations since the 1990s, with notable peaks in 2012 and 2019, reflecting heightened scholarly interest (Sang, 2024). The research focus has expanded from credit risk to include operational, liquidity, and other significant risk types. Additionally, governance and risk culture are becoming increasingly important. The geographic focus has shifted from primarily U.S. and European

studies to greater contributions from Asia and other emerging economies.

Nonetheless, key gaps still exist. There is a lack of empirical understanding regarding the role of internal audit as a strategic partner within ERM and the limits of technology-enabled assurance (Nkansa, Barr-Pulliam, and Walker, 2025). The impact of emerging threats, such as cybercrime and climate change, on bank risk management warrants further exploration (Sang, 2024). Additionally, there is relatively little research on the effectiveness of specific ERM implementation methods, especially for smaller, resource-limited institutions. The link between risk culture, governance, and ERM outcomes also requires further investigation: risk management culture is deemed vital for organizational resilience, which mediates the translation of risk culture into competitive advantage (Nguyen, Bui, and Corvello, 2026). However, the exact mechanisms by which culture influences risk behaviors and shapes outcomes across various institutional contexts remain unclear.

III. METHODOLOGY

This study utilizes an applied qualitative methodology based on systematic literature review and content analysis. A qualitative approach is particularly appropriate for topics like enterprise risk management, where understanding context, processes, and meanings is as important as measurable results. The aim is to produce practical insights that can guide real-world decisions rather than focusing solely on testing specific statistical hypotheses. The design blends elements of an integrative literature review, merging both theoretical and empirical sources to form a comprehensive overview of the field. It also synthesizes findings from diverse studies, including quantitative research, case studies, and conceptual analyses, to support the integrated framework outlined in Section 6.

The study adopts a hybrid approach that combines deductive and inductive methods: it begins with established frameworks such as COSO, Basel, and ISO 31000, then explores emerging themes and patterns in the literature. This approach allows for the confirmation of existing theories and the uncovering of new insights that may extend or challenge them. The research was conducted in five stages: first, identifying key thematic areas based on research questions; second, systematically searching for and retrieving relevant literature; third, critically analyzing and synthesizing findings within each theme; fourth, integrating these findings into the proposed ERM framework; and finally, developing recommendations based on the combined evidence.

The research utilizes three main categories of sources to ensure comprehensive coverage and validation. Academic journals including peer-reviewed articles from top finance, banking, risk management, and information systems publications were identified through systematic searches in databases such as Scopus, Web of Science, JSTOR, and specialized repositories, using search terms like “enterprise risk management,” “banking risk,” “financial institutions,” “credit risk,” “operational risk,” “cybersecurity,” “regulatory compliance,” and related keywords. Official regulatory publications from the Federal Reserve, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, and the Securities and Exchange Commission provided authoritative guidance on regulatory expectations and supervisory standards. Additionally, industry reports from trade associations (such as the American Bankers Association and the Bank Policy Institute), leading consulting firms (Deloitte, McKinsey, PwC, KPMG), and research organizations contributed a practical perspective on current ERM challenges and emerging trends.

Data collection and analysis were conducted using a systematic review protocol with predefined inclusion and exclusion criteria. Studies were included if they focused on enterprise risk management or a specific banking risk category, were published in English between 2015 and 2025, appeared in peer-reviewed journals or authoritative regulatory or industry sources, and offered empirical or theoretical insights relevant to the research questions. The analysis employed thematic coding, applied iteratively: initial codes were based on the research framework, while additional codes emerged inductively from the data and were validated through cross-source comparisons

© MAR 2026 | IRE Journals | Volume 9 Issue 9 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I9-1720341

and theoretical benchmarks. The synthesis involved narrative integration around key research themes; quantitative results from multiple studies were compared and contextualized to reveal patterns and disparities. Section 6's framework was iteratively refined based on this synthesized evidence, with a focus on practical application and regulatory alignment.

Reliability was maintained through detailed documentation of search strategies, clear inclusion and exclusion criteria, and triangulation across various source types. Continuous review and refinement of emerging themes ensured consistent analysis. Nonetheless, four limitations must be recognized. First, dependence on published literature can bias results toward studies with significant or aligned findings, potentially overlooking null or negative outcomes. Second, due to the fast-moving nature of cybersecurity and technology risks, some findings may quickly become outdated as new developments occur. Third, the relevance of the synthesized results to particular institutions depends on similarities in size, complexity, and regulatory environment. Fourth, since qualitative analysis is interpretive, it involves some subjectivity in coding and theme development, even with systematic efforts to reduce bias.

IV. FINDINGS AND DISCUSSION

4.1 Current ERM Practices

Research reveals significant differences in how U.S. financial institutions implement ERM, with maturity often dependent on their size and resources. Analyses of ERM components across various organizations show that effective ERM implementation is associated with improved reporting quality and reduced variability in future firm performance, such as operating cash flows and stock returns (Gao, Hsu, and Liu, 2025). This highlights the critical role of thorough ERM processes and points to inconsistencies in the extent to which this goal is realized.

