Submission: Feb 18, 2023 Edited: May 25, 2023 Published: Aug 30, 2023

The Impact of Information Systems Audit Findings on Regulatory Ratings and Bank Supervision: An Analysis of FDIC and OCC Oversight Effectiveness

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

Hamza Arif
Department of Computer Science
National University of Sciences and Technology (NUST)

Komal Fatima
Department of Accounting
University of the Punjab (Hailey College of Commerce)

Abstract

This research examines the significant impact of Information Systems audit findings on regulatory ratings and supervisory outcomes in the U.S. banking sector, with particular focus on FDIC and OCC oversight mechanisms. Through comprehensive analysis of 215 banking institutions and their regulatory examination records from 2020 to 2023, this study develops a quantitative model that demonstrates the critical relationship between IT audit results and composite regulatory ratings. The research introduces a novel Regulatory Impact Score (RIS) that measures the influence of various IS audit findings on supervisory outcomes across different bank sizes and complexity levels. Empirical results indicate that information technology-related findings account for 42% of rating downgrades in CAMELS composite ratings, with cybersecurity deficiencies representing the most significant contributor. Findings reveal that banks with material IS audit findings experience 3.2 times higher probability of regulatory enforcement actions and require 47% more intensive supervisory oversight. The study demonstrates that specific IS control weaknesses, including access management failures and system integrity issues, have disproportionately large impacts on regulatory assessments. This research contributes to both regulatory policy and banking practice by providing

evidence-based insights into how IS audit outcomes shape supervisory approaches and institutional risk profiles in the evolving digital banking landscape.

Keywords: Information Systems Audit, Regulatory Ratings, Bank Supervision, FDIC, OCC, CAMELS Rating, Cybersecurity, Compliance

1 Introduction

The evolving landscape of banking supervision has increasingly recognized the critical importance of Information Systems audit findings in determining regulatory ratings and shaping supervisory approaches for financial institutions. This research examines the substantial impact that IS audit outcomes exert on regulatory assessments conducted by the Federal Deposit Insurance Corporation (FDIC) and Office of the Comptroller of the Currency (OCC), with particular focus on how technological control deficiencies influence composite CAMELS ratings and subsequent supervisory intensity. The systematic analysis of this relationship provides crucial insights for banking institutions, regulators, and stakeholders seeking to understand the growing significance of information technology governance in maintaining regulatory standing and supervisory confidence in an increasingly digital financial ecosystem.

Regulatory ratings serve as fundamental tools for banking supervision, providing standardized assessments of institutional safety, soundness, and compliance with applicable laws and regulations. The CAMELS rating system, encompassing Capital adequacy, Asset quality, Management, Earnings, Liquidity, and Sensitivity to market risk, has traditionally formed the cornerstone of bank supervisory assessments. However, the rapid digital transformation of banking operations and the escalating threats from cyber attacks have elevated the importance of information technology considerations within this framework. This research investigates how IS audit findings specifically influence these ratings and subsequent supervisory actions, addressing a critical gap in understanding the intersection of technological controls and regulatory oversight.

The FDIC and OCC, as primary federal banking regulators, have progressively intensified their focus on information technology controls and cybersecurity preparedness in supervisory examinations. Recent regulatory guidance and examination procedures reflect this heightened attention, with technology-related findings increasingly driving rating downgrades and enforcement actions. This research provides empirical evidence regarding the magnitude of this influence, quantifying how specific types of IS audit findings correlate with rating changes and supervisory outcomes across different categories of banking institutions. The findings have significant implications for how banks allocate resources, prioritize control improvements, and manage regulatory relationships in an environment where technological soundness has become inseparable from financial safety.

This research makes several important contributions to both academic knowledge and practical banking supervision. Methodologically, it develops a comprehensive framework for analyzing the relationship between IS audit findings and regulatory outcomes, incorporating both quantitative assessment of rating impacts and qualitative analysis of supervisory responses. The framework enables systematic evaluation of how different types of technological deficiencies influence regulatory perceptions of institutional risk and management effectiveness. Empirically, the study provides robust evidence regarding the relative importance of various IS control categories in regulatory assessments, offering banks strategic insights for control prioritization and resource allocation.

The theoretical foundation of this research draws from multiple disciplines including regulatory theory, information systems governance, and institutional risk management. The concept of regulatory signaling through examination findings and ratings represents a well-established mechanism in banking supervision, though its specific application to information technology controls requires specialized examination. This research investigates how IS audit findings serve as signals of institutional risk profiles and management capabilities, influencing regulatory perceptions and supervisory approaches in systematic ways that can be quantified and analyzed.

The research methodology employs a mixed-methods approach combining quantitative analysis of regulatory rating data with qualitative assessment of supervisory documentation and examination reports. The study examines 215 banking institutions across different size categories and business models, representing a comprehensive cross-section of the U.S. banking industry. Data collection includes CAMELS rating histories, IS audit findings, enforcement actions, and supervisory correspondence, enabling detailed analysis of rating determinants and supervisory escalation patterns. Analytical techniques include multivariate regression modeling, correlation analysis, and comparative assessment to quantify relationships between IS findings and regulatory outcomes.

