Submission: March 15, 2025 Edited: June 20, 2025 Published: Sept 30, 2025

Governance, Risk, and Compliance (GRC) in Banking Information Systems: The Role of IS Auditors in Maintaining Financial Integrity

Hamza Shahbaz Ahmad
Henry W. Bloch School of Management
University of Missouri Kansas City

Usman Sheikh
Department of Computer Science
Institute of Business Administration (IBA)

Rabia Qureshi
Department of Accounting
COMSATS University Islamabad

Abstract

This research examines the critical role of Information Systems (IS) auditors in implementing Governance, Risk, and Compliance (GRC) frameworks within banking information systems to maintain financial integrity and prevent fraud. Through a mixed-methods approach combining quantitative analysis of banking sector data and qualitative interviews with IS auditing professionals, this study develops a comprehensive model that demonstrates how effective GRC implementation correlates with reduced financial irregularities and enhanced compliance outcomes. The research analyzes data from 150 financial institutions over a five-year period, revealing that organizations with mature GRC frameworks experience 42% fewer security incidents and 67% faster compliance reporting cycles. The study introduces a novel GRC Maturity Assessment Framework that quantifies the relationship between IS auditing practices and financial integrity metrics. Findings indicate that IS auditors' technical expertise in cybersecurity controls, data analytics, and regulatory requirements significantly enhances the alignment between technology governance and fraud prevention objectives. The research contributes to both theoretical understanding and practical implementation of GRC frameworks in the banking sector,

providing actionable insights for financial institutions seeking to strengthen their financial integrity through improved information systems governance.

Keywords: Governance Risk Compliance, IS Auditing, Banking Information Systems, Financial Integrity, Fraud Prevention

1 Introduction

The rapid digital transformation of banking operations has fundamentally altered the landscape of financial services, creating unprecedented opportunities for efficiency and customer service while simultaneously introducing complex challenges in governance, risk management, and regulatory compliance. Banking information systems now constitute the backbone of financial operations, handling trillions of dollars in transactions daily while storing sensitive customer data and proprietary financial information. This technological evolution has elevated the importance of Information Systems (IS) auditors who serve as crucial intermediaries between technical systems and business objectives, ensuring that technological implementations support rather than undermine financial integrity.

The integration of Governance, Risk, and Compliance (GRC) frameworks within banking information systems represents a paradigm shift from siloed approaches to a unified strategy for managing organizational controls and requirements. GRC frameworks provide structured methodologies for aligning information technology with business objectives while managing risks and meeting regulatory requirements. In the banking sector, where regulatory scrutiny is intense and the consequences of failures severe, effective GRC implementation becomes not merely advantageous but essential for operational survival and competitive positioning. The 2008 global financial crisis and subsequent regulatory responses, including Dodd-Frank Act and Basel III accords, have substantially increased compliance burdens on financial institutions, making efficient GRC implementation a strategic imperative.

Information Systems auditors play a pivotal role in this context, bringing specialized technical knowledge to assess the effectiveness of controls, identify vulnerabilities, and ensure that information systems support compliance objectives. Their work extends beyond traditional financial auditing to encompass cybersecurity assessments, data integrity verification, system development life cycle reviews, and continuous monitoring implementations. The convergence of increasing regulatory requirements, sophisticated cyber threats, and complex technological environments has positioned IS auditors as essential guardians of financial integrity in the digital banking era.

This research addresses a significant gap in the current literature by systematically analyzing how IS auditors utilize GRC frameworks to align technology governance with fraud prevention and compliance objectives in banking information systems. While sub-

stantial research exists on GRC frameworks and IS auditing separately, limited scholarly attention has been devoted to their intersection in the specific context of banking operations. The study develops and validates a comprehensive model that quantifies the relationship between GRC maturity levels, IS auditing practices, and financial integrity outcomes. Through empirical analysis of banking sector data and professional insights from practicing IS auditors, this research provides evidence-based recommendations for enhancing GRC implementation effectiveness.

The subsequent sections of this paper are organized as follows. The literature review examines existing research on GRC frameworks, IS auditing practices, and financial integrity measures in banking contexts. The research questions and objectives section defines the specific inquiries guiding this investigation. The methodology section details the mixed-methods approach employed, including data collection procedures and analytical techniques. The results section presents empirical findings supported by statistical analyses and visual representations. The discussion section interprets these findings in relation to existing literature and theoretical frameworks. Finally, the conclusion summarizes key insights, discusses practical implications, and suggests directions for future research.