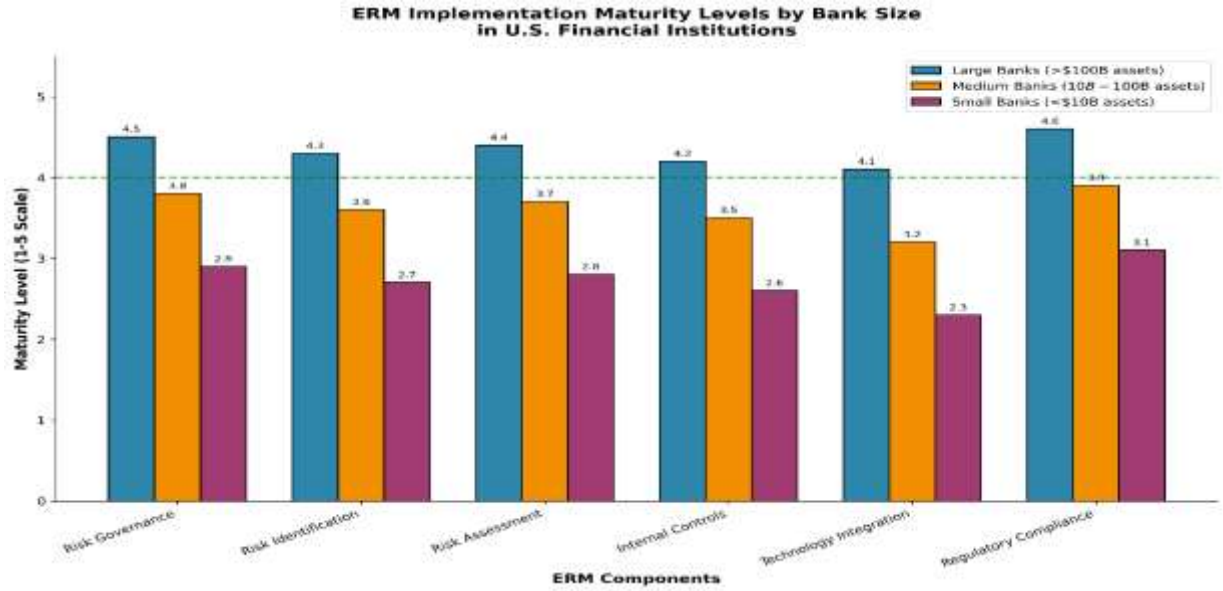

Figure 5. Illustrative ERM implementation maturity levels by bank size across six core ERM components, synthesized from the reviewed literature.

Large institutions typically exhibit more mature ERM practices across all areas due to dedicated risk management teams, advanced technological systems, and stricter regulatory oversight. Research indicates that larger banks often report significantly higher returns on assets and equity, reflecting superior governance. Additionally, economies of scale enable these banks to allocate resources toward advanced

© MAR 2026 | IRE Journals | Volume 9 Issue 9 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I9-1720341

risk analytics, hiring specialized personnel, and deploying comprehensive monitoring tools advantages that smaller institutions find more challenging to attain.

Medium-sized institutions must carefully balance their ERM goals with limited resources. These organizations are complex enough to require advanced risk management, yet they lack the scale to justify large investments in risk infrastructure. Research shows that factors such as relative advantage, top management support, and competitive pressure are critical to effective ERM adoption in these entities (Al-Shanableh et al., 2024). In contrast, smaller institutions tend to concentrate on basic risk management primarily to meet regulatory requirements. Despite facing talent shortages in risk management, their simpler organizational structures can enable more direct oversight and easier communication regarding risk issues.

4.2 Challenges Facing Financial Institutions

The literature identifies five persistent challenges that impede effective ERM implementation across U.S. financial institutions. These are summarized in Table 5 and discussed below.

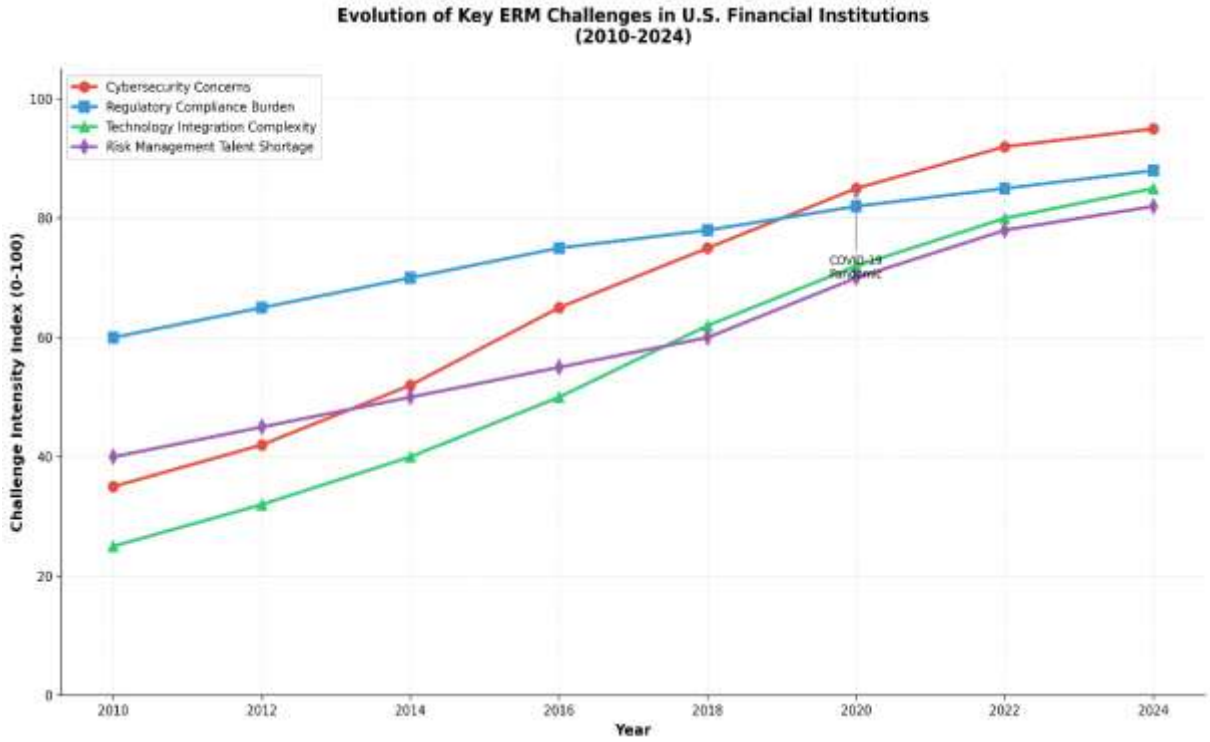

Figure 6. Evolution of key ERM challenge intensity in U.S. financial institutions, 2010–2024 (illustrative index synthesized from the reviewed literature).