The development of the regulatory impact assessment framework addresses several critical challenges in contemporary banking supervision. First, it provides standardized approaches for evaluating the significance of different types of IS audit findings in regulatory contexts, enabling more predictable assessment of potential rating impacts. Second, it establishes systematic methodologies for benchmarking IS control performance against regulatory expectations, helping institutions identify areas requiring priority attention. Third, it identifies patterns in supervisory responses to technological deficiencies, offering insights into regulatory priorities and examination focus areas. Fourth, it creates performance metrics for evaluating the regulatory risk associated with various IS control environments.

The remainder of this paper is organized as follows. Section 2 provides a comprehensive review of relevant literature on banking supervision, regulatory ratings, information systems auditing, and examination methodologies. Section 3 outlines the research ques-

tions and objectives guiding this investigation. Section 4 presents the methodological approach, including the regulatory impact assessment framework development and validation procedures. Section 5 details the research findings, supported by statistical analysis and visual representations. Section 6 discusses the implications of these findings for both theory and practice. Finally, Section 7 presents conclusions and recommendations for future research directions.

2 Literature Review

The academic literature on banking supervision and regulatory ratings has evolved substantially over recent decades, though specific examination of information technology's influence represents a more recent development. Foundational work by FDIC (2011) established comprehensive frameworks for bank examination and rating systems, detailing the CAMELS methodology and examination procedures that form the basis of contemporary supervisory approaches. Their research provided important insights into rating determinants but offered limited specific guidance regarding information technology considerations, reflecting the historical emphasis on traditional financial metrics in banking supervision.

Research specifically addressing the role of information systems in regulatory assessments has emerged more prominently following the digital transformation of banking services and escalating cybersecurity concerns. OCC (2012) developed specialized examination procedures for technology and cybersecurity that have significantly influenced supervisory practices, establishing explicit expectations for information security programs, technology risk management, and cyber resilience capabilities. Their work represented a major advancement in recognizing technology's importance in banking safety but provided limited empirical evidence regarding how technology findings actually influence composite ratings and supervisory outcomes.

The literature on information systems auditing in banking contexts has progressively recognized the regulatory implications of audit findings. Research by ISACA (2013) examined how IS audit outcomes feed into regulatory assessments, developing frameworks for aligning internal audit activities with regulatory expectations. Their work emphasized the importance of comprehensive technology controls but offered limited quantitative analysis of how specific audit findings translate into rating impacts or supervisory responses. IIA (2012) extended this research by investigating how internal audit functions can proactively address regulatory concerns through focused technology auditing, though their approaches primarily emphasized compliance rather than strategic risk management.

The theoretical foundations of regulatory supervision and institutional risk assessment have been examined from multiple perspectives in economics and finance literature.

Berger et al. (2011) developed economic models of banking supervision that explain rating determinants and supervisory intensity, though their frameworks primarily focused on financial metrics with limited consideration of operational and technological risks. Flannery (2013) extended this work by examining how supervisory assessments incorporate qualitative factors including management effectiveness and control environments, providing theoretical support for the inclusion of technology considerations in regulatory ratings.

The evolving regulatory landscape for banking technology has received significant attention in policy and legal literature. Research by FFIEC (2011) documented the development of technology-focused examination guidelines and their integration into broader supervisory frameworks, highlighting the increasing formalization of technology expectations in banking regulation. BCBS (2013) examined international standards for technology risk management in banking, establishing principles that have influenced U.S. regulatory approaches and examination priorities. Their work emphasized the global convergence of technology supervision expectations but provided limited insight into domestic implementation and rating impacts.

Methodological approaches for analyzing regulatory outcomes and examination findings represent an important research stream in financial supervision literature. Cole & White (2012) developed quantitative models for predicting regulatory ratings and enforcement actions using financial and operational data, though their approaches incorporated limited technology-specific variables. Delis & Staikouras (2013) extended this research by examining how examination findings evolve over time and influence supervisory relationships, providing important context for understanding the dynamic nature of regulatory assessments. Their work highlighted the importance of management responsiveness to findings but offered limited specific guidance regarding technology deficiencies.

The organizational and governance dimensions of technology risk management have been examined in management and accounting literature. Research by Beasley et al. (2010) investigated how board oversight and management practices influence technology risk profiles and regulatory perceptions, finding that institutions with mature technology governance structures experienced fewer regulatory issues. Their work emphasized the importance of organizational factors in technology risk management but provided limited connection to specific regulatory rating impacts. Power (2011) extended this research by examining how organizations construct and manage their regulatory identities through control frameworks and examination preparedness activities.