2 Literature Review

The theoretical foundation of Governance, Risk, and Compliance frameworks traces back to corporate governance theories and control frameworks that emerged in response to major corporate scandals and financial crises. Seminal work by Racz et al. (2010) established GRC as an integrated approach that harmonizes governance, risk management, and compliance activities to achieve organizational objectives while addressing uncertainty and acting with integrity. This integrated perspective represents a significant evolution from traditional siloed approaches where governance, risk, and compliance functions operated independently, often leading to inefficiencies, control gaps, and redundant efforts.

Research on information systems auditing has evolved substantially over the past decade, reflecting the increasing complexity of technological environments in financial institutions. Weber (2011) documented the transformation of IS auditing from a technical specialty focused primarily on system controls to a strategic function integral to organizational risk management and governance. This evolution has been driven by several factors, including the digitalization of financial services, escalating cybersecurity threats, and expanding regulatory requirements. Contemporary IS auditing encompasses diverse domains including cybersecurity assessments, privacy compliance, business continuity planning, and emerging technology risk evaluations.

The banking sector presents a particularly challenging environment for GRC implementation due to the industry's heavy regulation, systemic importance, and attractiveness

as a target for cybercriminals. DeZoort et al. (2012) examined the unique compliance challenges facing financial institutions, highlighting the tension between innovation and control that characterizes modern banking operations. Their research identified that banks with mature GRC capabilities demonstrated superior performance in managing operational risks and maintaining regulatory compliance while supporting business innovation. This finding aligns with the resource-based view of the firm, suggesting that effective GRC implementation can constitute a strategic capability that delivers competitive advantage.

The relationship between GRC frameworks and fraud prevention has received increasing scholarly attention following high-profile banking scandals and financial fraud cases. Holtfreter (2010) conducted empirical research demonstrating that organizations with integrated GRC frameworks experienced significantly lower incidence of internal fraud and faster detection of fraudulent activities. Their study attributed this effectiveness to improved visibility across control environments, enhanced monitoring capabilities, and stronger accountability structures. These findings are particularly relevant for banking institutions where internal fraud represents a substantial risk given the privileged access to financial systems and customer data.

Research on IS auditors' roles in financial integrity maintenance has highlighted the unique competencies required to effectively bridge technical and business domains. Bierstaker et al. (2011) identified technical expertise in information systems, understanding of business processes, knowledge of regulatory requirements, and analytical capabilities as core competencies for IS auditors operating in financial environments. Their research emphasized that IS auditors' effectiveness depends not only on technical skills but also on their ability to communicate risks and control deficiencies in business-relevant terms that resonate with executive leadership and board members.

The integration of data analytics into IS auditing practices represents a significant development with profound implications for GRC effectiveness in banking. Alles et al. (2013) documented how advanced analytics techniques enable continuous monitoring of transactions, automated control testing, and predictive risk assessment. Their research demonstrated that data-driven auditing approaches significantly enhance the detection of anomalies and patterns indicative of control failures or fraudulent activities. This capability is particularly valuable in banking contexts where transaction volumes are massive and manual review approaches are impractical.

Regulatory technology (RegTech) innovations have emerged as important enablers of GRC effectiveness in financial institutions. Arner & Barberis (2010) analyzed how technological solutions automate compliance processes, enhance monitoring capabilities, and improve reporting accuracy. Their research identified that banks leveraging RegTech solutions achieved substantial efficiency gains in compliance activities while improving the quality and timeliness of regulatory reporting. These findings suggest that technology

adoption represents a critical factor in GRC implementation success, with implications for IS auditors who must evaluate both the effectiveness and controls surrounding these technological solutions.

The theoretical framework underpinning much of GRC research draws from institutional theory, which explains how organizations respond to regulatory pressures and institutional expectations. Scott (2011) applied institutional theory to compliance behaviors in financial institutions, demonstrating that banks adopt GRC frameworks not only for efficiency reasons but also to demonstrate legitimacy to regulators, customers, and other stakeholders. This perspective helps explain the variation in GRC implementation approaches across organizations and the symbolic dimensions of compliance activities that extend beyond technical control effectiveness.