Integrating advanced technology into existing risk management systems involves significant challenges. Research on the use of AI in finance highlights concerns such as data privacy, cybersecurity, algorithmic bias, and transparency (Ally, 2025). Organizations must balance the advantages of tech-driven risk management against hurdles such as implementation complexity, regulatory uncertainties, and the need for proper algorithmic governance. An analogous area is mobile banking adoption: a survey of senior bankers from Indonesia's top twenty-five banks revealed that effective ERM implementation correlates with improved bank performance, while adopting mobile banking boosts customer satisfaction, operational efficiency, and profits by enhancing convenience and streamlining processes (Yoewono & Ananto, 2024). Although derived from a different market, this pattern aligns with broader

findings: technology adoption and mature risk governance tend to support each other.

Cybersecurity is increasingly urgent as threats grow more complex and increasingly targeted at financial institutions. The evolving threat landscape complicates the maintenance of defenses, especially for smaller organizations with limited resources to invest in robust cybersecurity measures (Shahzadi et al., 2025). Additionally, the rise of digital banking broadens the attack surface, necessitating innovative methods for user education and security awareness, as well as advanced technical safeguards.

Regulatory burden has grown significantly since 2008, with authorities enforcing more detailed and strict rules for risk management, governance, and capital adequacy. Basel III stands out as the most important global regulation in this area, and the combined complexity of overlapping requirements heavily taxes compliance efforts. RegTech offers administrative benefits by simplifying reporting processes and improving accountability. Nevertheless, its adoption faces barriers such as cybersecurity risks, lack of transparency in algorithms, and fragmented regulations (Bagherifam et al., 2025), causing institutions to juggle complex and sometimes conflicting expectations while striving to stay operationally efficient.

Talent shortage continues to challenge organizations in hiring and retaining skilled risk management professionals, especially those with expertise in cybersecurity, data analytics, or regulatory compliance. Current training methods may lag behind the rapid pace of organizational needs, exposing a gap between existing learning programs and the evolving skill demands (Alrifae et al., 2025).

Structural disconnects occur when there is a "silo effect," where board-level governance does not consistently influence operational risk management (Sringam & Wuttidittachotti, 2026). This misalignment can cause strategic policies to stray from frontline practices, leading to gaps in risk oversight and uneven risk culture throughout the organization. To address these issues, it is essential to foster deliberate alignment between governance structures and everyday operational procedures.

Challenge Category	Primary Manifestations	Impact Level	Trend
Cybersecurity	Sophisticated attacks, data breaches, ransomware	Very High	Escalating
Regulatory compliance	Complex requirements, enforcement uncertainty	High	Stable
Technology integration	Legacy systems, AI governance, data quality	High	Escalating
Talent management	Skills gaps, retention, training effectiveness	Moderate–High	Worsening
Governance alignment	Strategy–operations disconnect, culture	Moderate	Improving

Table 5. Summary of major ERM challenges in U.S. financial institutions.

4.3 Role of Technology in Risk Management

Technology is becoming more crucial in enterprise risk management, with advanced analytics, AI, and automation changing how organizations detect, evaluate, and address risks. Machine learning techniques have significantly outperformed traditional methods: deep neural networks now achieve 96 percent accuracy in fraud detection, while other ML methods have notably reduced default rates (Ma, 2025).

© MAR 2026 | IRE Journals | Volume 9 Issue 9 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I9-1720341

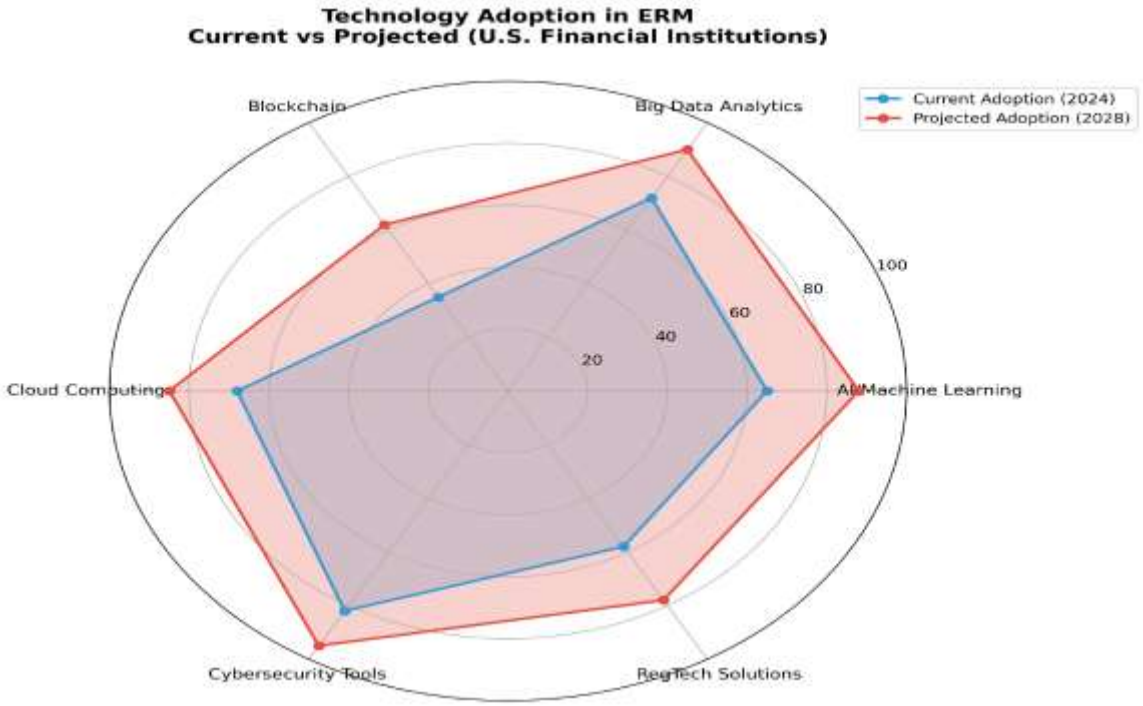

Figure 7. Current versus projected technology adoption in ERM among U.S. financial institutions, by technology category.