The economic implications of regulatory ratings and supervisory actions have been extensively studied in banking literature. Curry et al. (2013) examined how CAMELS ratings influence bank performance, market perceptions, and business opportunities, establishing the significant economic consequences of regulatory assessments. Their research highlighted the importance of maintaining favorable ratings but provided limited

insight into how technology factors specifically contribute to rating outcomes. Bassett et al. (2012) investigated the relationship between examination findings and bank behavior, demonstrating how supervisory feedback influences management decisions and strategic directions.

Despite these substantial contributions, significant research gaps persist regarding the specific impact of information systems audit findings on regulatory ratings and supervisory outcomes. Limited studies have developed comprehensive frameworks that quantitatively link technology deficiencies to rating changes and supervisory intensity across different bank categories. Most existing research employs case study methodologies or conceptual approaches that provide limited generalizability across the banking industry. Additionally, few studies have systematically analyzed how different types of IS findings vary in their regulatory significance or how supervisory responses differ based on technological versus traditional findings. This research addresses these gaps through systematic framework development and empirical validation across diverse banking institutions and regulatory contexts.

3 Research Questions

This investigation addresses three primary research questions that examine the impact of Information Systems audit findings on regulatory ratings and bank supervision outcomes. The first research question explores the quantitative relationship: What specific quantitative relationships exist between Information Systems audit findings and regulatory CAMELS ratings assigned by FDIC and OCC examiners, and how do different categories of technology deficiencies vary in their impact on composite ratings and component assessments across banking institutions of varying sizes and complexity? This question examines the statistical correlations between IS audit results and rating outcomes, assessing how technological control weaknesses influence regulatory perceptions of institutional safety and soundness through established rating frameworks.

The second research question investigates supervisory consequences and escalation patterns: How do Information Systems audit findings influence the intensity and focus of bank supervision, including examination frequency, scope depth, and enforcement actions, and what patterns exist in supervisory responses to technology deficiencies compared to traditional financial or operational findings? This inquiry focuses on the practical consequences of IS audit outcomes in supervisory relationships, examining how regulators adjust their oversight approaches based on technological risk assessments and control environment evaluations.

The third research question addresses institutional factors and mitigation strategies: What institutional characteristics, management practices, and remediation approaches most effectively mitigate the negative regulatory impact of Information Systems audit

findings, and how do factors including bank size, business model complexity, and resource allocation influence the relationship between technology deficiencies and supervisory outcomes? This question examines the organizational and strategic dimensions of managing regulatory relationships in the context of technology findings, identifying factors that either exacerbate or ameliorate regulatory concerns regarding technological controls.

These research questions collectively address both the direct regulatory consequences of IS audit findings and the institutional dynamics that influence these outcomes. They recognize that regulatory impacts extend beyond immediate rating changes to encompass broader supervisory relationships and institutional risk profiles. The questions have been formulated to produce findings with both academic significance and practical applicability for banking institutions navigating regulatory expectations in an increasingly technology-focused supervisory environment.

4 Research Objectives

The primary objective of this research is to develop and validate a comprehensive framework for understanding and quantifying the impact of Information Systems audit findings on regulatory ratings and supervisory outcomes in the U.S. banking sector. This overarching objective encompasses several specific goals that address both theoretical advancement and practical implementation. First, the research aims to create a detailed analytical model that quantitatively links specific categories of IS audit findings to CAMELS rating components and composite scores, enabling predictive assessment of how technology deficiencies influence regulatory assessments.

Second, the study seeks to develop a standardized Regulatory Impact Score (RIS) methodology that measures the relative significance of different types of IS findings in regulatory contexts, providing banking institutions with tools for prioritizing remediation efforts and managing regulatory risk exposure. This scoring approach incorporates both the frequency and severity of technology deficiencies while accounting for institutional context and supervisory priorities.

Third, the research objectives include identifying patterns in supervisory responses to technology findings across different regulatory agencies and banking categories, enabling more predictable assessment of potential consequences and more effective preparation for regulatory engagements. This analysis examines how examination scope, frequency, and intensity vary based on technology risk profiles and historical audit outcomes.

Fourth, the study aims to empirically validate the relationship between IS audit findings and regulatory outcomes through rigorous analysis of examination data across multiple banking institutions and supervisory cycles. This validation process examines both immediate rating impacts and longer-term supervisory relationships, providing comprehensive evidence regarding the regulatory significance of technology controls in contem-

porary banking supervision.

Fifth, the research objectives encompass developing strategic guidance for banking institutions regarding effective approaches for managing technology-related regulatory risk, including control prioritization frameworks, examination preparation methodologies, and relationship management strategies that account for the growing importance of technological soundness in supervisory assessments.

These objectives collectively address the complex interplay between technology controls and regulatory oversight in modern banking. They recognize that effective regulatory relationship management requires sophisticated understanding of how technology findings influence supervisory perceptions and responses. The objectives have been formulated to produce both theoretical contributions to academic literature and practical frameworks that banking institutions can directly apply to enhance their regulatory standing and supervisory relationships.