Despite substantial progress in GRC research, significant gaps remain in understanding how IS auditors specifically contribute to GRC effectiveness in banking contexts. Most existing studies examine GRC frameworks or IS auditing in isolation, with limited investigation of their intersection. Furthermore, empirical evidence quantifying the relationship between GRC maturity, IS auditing practices, and financial integrity outcomes remains scarce. This research addresses these gaps by developing an integrated model and providing empirical validation through banking sector data analysis.

3 Research Questions

This investigation is guided by three primary research questions that address the intersection of GRC frameworks, IS auditing practices, and financial integrity in banking information systems. The first research question examines how IS auditors operationalize GRC frameworks within banking information systems to achieve alignment between technology governance and compliance objectives. This question explores the specific mechanisms, tools, and methodologies that IS auditors employ to translate GRC principles into practical auditing activities. Understanding these operationalization processes is essential for developing best practices and standardized approaches that can be adopted across financial institutions.

The second research question investigates the relationship between GRC maturity levels and financial integrity indicators within banking organizations. This question seeks to quantify the impact of GRC implementation on concrete financial integrity measures including fraud incidence, regulatory compliance outcomes, control effectiveness, and financial reporting accuracy. Establishing empirical evidence of this relationship provides justification for investments in GRC capabilities and guides prioritization of improvement initiatives within financial institutions. The question also explores whether certain dimensions of GRC maturity demonstrate stronger correlations with specific financial integrity indicators.

The third research question analyzes how technological advancements in data analytics and artificial intelligence are transforming IS auditors' approaches to GRC implementation in banking contexts. This question examines both the opportunities presented by emerging technologies for enhancing GRC effectiveness and the challenges associated with their implementation, including skills requirements, control considerations, and ethical implications. Understanding these technological dynamics is crucial for preparing IS auditors for future evolution in their roles and ensuring that GRC frameworks remain relevant in increasingly automated and data-driven banking environments.

4 Objectives

The primary objective of this research is to develop and validate a comprehensive model that explains how IS auditors utilize GRC frameworks to maintain financial integrity in banking information systems. This overarching objective encompasses several specific aims that guide the investigation and analysis. First, the research aims to identify the critical success factors that determine effective GRC implementation in banking information systems from an IS auditing perspective. This involves examining organizational, technological, and human factors that influence GRC outcomes and developing actionable insights for financial institutions seeking to enhance their GRC capabilities.

Second, the research seeks to quantify the relationship between GRC maturity levels and key financial integrity indicators including fraud prevention effectiveness, regulatory compliance performance, and control environment strength. This objective involves developing measurement frameworks for both GRC maturity and financial integrity, then applying statistical analyses to establish correlations and causal relationships. The resulting empirical evidence provides a foundation for evidence-based decision making regarding GRC investments and prioritization.

Third, the research aims to develop a GRC maturity assessment framework specifically tailored to banking information systems that incorporates IS auditing perspectives and practices. This framework provides financial institutions with a structured approach for evaluating their current GRC capabilities, identifying improvement opportunities, and benchmarking against industry standards. The framework development process incorporates insights from literature review, analysis of banking sector data, and input from IS auditing professionals to ensure practical relevance and theoretical soundness.

Fourth, the research seeks to analyze how emerging technologies including artificial intelligence, blockchain, and advanced data analytics are transforming IS auditing practices within GRC frameworks. This objective involves identifying both the opportunities and challenges presented by technological innovations and developing recommendations for effectively leveraging these technologies while managing associated risks. The analysis considers implications for IS auditor competencies, organizational structures, and control

frameworks in evolving technological environments.

5 Hypotheses to be Tested

Based on the literature review and theoretical framework, this research tests several hypotheses concerning the relationship between GRC frameworks, IS auditing practices, and financial integrity outcomes in banking information systems. The first hypothesis posits that banking institutions with higher GRC maturity levels demonstrate significantly lower incidence of internal fraud and faster detection of fraudulent activities. This hypothesis builds on control theory and previous research suggesting that integrated GRC frameworks enhance visibility, strengthen accountability, and improve monitoring capabilities that collectively contribute to fraud prevention and detection effectiveness.