Artificial intelligence and machine learning applications now span credit scoring, fraud detection, market-risk modeling, and cybersecurity threat identification. Studies of fraud detection in banking find that machine-learning algorithms have superior discriminatory power compared with classical models, strengthening both security and resilience (Dichev, Zarkova, and Angelov, 2025), and the adoption of generative AI is beginning to transform banking operations through automated content generation, regulatory reporting, and intelligent virtual assistants (Hirani, 2025). That said, AI adoption introduces risks of its own that require dedicated governance attention: output hallucinations, amplification of algorithmic bias, data security vulnerabilities, and compliance challenges specific to highly regulated financial markets (Hirani, 2025). Effective integration depends on human oversight mechanisms, model validation protocols, and robust auditability.

Big data analytics enhances this capability by allowing institutions to process vast amounts of both structured and unstructured data, leading to more advanced risk evaluations and earlier warnings. Its adoption depends on factors such as relative advantages, compatibility, complexity, top-management support, and security issues (Al-Shanableh et al., 2024). When used effectively, big data analytics can improve decision-making, strengthen strategic positioning, and help organizations maintain competitive advantage in rapidly changing markets (Aldossari, Mokhtar, and Ghani, 2025). Building on this, predictive analytics supports proactive risk management by forecasting potential issues. Models have successfully predicted liquidity shortages up to three months in advance and detected unauthorized transactions worth millions within short timeframes (Ma, 2025), enabling organizations to take preventive measures and allocate resources more efficiently.

Cybersecurity technology continually advances in tandem with evolving threats, emphasizing multi-layered strategies that integrate endpoint and network security, penetration testing, threat intelligence feeds, and regular assessments (Shahzadi et al., 2025). The integration of machine learning into cybersecurity tools is revolutionizing detection and response capabilities, with AI-driven systems now detecting

anomalous patterns in real time (Shahzadi et al., 2025). Meanwhile, regulatory and supervisory technologies (RegTech and SupTech) enhance compliance management and risk oversight. Research shows that these tools boost supervisory agility, transparency, and real-time monitoring for regulators (Bagherifam et al., 2025), and further advancements are expected to improve regulatory efficiency.

4.4 Impact of ERM on Organizational Resilience

The link between ERM implementation and organizational resilience has gained significant attention, particularly amid the COVID-19 pandemic and recent shocks. Strong evidence shows that effective ERM boosts resilience, enhances financial performance, and increases value. Studies indicate that ERM adoption is positively associated with firm performance, firm value, and lower insolvency risk, particularly in the banking sector (Akbaş, 2024). This highlights ERM's comprehensive approach to risk management, enabling organizations to foresee threats, respond efficiently to disruptions, and recover swiftly from crises. Such capabilities are increasingly vital in today's unpredictable environment faced by financial institutions.

The empirical evidence confirms the mediating role of IT security in the ERM-performance link: ERM enhances both financial and non-financial outcomes, with IT security fully mediating the relationship specifically for financial performance (Weld-Ali, Zakuan, and Setap, 2025). This highlights the interconnectedness of various risk domains and supports the need for integrated approaches that explicitly acknowledge these linkages. Broader research on organizational resilience also emphasizes risk management culture as a vital foundation, with resilience mediating the translation of that culture into competitive advantage (Nguyen, Bui, and Corvello, 2026). Organizations with robust risk cultures are better equipped to adapt, maintain operational continuity during disruptions, and recover stronger from crises. A systemic view adds further nuance: comparative studies of financial system stability show that Islamic financial institutions tend to be more resilient and experience lower contagion during crises than conventional institutions (Khurram, Iqbal, and Pappas, 2025). This suggests that institutional design and operating principles can significantly influence resilience characteristics, informing framework development.

ERM Component	Resilience Impact	Performance Impact	Evidence Strength
Risk governance	High	High	Strong
Risk identification	Very High	Moderate	Strong
Risk assessment	High	High	Strong
Internal controls	High	High	Strong
Technology integration	Moderate–High	High	Moderate
Monitoring	High	Moderate	Moderate
Compliance	Moderate	Moderate	Strong
Business continuity	Very High	Low–Moderate	Moderate

Table 6. Estimated impact of ERM components on organizational resilience and performance, synthesized from the reviewed literature.

V. PROPOSED INTEGRATED ERM FRAMEWORK

Building on academic research, regulatory guidance, and industry best practices outlined earlier, this section introduces an integrated ERM framework tailored for U.S. financial institutions in today's risk landscape. The framework comprises eight interconnected components, with risk governance as

© MAR 2026 | IRE Journals | Volume 9 Issue 9 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I9-1720341

the central element that coordinates and unifies the other seven.