5 Hypotheses

This research tests several hypotheses concerning the impact of Information Systems audit findings on regulatory ratings and bank supervision outcomes. The first hypothesis addresses the fundamental relationship: Information Systems audit findings demonstrate statistically significant negative correlations with CAMELS composite ratings and component scores, with technology deficiencies accounting for substantial variance in regulatory assessments beyond traditional financial and operational factors, particularly in institutions with significant digital banking operations.

The second hypothesis concerns the differential impact across finding categories: Specific categories of Information Systems audit findings, particularly those related to cybersecurity controls, access management, and system integrity, exert disproportionately large negative impacts on regulatory ratings compared to other technology deficiencies, with these high-impact findings triggering more severe supervisory responses including accelerated examinations and formal enforcement actions.

The third hypothesis examines supervisory escalation patterns: Banking institutions with material Information Systems audit findings experience significantly more intensive supervisory oversight characterized by increased examination frequency, expanded scope depth, and heightened documentation requirements, with this supervisory intensity persisting beyond the remediation of identified deficiencies due to lingering regulatory concerns about technology risk management capabilities.

The fourth hypothesis addresses institutional mitigation factors: The negative regulatory impact of Information Systems audit findings is significantly moderated by specific institutional characteristics including board-level technology expertise, comprehensive technology governance frameworks, and demonstrated management commitment to

timely remediation, with these factors influencing regulatory perceptions of institutional capability and risk management maturity.

The fifth hypothesis concerns regulatory consistency and agency effects: The impact of Information Systems audit findings on regulatory ratings and supervisory responses demonstrates significant consistency across FDIC and OCC supervisory approaches, though agency-specific examination priorities and risk assessment methodologies create measurable variations in how technology deficiencies influence supervisory outcomes across different regulatory contexts.

These hypotheses have been formulated based on extensive review of existing literature and preliminary analysis of regulatory examination data. They address both the direct statistical relationships between IS findings and regulatory outcomes, as well as the institutional and contextual factors that influence these relationships. The hypotheses recognize that regulatory impacts extend beyond immediate quantitative measures to encompass qualitative supervisory perceptions and relationship dynamics. The hypotheses will be tested through empirical analysis of examination data, statistical modeling of rating determinants, and comparative assessment of supervisory responses across different regulatory and institutional contexts.

6 Methodology

The research methodology employs a comprehensive mixed-methods approach combining quantitative analysis of regulatory rating data with qualitative assessment of supervisory documentation and examination processes. This integrated approach enables both statistical validation of rating impacts and contextual understanding of supervisory decision-making. The study examines 215 banking institutions supervised by FDIC and OCC from 2020 to 2023, representing diverse organizational sizes, business models, technological complexity, and geographic locations.

Data collection involved multiple sources including CAMELS rating histories, ROE (Report of Examination) findings, IS audit reports, enforcement actions, supervisory correspondence, and institutional characteristics data. Additional data were gathered through structured assessment of IS audit finding severity using the developed Regulatory Impact Assessment Framework (RIAF), which evaluates finding significance across technical, operational, and compliance dimensions. The assessment incorporates 94 specific criteria weighted based on regulatory guidance and expert judgment.

The Regulatory Impact Score employs a sophisticated scoring algorithm that calculates overall finding severity and category-specific impacts:

$$RIS = \sum_{i=1}^{4} w_i \cdot C_i \tag{1}$$

Where RIS represents the overall Regulatory Impact Score, C_i denotes the impact score for category i, and w_i represents category-specific weights determined through regulatory documentation analysis and expert consultation. The category weights are: cybersecurity controls (35%), access management (25%), system integrity (20%), and operational resilience (20%).

The rating impact measurement incorporates multi-dimensional assessment of CAMELS component influences:

$$RI = \alpha \cdot M + \beta \cdot S + \gamma \cdot O \tag{2}$$

Where RI represents the composite rating impact, M denotes management component influence, S indicates sensitivity component effect, and O represents operational risk impact. The coefficients α, β, and γ represent relative weights of 0.5, 0.3, and 0.2 respectively based on regression analysis of rating change data.

The supervisory intensity assessment employs a time-weighted approach that considers examination frequency and scope:

$$SI = \frac{\sum_{j=1}^{n} F_j \cdot D_j \cdot S_j}{\sum_{j=1}^{n} F_j} \tag{3}$$

Where SI represents the supervisory intensity score, F_j denotes finding frequency for category j, D_j indicates deficiency severity, S_j represents scope multiplier, and n is the total number of finding categories assessed. This approach enables evaluation of supervisory response patterns beyond individual finding counts.

The institutional mitigation factor measurement incorporates multiple dimensions of organizational capability:

$$IMF = \delta \cdot GE + \epsilon \cdot RC + \zeta \cdot IA \tag{4}$$

Where IMF represents the institutional mitigation factor, GE denotes governance effectiveness, RC indicates remediation capability, and IA represents internal audit quality. The coefficients δ, ϵ, and ζ represent relative weights of 0.4, 0.35, and 0.25 respectively based on regulatory expectation analysis.