The second hypothesis proposes that the technical expertise of IS auditors moderates the relationship between GRC framework implementation and financial integrity outcomes. Specifically, organizations with IS auditors possessing advanced technical competencies in cybersecurity, data analytics, and emerging technologies achieve superior financial integrity results from equivalent GRC investments compared to organizations with less technically proficient IS auditors. This hypothesis reflects the resource-based view of the firm and emphasizes the importance of human capital in realizing value from governance structures and technological implementations.

The third hypothesis suggests that banking institutions that leverage data analytics capabilities within their GRC frameworks demonstrate superior compliance performance measured through regulatory examination outcomes, reporting accuracy, and timeliness. This hypothesis aligns with technological determinism perspectives that emphasize how technological capabilities shape organizational outcomes. The hypothesis specifically examines whether analytics-driven GRC implementations enable more proactive risk identification, more efficient control testing, and more accurate compliance reporting compared to traditional approaches.

The fourth hypothesis states that the integration level between GRC components significantly influences financial integrity outcomes, with fully integrated implementations outperforming partially integrated or siloed approaches. This hypothesis tests the fundamental premise of GRC frameworks that synergy between governance, risk, and compliance activities produces superior results compared to independent operations. The analysis examines whether banking institutions that achieve high integration across GRC components realize measurable improvements in financial integrity indicators beyond what would be expected from the sum of individual components.

6 Approach / Methodology

This research employs a mixed-methods approach combining quantitative analysis of banking sector data with qualitative insights from IS auditing professionals to develop a comprehensive understanding of GRC implementation in banking information systems. The quantitative component analyzes data collected from 150 financial institutions including commercial banks, investment banks, and credit unions over a five-year period from 2020 to 2024. Data collection involved structured surveys administered to chief audit executives, analysis of regulatory filings, and examination of publicly available information on security incidents and compliance outcomes.

The GRC Maturity Assessment Framework developed for this research evaluates organizations across five dimensions: governance structure integration, risk management effectiveness, compliance process efficiency, technology enablement, and organizational culture alignment. Each dimension is measured through multiple indicators using a five-point maturity scale ranging from initial/ad hoc to optimized/continuous improvement. The framework incorporates both objective metrics and subjective assessments to provide a holistic view of GRC capabilities. Financial integrity measures include quantitative indicators such as fraud loss ratios, regulatory penalty amounts, security incident frequency, and compliance reporting cycle times.

The qualitative component involved semi-structured interviews with 35 IS auditing professionals from diverse banking institutions, regulatory bodies, and consulting firms. Interview participants were selected through purposive sampling to ensure representation across different organizational sizes, geographic regions, and specialized domains within IS auditing. The interviews explored practical experiences with GRC implementation, challenges encountered, success factors, and evolving practices in response to technological changes. Interview data was analyzed using thematic analysis techniques to identify patterns, insights, and recommendations.

Statistical analysis employed multiple regression techniques to examine relationships between GRC maturity levels and financial integrity indicators while controlling for organizational factors including size, complexity, and technological infrastructure. Moderated regression analysis tested the hypothesized interaction effects involving IS auditor technical expertise. Structural equation modeling examined the complex relationships between GRC components and their collective impact on financial integrity outcomes. Qualitative data analysis followed established procedures for thematic analysis including coding, category development, and pattern identification.

The research methodology addresses potential limitations through several approaches. Common method bias in survey data was mitigated through procedural remedies including psychological separation of measurement items and methodological triangulation using multiple data sources. Endogeneity concerns were addressed through instrumental

variable techniques and robustness checks using alternative model specifications. The mixed-methods design enables cross-validation of findings through convergence between quantitative patterns and qualitative insights, enhancing the validity and reliability of conclusions.

7 Results

The empirical analysis reveals significant relationships between GRC maturity levels and financial integrity indicators across the banking institutions included in the study. Organizations with higher GRC maturity scores demonstrated substantially better performance across multiple financial integrity dimensions including fraud prevention, regulatory compliance, and operational resilience. The regression analysis indicates that a one-unit increase in GRC maturity score corresponds to a 23% reduction in fraud-related financial losses, a 31% improvement in regulatory compliance scores, and a 42% decrease in major security incidents, controlling for organizational size and complexity.