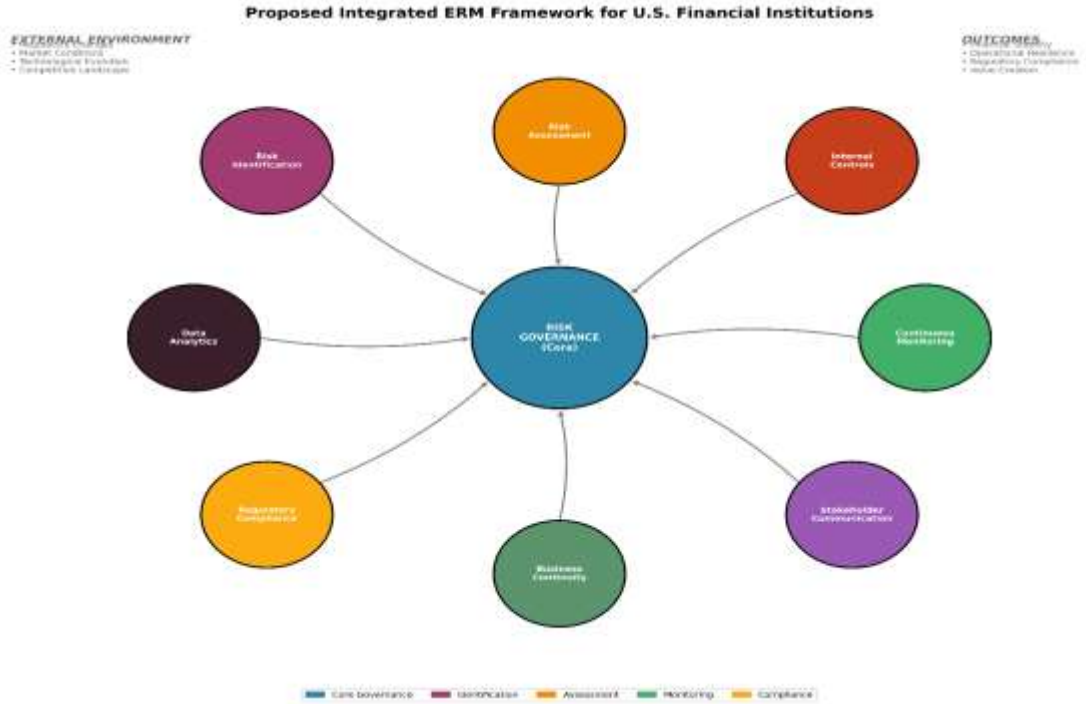

Figure 8. Proposed integrated ERM framework for U.S. financial institutions, with risk governance as the central coordinating function.

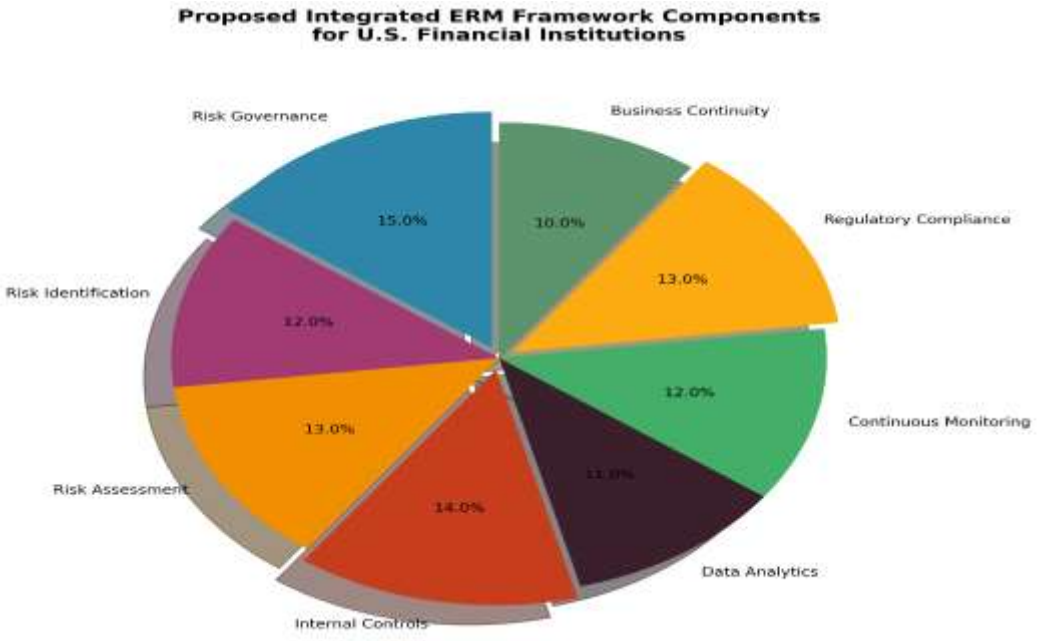

Figure 9. Illustrative weighting of the eight framework components within the proposed integrated ERM model.

© MAR 2026 | IRE Journals | Volume 9 Issue 9 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I9-1720341

Component	Function	Key Elements
Risk governance	Foundation and central coordinating mechanism; ensures risk management is integrated into strategic decision-making, adequately resourced, and consistently applied.	Board risk committee; risk appetite framework; Chief Risk Officer with direct board access; deliberate risk culture
Risk identification	Systematic recognition of existing and emerging risk across all organizational activities; the strongest positive driver of organizational readiness in the literature.	Risk universe inventory; emerging-risk scanning; internal risk-source assessment; stakeholder input channels
Risk assessment	Evaluation of identified risks by likelihood and impact to enable prioritization of management effort.	Qualitative assessment and scenario planning; quantitative modeling; stress testing; interconnection analysis
Internal controls	Policies, procedures, and mechanisms that ensure operational effectiveness, reliable reporting, and regulatory compliance.	Preventive, detective, and corrective controls; Three Lines Model
Data analytics	Advanced analytics supporting more sophisticated identification, assessment, monitoring, and data-driven decision-making.	Data infrastructure; analytical tooling; model governance; data-quality standards
Continuous monitoring	Ongoing visibility into risk exposures and control effectiveness, enabling timely response to emerging issues.	Key risk indicators; control monitoring; threshold alerts; real-time dashboard reporting
Regulatory compliance	Processes for understanding, implementing, and demonstrating adherence to applicable laws and supervisory expectations.	Regulatory tracking; documented compliance programs; testing and validation; proactive regulator relationships
Business continuity	Capability to sustain critical operations through disruption and recover effectively afterward.	Business impact analysis; recovery strategies; testing and exercises; crisis management protocols

Table 7. The eight components of the proposed integrated ERM framework.

Risk governance forms the foundation of the framework. Studies show a positive link between governance traits and financial results, with factors such as board size, independence, and gender diversity notably boosting return on assets and return on equity (Abiad et al., 2025). The presence of formal risk governance arrangements is crucial: having a dedicated risk management function influences how board characteristics relate to financial performance, highlighting the need to turn governance quality into specific organizational structures (Musallam, 2024). In practice, this involves defining clear risk ownership, escalation procedures, and accountability systems, as well as the board-level structures outlined in Table 3.

Risk identification should be an ongoing process rather than a periodic one, integrating qualitative judgment with quantitative indicators. It should also expand beyond traditional credit risk to include operational, liquidity, cybersecurity, and strategic risks (Sang, 2024).

Risk assessment should combine analytical depth with practicality to provide useful insights for decision-making. The literature highlights the

importance of embedding assessment within a larger sustainability strategy to enhance organizational resilience (Anton, Baba, and Bucșoiu, 2025).