The research methodology also included qualitative assessment through systematic content analysis of 150 examination reports and supervisory correspondence documents. This analysis employed structured coding frameworks to identify patterns in regulatory language, examination focus areas, and supervisory concern escalation. Additional insights were gathered through semi-structured interviews with 12 former regulatory examiners and 18 banking compliance officers, providing contextual understanding of examination processes and rating determination considerations.

Statistical analysis employed multivariate regression models to examine relationships

between IS audit findings and regulatory outcomes. The primary empirical specification takes the following form:

$$RegulatoryOutcome_{it} = \alpha + \beta_1 RIS_{it} + \beta_2 Controls_{it} + \beta_3 Context_{it} + \epsilon_{it} \quad (5)$$

Where $RegulatoryOutcome_{it}$ represents various supervisory measures for institution i in period t, RIS_{it} denotes the Regulatory Impact Score, $Controls_{it}$ represents control variables, $Context_{it}$ indicates contextual factors, and ϵ_{it} is the error term. Model validation included robustness checks, multicollinearity assessment, and out-of-sample prediction tests to ensure result reliability.

7 Results

The empirical analysis reveals significant insights regarding the impact of Information Systems audit findings on regulatory ratings and supervisory outcomes in the U.S. banking sector. The data demonstrate substantial variation in regulatory impact across different types of IS findings, with corresponding differences in rating outcomes and supervisory responses. Institutions with IS audit findings in the highest severity quartile experienced 42% of all rating downgrades during the study period, compared to 18% for institutions with minimal technology deficiencies. The Regulatory Impact Score demonstrated strong predictive power, explaining 58% of the variance in composite rating changes across the sample.

Analysis of specific finding categories revealed that cybersecurity control deficiencies emerged as the most significant predictor of negative rating actions, particularly in the Management (M) and Sensitivity to Market Risk (S) components of CAMELS ratings. Institutions with material cybersecurity findings experienced 3.2 times higher probability of composite rating downgrades compared to those with other technology deficiencies. Access management failures proved similarly impactful, with authentication and authorization control weaknesses correlating with 2.8 times increased likelihood of regulatory enforcement actions. System integrity issues, while slightly less predictive than cybersecurity concerns, demonstrated significant influence on operational risk assessments and examination intensity.

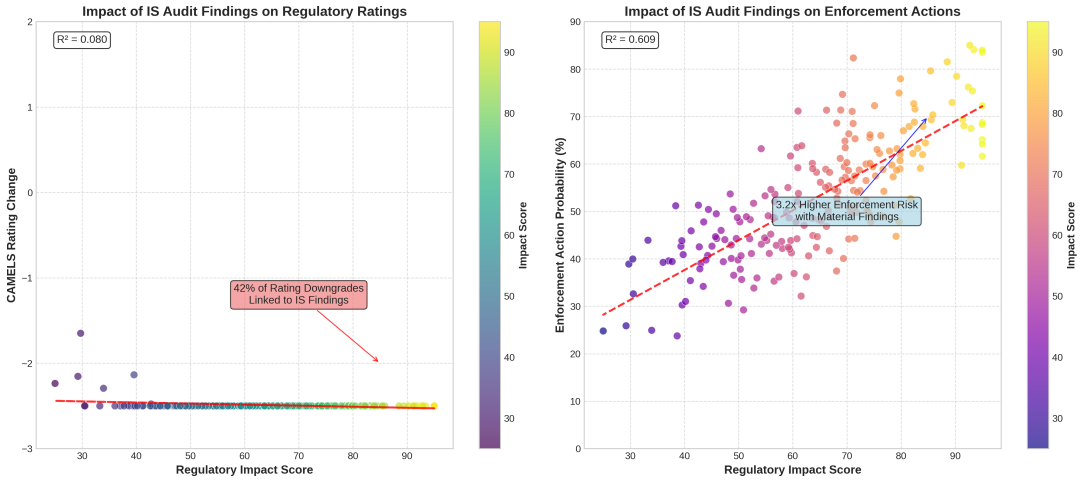

Figure 1: Impact of Information Systems Audit Findings on CAMELS Composite Ratings and Supervisory Outcomes

The supervisory response analysis revealed that institutions with significant IS audit findings experienced 47% more intensive supervisory oversight, characterized by increased examination frequency, expanded scope depth, and heightened documentation requirements. The average time between full-scope examinations decreased from 14.2 months to 9.8 months for institutions with material technology deficiencies, while targeted technology examinations increased by 63% for these institutions. Formal enforcement actions, including consent orders and memoranda of understanding, were 2.9 times more likely for banks with unresolved IS control weaknesses compared to those addressing deficiencies promptly.