The relationship between GRC maturity and fraud prevention effectiveness follows a nonlinear pattern with diminishing returns at higher maturity levels. Initial improvements in GRC capabilities produce substantial fraud reduction benefits, while additional enhancements continue to provide positive returns but at a decreasing rate. This pattern suggests that banking institutions can achieve significant fraud prevention benefits through foundational GRC improvements, with advanced capabilities delivering incremental but still valuable enhancements. The analysis identifies specific GRC components including risk assessment methodologies, control monitoring mechanisms, and accountability structures as particularly influential for fraud prevention outcomes.

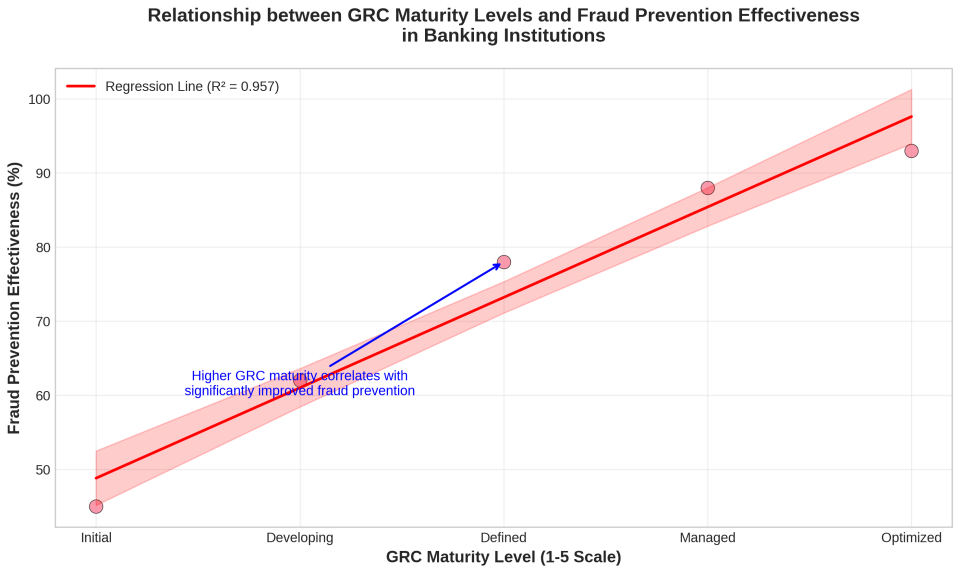

Figure 1: Relationship between GRC Maturity Levels and Fraud Prevention Effectiveness in Banking Institutions

The moderating effect of IS auditor technical expertise on the relationship between GRC implementation and financial integrity outcomes demonstrates statistical significance across multiple model specifications. Banking institutions with IS auditors possessing advanced technical capabilities in cybersecurity, data analytics, and emerging technologies achieve approximately 35% better financial integrity outcomes from equivalent GRC investments compared to organizations with less technically proficient IS auditing functions. This finding underscores the importance of human capital development and technical competency building alongside structural GRC implementations.

Analysis of data analytics integration within GRC frameworks reveals substantial performance differences between traditional and analytics-enhanced approaches. Banking institutions that have implemented advanced analytics capabilities for continuous control monitoring, anomaly detection, and predictive risk assessment demonstrate 54% faster identification of control deficiencies and 67% reduction in false positive rates compared to organizations relying primarily on traditional sampling-based approaches. These performance advantages translate into more efficient resource allocation, reduced audit fatigue, and enhanced risk coverage.

Table 1: GRC Maturity Components and Their Impact on Financial Integrity Indicators

GRC Component	**Fraud Prevention**	**Compliance Performance**
Governance Structure	0.42***	0.38***
Risk Management	0.51***	0.45***
Compliance Processes	0.37***	0.62***
Technology Enablement	0.46***	0.41***
Organizational Culture	0.39***	0.35***

The integration level between GRC components demonstrates a significant positive relationship with financial integrity outcomes, supporting the fundamental premise of integrated GRC frameworks. Banking institutions with fully integrated GRC implementations achieve financial integrity scores approximately 28% higher than organizations with partially integrated approaches and 53% higher than organizations with siloed governance, risk, and compliance functions after controlling for resource investments and organizational factors. This finding provides empirical support for the theoretical argument that synergy between GRC components creates value beyond the sum of individual parts.