Internal controls demand continuous investment and adjustment as risk profiles and operational procedures evolve. Studies show that effective internal controls and audit committees notably decrease financial risk (Surana, 2025). Additionally, literature on internal audit's changing role in ERM highlights the need to balance assurance and consulting functions while maintaining independence (Nkansa, Barr-Pulliam, and Walker, 2025).

Data analytics plays a vital role in modern risk management. Machine-learning methods have greatly improved fraud detection, default prediction, and portfolio optimization (Ma, 2025). For example, real-time fraud detection systems now achieve up to 98.5% accuracy while efficiently handling large volumes of data (Sathupadi et al., 2025). However, achieving these benefits depends on institutions properly governing algorithmic decisions, rather than viewing analytical complexity as an end in itself.

Continuous monitoring creates a feedback loop that enables the risk management strategy to adapt in real-time. It should leverage information from across the organization to offer truly comprehensive visibility. Research on cyber resilience highlights the importance of combining monitoring systems with threat intelligence for effective detection (Shahzadi et al., 2025), with the results directly informing governance debates and control modifications.

Regulatory compliance should be integrated into the broader ERM function rather than treated as a separate activity. Research on RegTech adoption indicates that these tools enhance compliance management while addressing issues such as regulatory fragmentation and enforcement uncertainty (Bagherifam et al., 2025). When embedded within this framework, the compliance function is most well-placed to participate in strategic discussions on regulatory changes.

Business continuity planning completes the framework by ensuring that institutions can sustain critical functions during disruptions and recover efficiently afterward. Recent crises have highlighted the importance of this capability, and research confirms its vital role in supporting sustainable organizational performance (Gul, Karaatmaca, and Raza, 2025). The planning process should consider all possible disruptions, including technology failures, natural disasters, pandemics, and cyberattacks. Additionally, it must be regularly reviewed and updated as risk profiles evolve and insights from exercises and actual events emerge.

VI. RECOMMENDATIONS

Building on the findings above and the framework outlined in Section 5, this section presents six practical recommendations for U.S. financial institutions aiming to enhance their ERM capabilities and organizational resilience. These recommendations are summarized in Table 8 and elaborated on below.

Recommendation	Priority Actions
Improve governance and board oversight.	Dedicated risk committees; enhanced director risk qualifications; direct CRO board access; regular board risk-competency assessment
Strengthen internal controls	Risk-based control testing; stronger segregation of duties in high-risk areas; automated controls where feasible; adequately resourced internal audit
Adopt predictive analytics	Investment in data infrastructure and analytical talent; early-warning systems for credit deterioration; real-time fraud detection; robust model-validation governance
Enhance cybersecurity	Multi-layered defense and zero-trust architecture; regular penetration testing; incident response planning; cybersecurity embedded in third-party vendor management

Recommendation	Priority Actions
Invest in employee training.	Role-tailored training with emphasis on compliance, fraud prevention, and information security; regular effectiveness assessment; a culture that empowers escalation
Improve regulatory compliance	Proactive regulatory affairs capability; compliance integrated with broader ERM; active engagement in consultations and industry working groups

Table 8. Summary of recommendations and priority actions.

Improve governance and board oversight: Financial institutions need to boost board-level engagement in risk management by establishing dedicated risk committees, enhancing director qualifications, and improving information flow. Research shows that board traits such as size, independence, and diversity greatly improve financial performance (Abiad et al., 2025). Boards should also receive regular, comprehensive risk reports to enable effective oversight and strategic decisions. Practically, this involves having clear risk-appetite statements aligned with strategic goals, providing the Chief Risk Officer with direct access to the board, and regularly evaluating the board's risk management skills. Governance frameworks should also enable the board to challenge management's risk choices while encouraging responsible risk-taking to achieve strategic aims.

Strengthen internal controls: Control environments require continuous investment to remain effective amid evolving risks. Studies indicate that improved internal controls and a more effective audit committee substantially lower financial risk (Surana, 2025). Therefore, institutions should regularly evaluate both the design and operational effectiveness of controls and quickly address any weaknesses. Key priorities include enhancing segregation of duties in high-risk zones, implementing automated controls where possible, and ensuring sufficient resources for internal audits. The Three Lines Model should be clearly adopted, with control testing focused on areas of higher inherent risk or prior issues.

Adopt predictive analytics: Institutions need to accelerate the adoption of advanced analytics to better identify, assess, and monitor risk. Machine-learning frameworks have shown significant improvements in areas such as fraud detection, default prediction, and risk warning (Ma, 2025), enabling more proactive risk management than traditional reactive methods. Achieving this requires investing in data infrastructure, analytical expertise, and model-validation systems, and establishing clear responsibilities for model performance and maintaining human oversight of automated decisions, ensuring that technology complements rather than replaces human judgment.

Enhance cybersecurity: As cyber threats become more sophisticated and frequent, institutions must continuously update their defenses. Key measures include implementing a multi-layered cybersecurity architecture, adopting a zero-trust approach, and developing mature incident-response capabilities. Since failures at systemically important institutions can threaten the broader financial system, industry-wide coordination is essential alongside individual investments. Critical priorities include vulnerability management, employee security awareness training, regular penetration testing with swift fixes, and applying cybersecurity standards to third-party vendors, especially as supply chain vulnerabilities grow.

Invest in employee training: Since individuals at all levels influence organizational risk outcomes, training programs should enhance risk awareness, clarify compliance requirements, and develop technical risk management skills across the institution. These programs should be role-specific, with a strong focus on compliance, fraud prevention, and information security, and should be regularly updated based on assessments of their effectiveness. Additionally, institutions should foster a risk culture

in which employees feel empowered to identify and escalate concerns.

Improve regulatory compliance: As the regulatory landscape evolves amid emerging risks and threats, institutions should develop strong regulatory affairs capabilities and adopt a proactive approach rather than a solely compliance-focused stance. This involves engaging with industry groups and consultations, and integrating compliance efforts into the wider ERM framework, acknowledging that regulatory requirements are rooted in risk-based thinking.