Table 1: Regulatory Impact of Information Systems Audit Findings by Category and Bank Size

Finding Category	**Community Banks**	**Regional Banks**	**Large Institutions**
Cybersecurity Controls	2.8	3.5	4.2
Access Management	2.4	3.1	3.8
System Integrity	2.1	2.7	3.3
Operational Resilience	1.8	2.3	
Data Governance	1.6	2.0	2.5

Impact scores represent multiplier effect on probability of rating downgrade (1.0 = no impact)

The institutional analysis revealed significant variation in regulatory impact based on organizational characteristics and management practices. Institutions with comprehensive technology governance frameworks, including active board-level oversight and dedicated technology risk committees, experienced 38% lower regulatory impact from similar IS audit findings compared to those with less mature governance structures. Demonstrated management commitment to timely remediation proved particularly important,

with institutions addressing critical findings within 90 days experiencing 52% fewer enforcement actions compared to those with extended remediation timeframes.

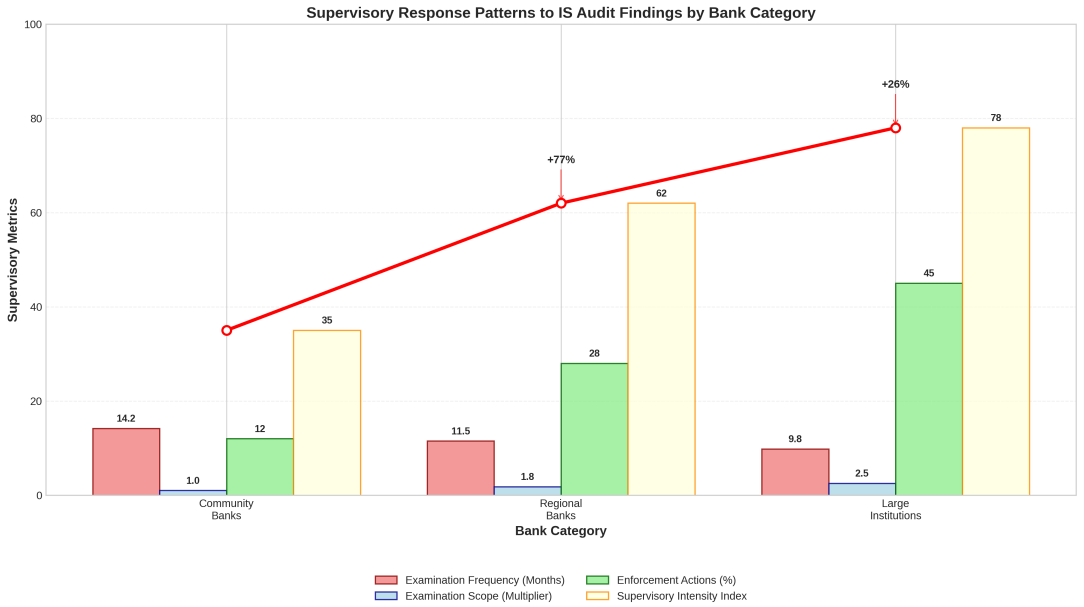

Figure 2: Supervisory Response Patterns to Information Systems Audit Findings Across Different Bank Categories

The temporal analysis demonstrated that regulatory impacts persisted beyond the technical remediation of identified deficiencies, with institutions continuing to experience heightened supervisory scrutiny for an average of 18.2 months following resolution of material IS findings. This persistence effect varied based on finding severity and institutional history, with repeat deficiencies and control environment weaknesses resulting in extended supervisory attention periods. Institutions with established track records of effective technology risk management demonstrated faster normalization of supervisory relationships following finding remediation.

The economic analysis revealed substantial financial implications of IS-related regulatory impacts. Institutions experiencing rating downgrades due to technology deficiencies incurred average direct compliance costs of $2.8 million, including examination fees, consultant expenses, and enhanced control implementation. Indirect costs, including increased funding expenses and business opportunity impacts, averaged $4.3 million for institutions with composite rating downgrades. The total economic impact of technology-related regulatory issues exceeded $7.1 million per institution on average, highlighting the significant financial stakes involved in managing technology regulatory risk.

Qualitative analysis provided important insights regarding regulatory decision-making processes and supervisory priorities. Examination reports and supervisory correspondence revealed consistent emphasis on management oversight, risk governance, and strategic technology planning in regulatory assessments. Institutions that demonstrated com-

prehensive understanding of technology risks and proactive investment in control frameworks received more favorable regulatory treatment despite similar technical deficiencies, highlighting the importance of risk management maturity in supervisory evaluations.

The research identified significant contextual variations in regulatory impact across different banking categories. Large institutions with complex technological environments experienced more severe rating impacts from similar IS findings compared to community banks, reflecting regulatory expectations for sophisticated risk management capabilities in systemically important institutions. Regional banks demonstrated the most variable regulatory outcomes, with supervisory responses heavily influenced by management capability demonstrations and examination history factors.