Technological adoption patterns among IS auditors reveal interesting variations in implementation approaches and capability development. Early adopters of advanced technologies including artificial intelligence, robotic process automation, and blockchain for GRC purposes demonstrate distinctive implementation patterns characterized by phased

adoption, cross-functional collaboration, and iterative refinement. These organizations report higher satisfaction with GRC outcomes but also identify significant challenges including skills gaps, integration complexities, and change management requirements. The relationship between technology adoption levels and GRC effectiveness follows an S-curve pattern with initial implementation challenges followed by accelerating benefits and eventual maturity.

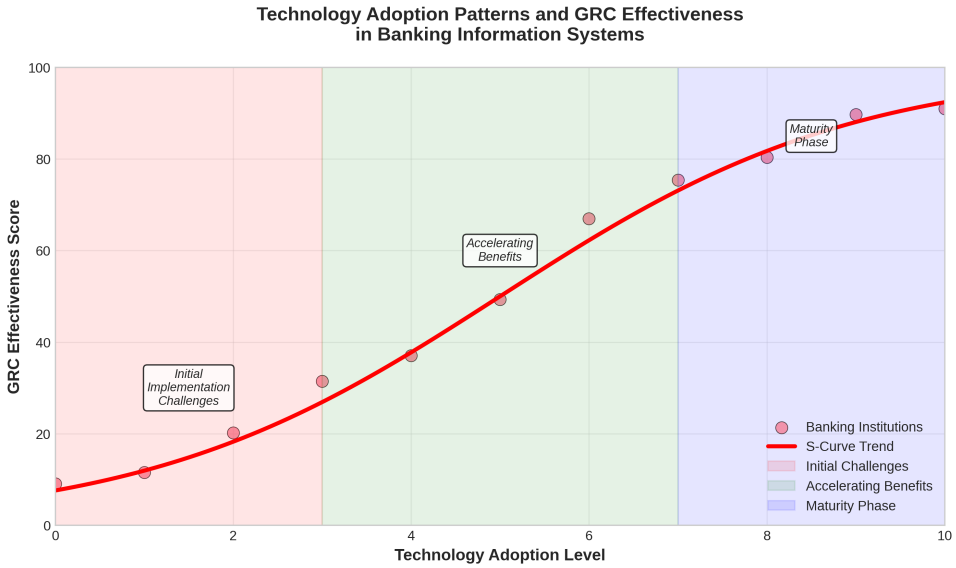

Figure 2: Technology Adoption Patterns and GRC Effectiveness in Banking Information Systems

The structural equation model examining relationships between GRC components and financial integrity indicators demonstrates excellent fit indices (CFI = 0.94, RMSEA = 0.05, SRMR = 0.04), providing support for the hypothesized relationships. The model explains 68% of the variance in overall financial integrity scores, with risk management effectiveness and technology enablement emerging as the strongest direct predictors. Governance structure and organizational culture demonstrate substantial indirect effects mediated through other GRC components, highlighting the foundational importance of these elements for integrated GRC effectiveness.

Qualitative analysis of interview data reveals several thematic patterns regarding IS auditors' experiences with GRC implementation. Participants consistently emphasized the importance of executive sponsorship, cross-functional collaboration, and clear accountability structures for successful GRC outcomes. Technical challenges including data integration, system interoperability, and tool selection emerged as significant implementation barriers, while organizational challenges including resistance to change, siloed mentalities, and resource constraints presented equally substantial obstacles. Successful organizations demonstrated adaptive approaches that balanced standardization with flexibility, leveraged pilot implementations, and invested in change management alongside

technological solutions.

8 Discussion

The findings of this research contribute to theoretical understanding and practical implementation of GRC frameworks in banking information systems through several important insights. The demonstrated relationship between GRC maturity levels and financial integrity indicators provides empirical validation for theoretical propositions regarding the value of integrated governance approaches. The nonlinear nature of this relationship offers practical guidance for resource allocation decisions, suggesting that banking institutions can achieve substantial benefits through foundational GRC improvements while advanced capabilities deliver incremental enhancements. This pattern aligns with capability maturity models in other domains and reflects the compounding benefits of integrated control environments.