VII. IMPLICATIONS FOR THE U.S. FINANCIAL SYSTEM

Financial stability: Enhanced ERM practices across financial institutions play a crucial role in supporting overall macroeconomic financial stability. Firms with stronger risk management systems generally experience lower default rates and are better able to withstand market stress. As more institutions improve their risk strategies, overall systemic risk diminishes, reducing both the likelihood and the potential impact of financial crises. When many adopt advanced ERM methods, it creates positive external effects for the entire financial system: better risk detection helps identify emerging systemic threats earlier and facilitates timely regulatory responses. Additionally, improved governance and accountability frameworks bolster market discipline across the sector.

Banking resilience and stability: Resilience at the individual institution level directly enhances the overall banking system's ability to sustain credit and financial services during stressful periods. Institutions with robust ERM frameworks are better equipped with sufficient capital and liquidity buffers, foster longer-term lending relationships, and ensure greater business continuity amid disruptions advantages that benefit customers, counterparties, and the economy at large. By strengthening risk management in good times, resilient institutions maintain their capacity for prudent lending during downturns, helping to lessen their severity and facilitate faster recovery.

Fraud reduction: Enhanced analytics and tighter controls directly reduce fraud losses that impact institutions, customers, and the entire financial system, an important benefit, given that the industry loses billions to fraud each year. As detection capabilities advance, fraudsters encounter a greater chance of being caught and facing consequences, which acts as a deterrent. This decline in fraud helps maintain institutional profitability and sustains customer confidence across the system.

Consumer confidence: Consumer trust in financial institutions is crucial to the stability of the banking system and the efficient delivery of financial services. This trust can erode rapidly if failures, fraud, or poor risk management become evident, so demonstrating sincere commitment to risk management and communicating it clearly helps build customer loyalty and market confidence. When consumers see that an institution has strict risk controls and accountability, they feel more assured and continue to depend on its services.

Economic growth support: Financial institutions play a crucial role in enabling economic activity by offering credit, investment services, and payment systems. When these institutions are resilient and manage risks effectively, they can support business investments, home purchases, and overall economic growth. On the other hand, financial instability reduces credit availability and hampers growth. Improving risk management at the institutional level helps the U.S. financial system better withstand economic shocks, ensuring continued support for creditworthy borrowers and productive investments.

VIII. CONCLUSION

Enterprise Risk Management has evolved from a compliance-oriented function into a strategic imperative for financial institutions operating in an increasingly complex risk environment. This research shows that ERM frameworks that integrate governance, risk identification, assessment, monitoring, and controls enable institutions to balance risk-taking with prudent risk management (Abiad et al., 2025). It also shows that the convergence of technological disruption, regulatory

evolution, geopolitical tension, and emerging environmental risk makes continuous ERM enhancement an ongoing imperative rather than a one-time project.

The ERM framework outlined in Section 5 combines best practices with new methods, guiding U.S. financial institutions toward resilience in various risk areas. The six recommendations in Section 6, enhancing governance, controls, predictive analytics, cybersecurity, employee training, and regulatory engagement, offer clear steps for institutions to implement the framework effectively, boosting risk management and organizational resilience.

Future research should explore emerging risks, including artificial intelligence governance, climate risk assessment methods, and the effects of digital assets on financial stability. As financial institutions and regulatory frameworks evolve, continuous investigation into ERM effectiveness, implementation hurdles, and new risk-management practices will be crucial. Ultimately, the success of ERM relies on organizations viewing risk management as a key strategic skill rather than merely a compliance requirement. Robust enterprise risk management enhances individual institutions, bolsters the resilience of the banking system, and supports U.S. economic growth and stability. By adopting the recommendations outlined here, financial institutions can better navigate current complexities and prepare for future challenges.

REFERENCES

[1] Abiad, Z., Abraham, R., El-Chaarani, H., & Binsaddig, R. (2025). The impact of board of directors' characteristics on the financial performance of the banking sector in Gulf Cooperation Council (GCC) countries: The moderating role of bank size. Journal of Risk and Financial Management. https://doi.org/10.3390/jrfm18010040

[2] Akbaş, M. Ç. (2024). Measuring the impact of enterprise risk management on the performance, value, and risk indicators of Borsa Istanbul XBANK companies using data-mining prediction models. Humanities and Social Sciences Communications. https://doi.org/10.1057/s41599-024-03871-z

[3] Aldossari, S., Mokhtar, U. A., & Ghani, A. T. A. (2025). Empowering Saudi manufacturing small and medium enterprises: A framework for big data analytics adoption and its impact on decision-making. SAGE Open. https://doi.org/10.1177/21582440251369162

[4] Ally, A. M. (2025). Artificial intelligence (AI) and financial technology (FinTech) in Tanzania: Legal and regulatory issues. International Journal of Law and Management. https://doi.org/10.1108/ijlma-07-2024-0251

[5] Alrifae, A. A. M., Alhabeeb, A., Alhanatleh, H., & Alnajdawi, S. (2025). Exploring the role of succession planning and talent development in enhancing organizational agility: The case of Saudi Arabia's banking sector. Sustainability. https://doi.org/10.3390/su172411215

[6] Al-Shanableh, N., Alzyoud, M., Al-Omar, S., Kilani, Y., Nashnush, E., Al-Hawary, S. I. S., & Al-Momani, A. M. (2024). The adoption of big data analytics in Jordanian SMEs: An extended technology-organization-environment framework with diffusion of innovation and perceived usefulness. International Journal of Data and Network Science. https://doi.org/10.5267/j.ijdns.2024.1.003

[7] Anton, C. E., Baba, C. M., & Bucșoiu, O.-A. (2025). Perspectives on integrating risk management and sustainability for financial performance: A systematic literature review. Sustainability. https://doi.org/10.3390/su17083456

[8] Bagherifam, N., Naghdi, S., Ahmadian, V., Fazlzadeh, A., & Baghalzadeh Shishehgarkhaneh, M. (2025). Digital regulatory governance: The role of RegTech and SupTech in transforming financial oversight and administrative capacity. International Journal of Financial Studies. https://doi.org/10.3390/ijfs13040217