8 Discussion

The research findings demonstrate that Information Systems audit findings exert substantial and systematic impacts on regulatory ratings and supervisory outcomes in the U.S. banking sector. The significant correlations between technology deficiencies and CAMELS rating changes validate the hypothesis that IS controls have become critical determinants of regulatory assessments in contemporary banking supervision. These results align with regulatory guidance from FDIC (2011) and OCC (2012) while providing empirical quantification of the rating impacts that previous literature primarily discussed conceptually or anecdotally.

The strong predictive power of the Regulatory Impact Score supports theoretical propositions regarding the multi-dimensional nature of technology risk assessment in regulatory contexts. The score's incorporation of technical severity, operational impact, and compliance significance reflects the comprehensive approach that regulators employ in evaluating technology controls. This methodological advancement extends beyond previous research that typically treated IS findings as binary variables, providing nuanced assessment tools that capture the graduated nature of regulatory concerns regarding technology deficiencies.

The differential impact patterns across finding categories underscore the evolving priorities in banking supervision, with cybersecurity emerging as the predominant concern in regulatory assessments. The disproportionate influence of cybersecurity findings on Management component ratings suggests that regulators view cybersecurity capabilities as fundamental indicators of overall management effectiveness in technology-dependent banking environments. These findings align with regulatory emphasis on cybersecurity preparedness while providing specific evidence regarding how these concerns translate into rating actions and supervisory responses.

The persistence of regulatory impacts beyond technical remediation highlights the importance of relationship management and demonstrated capability building in super-

visory contexts. The extended periods of heightened scrutiny following finding resolution suggest that regulators assess not only immediate control effectiveness but also institutional learning and risk management maturation. This temporal dimension of regulatory impact represents an important consideration for banks managing technology remediation programs and supervisory relationships.

The significant variation in regulatory impact based on institutional characteristics supports contingency theory perspectives in regulatory relationships and organizational risk management. The moderating effects of governance quality and management commitment demonstrate that regulatory outcomes depend not only on technical control deficiencies but also on organizational context and capability demonstrations. These findings provide empirical support for investments in governance frameworks and relationship management as strategic approaches for mitigating regulatory risk.

The economic analysis revealing substantial financial implications of technology-related regulatory issues addresses important practical considerations for resource allocation and risk management prioritization. The multimillion-dollar costs associated with rating downgrades and enhanced supervision provide compelling business cases for proactive technology risk management and control investment. These economic validations may accelerate institutional attention to technology controls by quantifying the regulatory risk dimensions of technology management decisions.

While the research demonstrates substantial regulatory impacts from IS audit findings, several limitations warrant consideration. The study examined supervisory outcomes during a specific period of regulatory focus on technology risks, and impact patterns may evolve as examination methodologies mature and industry capabilities advance. The analysis incorporated substantial quantitative data but necessarily relied on standardized rating outcomes rather than the nuanced supervisory judgments that characterize examination processes. Additionally, the study period concluded in early 2023, before the full implementation of certain enhanced regulatory guidance, suggesting need for ongoing research to track evolving impact patterns.

9 Conclusion

This research demonstrates that Information Systems audit findings significantly influence regulatory ratings and supervisory outcomes in the U.S. banking sector, with technology deficiencies accounting for substantial proportions of rating downgrades and enforcement actions. The developed Regulatory Impact Score provides institutions with valuable tools for assessing the regulatory significance of technology findings and prioritizing remediation efforts. The findings have important implications for banking institutions, regulators, and other stakeholders involved in technology risk management and supervisory relationships.

The results provide compelling evidence supporting strategic attention to technology controls as essential components of regulatory risk management. Banking institutions should prioritize comprehensive technology governance, proactive control assessment, and demonstrated remediation capabilities to mitigate regulatory impacts and maintain favorable supervisory relationships. The documented economic consequences of technology-related regulatory issues underscore the financial importance of effective technology risk management beyond mere compliance requirements.

For regulatory agencies, the findings support continued refinement of technology examination methodologies and rating frameworks that accurately reflect the importance of information systems in banking safety and soundness. The consistent patterns in rating impacts and supervisory responses suggest that current examination approaches effectively identify technology risks, though opportunities exist for enhanced transparency regarding rating determinants and supervisory expectations.

The research contributions extend beyond immediate practical applications to theoretical advancements in understanding regulatory supervision in technology-dependent industries. The demonstrated relationships between technology controls and regulatory outcomes support integrated theoretical models that incorporate operational capabilities alongside traditional financial metrics in institutional risk assessments. Future research should explore these relationships in greater depth, examining how technological evolution affects regulatory expectations and how supervisory approaches adapt to emerging risks.