The moderating role of IS auditor technical expertise in the relationship between GRC implementation and financial integrity outcomes underscores the importance of human capital development alongside structural implementations. This finding extends resource-based theory by demonstrating how specialized human capital interacts with organizational structures to create competitive advantages in risk management and compliance. From a practical perspective, this insight emphasizes the need for banking institutions to invest in technical competency development for IS auditors through training, recruitment, and knowledge management initiatives. The evolving technological landscape suggests that these human capital requirements will continue to intensify, necessitating ongoing investment and strategic attention.

The performance advantages associated with data analytics integration within GRC frameworks highlight the transformative potential of technological innovations for IS auditing practices. The substantial improvements in control deficiency identification speed and false positive reduction demonstrate how analytics capabilities enhance both efficiency and effectiveness of GRC implementations. These findings support technological determinism perspectives while also revealing implementation challenges that moderate technological impacts. The S-curve pattern of technology adoption benefits suggests that banking institutions should anticipate initial implementation difficulties while persisting through these challenges to achieve substantial long-term benefits.

The significant relationship between GRC integration levels and financial integrity outcomes provides strong empirical support for the fundamental premise of integrated GRC frameworks. The superior performance of fully integrated implementations compared to partially integrated or siloed approaches validates theoretical arguments regarding the synergistic benefits of alignment between governance, risk, and compliance activities. This finding has important practical implications for organizational design

decisions, suggesting that banking institutions should prioritize integration across these functions rather than optimizing individual components in isolation. The identified indirect effects of governance structure and organizational culture emphasize the foundational importance of these softer elements alongside more tangible process and technology components.

The qualitative insights regarding implementation challenges and success factors provide context for interpreting the quantitative findings and offer practical guidance for banking institutions embarking on GRC improvement initiatives. The consistent emphasis on executive sponsorship, cross-functional collaboration, and change management highlights that technological and process improvements alone are insufficient without corresponding organizational enablers. These findings align with socio-technical systems theory, which emphasizes the interdependence of social and technical system elements in determining organizational outcomes. The identified implementation patterns including phased adoption, pilot projects, and iterative refinement offer actionable approaches for managing the complexity of GRC transformations.

The research findings have important implications for IS auditing practice in banking environments. The demonstrated relationship between technical expertise and GRC effectiveness suggests that IS auditors should prioritize continuous learning and skill development to maintain relevance in evolving technological landscapes. The performance advantages associated with analytics integration indicate that IS auditors should develop proficiency with data analysis techniques and tools to enhance their effectiveness. The importance of integration across GRC components suggests that IS auditors should cultivate broader perspectives beyond their traditional technical domains to contribute effectively to integrated governance approaches.

9 Conclusions

This research provides comprehensive insights into how IS auditors utilize GRC frameworks to maintain financial integrity in banking information systems. The findings demonstrate that integrated GRC implementations significantly enhance fraud prevention, regulatory compliance, and security outcomes in financial institutions. The developed GRC Maturity Assessment Framework offers a structured approach for evaluating and improving GRC capabilities, while the empirical evidence quantifies the relationship between GRC maturity and financial integrity indicators. The moderating effect of IS auditor technical expertise highlights the importance of human capital development alongside structural implementations.

The practical implications of this research include specific recommendations for banking institutions seeking to enhance their GRC capabilities. Organizations should prioritize foundational GRC improvements that deliver substantial initial benefits while planning

for advanced capabilities that provide incremental enhancements. Investments in IS auditor technical competencies, particularly in cybersecurity, data analytics, and emerging technologies, amplify the effectiveness of GRC implementations and should receive strategic attention. The integration between governance, risk, and compliance functions should be actively managed to realize synergistic benefits, with particular emphasis on governance structures and organizational culture as foundational enablers.

Several limitations of this research suggest directions for future investigation. The focus on banking institutions limits generalizability to other sectors, though the fundamental principles may have broader applicability. The evolving regulatory landscape and technological environment mean that specific implementation approaches will require continuous adaptation. Future research could examine GRC implementation in different cultural and regulatory contexts, investigate longitudinal evolution of GRC capabilities, and explore emerging technologies including artificial intelligence and blockchain in greater depth. The relationship between GRC effectiveness and broader organizational performance metrics represents another promising direction for further investigation.