[9] Bank for International Settlements. (n.d.). Basel III: International regulatory framework for banks. https://www.bis.org/bcbs/basel3.htm

[10] Ch, R. K., Meenadevi, K., Kumar, D, D., & Nagaraj, R. (2026). Deep learning in credit risk assessment: A data-driven approach to transforming financial decision-making and risk analytics. Journal of Risk and Financial Management. https://doi.org/10.3390/jrfm19050361

[11] Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2020). Compliance risk management: Applying the COSO ERM framework. https://www.coso.org/_files/ugd/3059fc_5f9c50e005034badb07f94e9712d9a56.pdf

[12] Dichev, A. V., Zarkova, S., & Angelov, P. (2025). Machine learning as a tool for assessing and managing fraud risk in banking transactions. Journal of Risk and Financial Management. https://doi.org/10.3390/jrfm18030130

[13] Gao, S., Hsu, H.-T., & Liu, F. (2025). Enterprise risk management, financial reporting and firm operations. Risks. https://doi.org/10.3390/risks13030048

[14] Gul, T., Karaatmaca, A. G., & Raza, A. (2025). Impact of green human resources management practices on sustainability through organizational resilience and organizational learning in Pakistan's banking sector. Sustainability. https://doi.org/10.3390/su17052087

[15] Hirani, V. K. (2025). Generative artificial intelligence in banking: Risk management frameworks for responsible deployment. Journal of International Crisis and Risk Communication Research. https://doi.org/10.63278/jicrcr.vi.3455

[16] Ismail, S., & Ahmed, E. (2023). The impact of liquidity, credit, and operational risk on financial stability of conventional banks in Jordan. Uncertain Supply Chain Management. https://doi.org/10.5267/j.uscm.2023.3.006

[17] Kagima, J. W., & Munene, R. (2025). Evaluation of operational risk management practice and financial performance of commercial banks in Kenya. International Journal of Research and Innovation in Social Science. https://doi.org/10.47772/ijriss.2025.90500088

[18] Khurram, A., Iqbal, A., & Pappas, V. (2025). Systemic risk: New evidence from alternative financial systems. Review of Quantitative Finance and Accounting. https://doi.org/10.1007/s11156-025-01413-5

[19] Lawati, A. A., Hussin, B. M., Kadir, M. R. A., & Khudari, M. (2025). The impact of enterprise risk management on firm competitiveness: The mediating role of competitive advantage in the Omani insurance industry. Risks. https://doi.org/10.3390/risks13100199

[20] Ltaifa, M., & Derbali, A. M. S. (2026). The stability of European financial institutions amid systemic risk and unexpected shocks: An empirical study from 2005 to 2024. Journal of Economic Integration. https://doi.org/10.11130/jei.2026001

[21] Ma, T. (2025). Research on the application of artificial intelligence technology in enterprise financial risk warning – Based on machine learning method. Decision Making: Applications in Management and Engineering. https://doi.org/10.31181/dmame8120251489

[22] Miloș, M., & Miloș, L. (2022). Use of derivatives and market valuation of the banking sector: Evidence from the European Union. Journal of Risk and Financial Management. https://doi.org/10.3390/jrfm15110501

[23] Musallam, S. (2024). The effect of the board of directors on financial performance and the existence of risk management as an intervening variable. Journal of Islamic Marketing. https://doi.org/10.1108/jima-10-2022-0270

[24] Nguyen, P. V., Bui, L., & Corvello, V. (2026). Driving business performance through risk management culture and organizational

resilience: Examining the role of government support. Business Process Management Journal. https://doi.org/10.1108/bpmj-10-2025-1732

[25] Nkansa, P., Barr-Pulliam, D., & Walker, K. (2025). From compliance to strategic partnerships: The role of internal audit in enterprise risk management and opportunities for future research. Journal of Risk and Financial Management. https://doi.org/10.3390/jrfm18120707

[26] Sang, N. M. (2024). Evolution and future directions of banking risk management research: A bibliometric analysis. Banks and Bank Systems. https://doi.org/10.21511/bbs.19(2).2024.01

[27] Sathupadi, K., Achar, S., Bhaskaran, S. V., Faruqui, N., & Uddin, J. (2025). BankNet: Real-time big data analytics for secure internet banking. Big Data and Cognitive Computing. https://doi.org/10.3390/bdcc9020024

[28] Shahzadi, A., Ishaq, K., Nawaz, N. A., Rosdi, F., & Khan, F. A. (2025). Unveiling personalized and gamification-based cybersecurity risks within financial institutions. PeerJ Computer Science. https://doi.org/10.7717/peerj-cs.2598

[29] Sringam, A., & Wuttidittachotti, P. (2026). The paradox of cyber risk controls: An empirical analysis of readiness and protection inefficiencies in Thailand's financial sector. Risks. https://doi.org/10.3390/risks14010020

[30] Stasse, L. J. A., Hilhorst, C. A. R., & Rouwelaar, J. A. T. (2025). Enterprise risk management revisited: A study to identify the elements of ERM. Journal of Risk Research. https://doi.org/10.1080/13669877.2025.2553846

[31] Surana, S. (2025). The efficacy of internal controls and audit committees in mitigating financial risk: Perspectives from Indian corporate governance. Journal of International Crisis and Risk Communication Research. https://doi.org/10.63278/jicrcr.vi.3370

[32] Wang, W., & Wu, Y. (2025). Forecasting and hedging volatility indices in financial markets using a robust XGBoost model. SAGE Open. https://doi.org/10.1177/21582440251396044

[33] Weld-Ali, W. M., Zakuan, N., & Setap, M. (2025). The effect of enterprise risk management implementation and information technology security on organizational performance in Jordan manufacturing industry. Journal of Posthumanism. https://doi.org/10.63332/joph.v5i6.2203

[34] Yoewono, H., & Ananto, P. (2024). Enhancing bank performance: Integrating enterprise risk management with mobile banking applications. Journal of Economics, Business & Accountancy. https://doi.org/10.14414/jebav.v27i2.4572