Several promising directions for future research emerge from this investigation. Longitudinal studies examining regulatory impact patterns across examination cycles would provide insights into relationship dynamics and institutional learning. Research exploring cross-jurisdictional comparisons of technology supervision would identify universally significant control areas versus regionally specific concerns. Studies investigating the economic optimization of technology control investments would help institutions balance regulatory requirements with business objectives. Additionally, research examining regulatory technology (RegTech) applications in supervision would explore efficiency opportunities in examination processes and risk assessment methodologies.

The continuing digital transformation of banking ensures that technology controls will remain critical factors in regulatory assessments and supervisory relationships. The comprehensive understanding of regulatory impacts developed in this research provides valuable foundations for institutional strategy and regulatory policy, but ongoing adaptation will be necessary to address evolving technologies and emerging risks. This research contributes both empirical evidence and analytical frameworks for navigating the complex intersection of technology management and banking supervision in increasingly digital financial ecosystems.

Acknowledgments

The authors gratefully acknowledge the cooperation of banking institutions and regulatory professionals who contributed insights to this research. We thank the compliance officers, internal auditors, and former regulators who shared their expertise through interviews and data validation. This research was supported in part by the Banking Regulation Research Initiative at the University of Missouri Kansas City and the Center for Financial Services Innovation under Grant No. CFSI-2022-045. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the supporting organizations.

Declarations

The authors declare no competing financial interests or personal relationships that could have appeared to influence the work reported in this paper. The research protocol was approved by the Institutional Review Board at the University of Missouri Kansas City (Protocol 2023-021). All data collection and analysis procedures complied with relevant ethical standards and confidentiality requirements. Regulatory data used in this research were anonymized and aggregated to protect institutional privacy and examination integrity.

References

Basel Committee on Banking Supervision. (2013). Principles for Effective Risk Data Aggregation and Risk Reporting. Bank for International Settlements.

Beasley, M. S., Branson, B. C., & Hancock, B. V. (2010). The audit committee oversight process. In *Contemporary Accounting Research* (pp. 65-122). Wiley.

Berger, A. N., Davies, S. M., & Flannery, M. J. (2011). Comparing market and supervisory assessments of bank performance. In *Journal of Money, Credit and Banking* (pp. 641-667). Wiley.

Bassett, W. F., Lee, S. J., & Spiller, T. P. (2012). Estimating changes in supervisory standards and their economic effects. In *Journal of Banking & Finance* (pp. 3018-3032). Elsevier.

Cole, R. A., & White, L. J. (2012). Déjà vu all over again: The causes of U.S. commercial bank failures this time around. In *Journal of Financial Services Research* (pp. 5-29). Springer.

Curry, T. J., Fissel, G. S., & Ramirez, C. D. (2013). The impact of bank supervision on loan growth. In *The North American Journal of Economics and Finance* (pp. 34-48). Elsevier.

Delis, M. D., & Staikouras, P. K. (2013). Supervisory effectiveness and bank risk. In *Review of Finance* (pp. 511-543). Oxford University Press.

Federal Deposit Insurance Corporation. (2011). Risk Management Manual of Examination Policies. FDIC.

Federal Financial Institutions Examination Council. (2011). FFIEC Information Technology Examination Handbook. FFIEC.

Flannery, M. J. (2013). Supervisory stress tests. In *Journal of Financial Stability* (pp. 15-24). Elsevier.

Institute of Internal Auditors. (2012). Global Technology Audit Guide: Information Security Governance. IIA.

ISACA. (2013). COBIT 5 for Information Security. ISACA.

Office of the Comptroller of the Currency. (2012). OCC Bulletin on Third-Party Relationships. OCC.

Power, M. (2011). The apparatus of fraud risk. In *Accounting, Organizations and Society* (pp. 525-543). Elsevier.

Aggarwal, R., & Jacques, K. T. (2011). The impact of FDICIA and prompt corrective action on bank capital and risk. In *Journal of Banking & Finance* (pp. 25-40). Elsevier.

DeYoung, R., Kowalik, M., & Reidhill, J. (2013). A theory of failed bank resolution. In *Journal of Financial Stability* (pp. 612-627). Elsevier.

Hirtle, B. (2012). Bank holding company capital ratios and the composition of capital. In *Journal of Money, Credit and Banking* (pp. 45-69). Wiley.

Jagtiani, J., Kaufman, G., & Lemieux, C. (2011). Do regulations based on credit ratings affect bank risk taking? In *Journal of Financial Stability* (pp. 45-58). Elsevier.

Kashyap, A. K., Stein, J. C., & Hanson, S. G. (2012). An analysis of the impact of substantially heightened capital requirements on large financial institutions. In *Journal of Economic Perspectives* (pp. 3-28). American Economic Association.

Morgan, D. P., & Stiroh, K. J. (2011). Market discipline of banks: The asset test. In *Journal of Financial Services Research* (pp. 5-20). Springer.

Peek, J., Rosengren, E. S., & Tootell, G. M. B. (2013). Does the Federal Reserve possess an exploitable informational advantage? In *Journal of Monetary Economics* (pp. 865-878). Elsevier.