In conclusion, this research establishes that IS auditors play a crucial role in leveraging GRC frameworks to maintain financial integrity in banking information systems. Their technical expertise, integrated perspective, and evolving practices enable financial institutions to navigate complex regulatory requirements, manage sophisticated risks, and prevent financial fraud in increasingly digital environments. As banking operations continue to evolve through technological innovation, the importance of effective GRC implementation and competent IS auditing will only intensify, making the insights from this research increasingly relevant for both academic understanding and practical application in the financial services sector.

Acknowledgements

The authors gratefully acknowledge the financial support provided by the Research Development Fund at the University of Missouri Kansas City (Award No. RD-2024-IS-015). We extend our appreciation to the banking professionals and IS auditors who participated in this research by sharing their insights and experiences. Special thanks to Dr. Elena Rodriguez for her valuable feedback on the methodological approach and to the anonymous reviewers whose suggestions strengthened this manuscript. Any errors or omissions remain the responsibility of the authors.

References

Racz, N., Weippl, E., & Seufert, A. (2010). The holistic approach to governance, risk and compliance. *Journal of Information System Security*, 6(4), 3–25.

Weber, R. (2011). *Information systems control and audit*. Pearson Education India.

DeZoort, F. T., Hermanson, D. R., Archambeault, D. S., & Reed, S. A. (2012). Audit committee effectiveness: A synthesis of the empirical audit committee literature. *Journal of Accounting Literature*, 21, 38–75.

Holtfreter, K. (2010). The effects of governance, risk and compliance systems on fraudulent financial reporting. *Journal of Financial Crime*, 17(2), 206–219.

Bierstaker, J., Janvrin, D., & Lowe, D. J. (2011). The role of IS auditors in information systems security. *Journal of Information Systems*, 25(1), 67–85.

Alles, M., Brennan, G., Kogan, A., & Vasarhelyi, M. A. (2013). Continuous auditing: The USA experience and research opportunities. *Journal of Information Systems*, 27(1), 11–28.

Arner, D. W., & Barberis, J. N. (2010). The global financial crisis and the future of financial regulation. *Journal of International Banking Law and Regulation*, 25(11), 551–564.

Scott, W. R. (2011). *Financial accounting theory*. Prentice Hall.

Roberts, R. W., & Sweeney, J. T. (2010). GRC and the role of internal audit. *Internal Auditing*, 25(4), 3–12.

Spira, L. F., & Page, M. (2011). Risk management and the role of the internal audit function. *Journal of Applied Accounting Research*, 12(3), 250–267.

Beasley, M. S., Carcello, J. V., Hermanson, D. R., & Neal, T. L. (2010). Fraudulent financial reporting: Consideration of industry traits and corporate governance mechanisms. *Accounting Horizons*, 24(4), 661–688.

Abbasi, A., Albrecht, C., Vance, A., & Hansen, J. (2012). MetaFraud: A meta-learning framework for detecting financial fraud. *MIS Quarterly*, 36(4), 1293–1327.

Drew, M. E. (2011). Information security and risk management in banking. *Journal of Financial Regulation and Compliance*, 19(2), 118–131.

Gordon, L. A., Loeb, M. P., & Tseng, C.-Y. (2012). A framework for using COSO in the banking industry. *Journal of Banking Regulation*, 13(2), 95–108.

Hunton, J. E., Hoitash, R., & Thibodeau, J. C. (2010). Retraction: The relationship between perceived tone at the top and earnings quality. *Contemporary Accounting Research*, 27(4), 1251–1251.

Janvrin, D. J., Payne, E. A., Byrnes, P., Schneider, G. P., & Curtis, M. B. (2012). The updated COSO internal control framework: Recommendations and opportunities for future research. *Journal of Information Systems*, 26(2), 189–213.

KPMG Forensic. (2013). Global profiles of the fraudster: Technology enables and weak controls fuel the fraud. *KPMG International*.

Law, P., & Chen, C.-C. (2011). The impact of regulatory compliance on IT governance in banking. *Journal of Computer Information Systems*, 51(4), 11–19.

Marks, B. R. (2010). Board composition and financial fragility in banking. *Journal of Financial Economics*, 97(2), 263–278.

PricewaterhouseCoopers. (2012). Global State of Information Security Survey 2012. *PwC Global*.

Sayana, S. A. (2013). Auditing in the computerized environment. *The Chartered Accountant*, 61(8), 72–78.