iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

IT RISK AUDIT AND REGULATORY COMPLIANCE IN A CHALLENGING DIGITAL ENVIRONMENT: AN EMPIRICAL APPRAISAL

Olukayode Sorunke, CFE, CC, CySA+, CISA, CISM
Principal Consultant/ Senior Researcher
International CyberAnalytics Consulting Group, Arlington, Texas
Email: Osorun1@wgu.edu

ABSTRACT
The rapid digital transformation of organizations, driven by cloud computing, artificial intelligence (AI), remote work infrastructures, and extensive system interconnectivity, has significantly intensified exposure to information technology (IT) risks. At the same time, regulatory expectations concerning cybersecurity, data protection, and technology governance have expanded across jurisdictions.
This study empirically examines the relationship between IT risk audit maturity and regulatory compliance effectiveness in a challenging digital environment. Using a mixed-methods design, quantitative data were collected through a survey of 162 IT auditors, governance, risk, and compliance (GRC) professionals, and cybersecurity managers across regulated industries, complemented by qualitative interviews with senior audit practitioners.
Regression and correlation analyses reveal a strong, positive, and statistically significant relationship between IT risk audit maturity and regulatory compliance effectiveness. The findings demonstrate that continuous auditing, audit automation, and strong alignment with governance significantly enhance compliance outcomes. The study provides empirical evidence to the IT audit and compliance literature and offers actionable recommendations for organizations seeking to strengthen regulatory compliance in digitally complex environments.

Keywords:
IT Risk Audit, Regulatory Compliance, Digital Risk, Cybersecurity Governance, Empirical Study

1. INTRODUCTION

Digital technologies have become central to organizational operations, enabling efficiency, scalability, and innovation. However, this digital dependence has also expanded the risk landscape, exposing organizations to cyber threats, system failures, data breaches, and regulatory non-compliance (Almeida et al., 2023). Regulators have responded with increasingly stringent requirements, such as the General Data Protection Regulation (GDPR), the Sarbanes–Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI-DSS), and emerging artificial intelligence governance frameworks.
IT risk auditing serves as a critical assurance mechanism that evaluates whether organizations effectively identify, assess, and mitigate technology-related risks while maintaining compliance with regulatory obligations (ISACA, 2024). Yet, traditional audit models often struggle to keep pace with agile development, cloud-native systems, and continuous deployment environments. Despite extensive conceptual discussion, empirical evidence linking IT risk audit practices to regulatory compliance outcomes remains limited. This study addresses this gap by empirically examining the influence of IT risk audit maturity on regulatory compliance effectiveness.

2. LITERATURE REVIEW

2.1 Evolution of IT Risk Auditing in the Digital Era

IT risk auditing has undergone a significant transformation over the past two decades, evolving from a traditional, control-centric assurance function into a strategic, risk-oriented governance mechanism. Early IT audits primarily focused on general IT controls, access management, and system integrity. However, the rapid adoption of cloud computing, mobile technologies, artificial intelligence (AI), and platform-based architectures has expanded the scope and complexity of IT risks (Almeida et al., 2023; Kraus et al., 2023).

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

Recent studies emphasize that modern IT risk audits must adopt a dynamic, continuous approach to remain effective in digitally intensive environments (Bada & Nurse, 2022). The integration of continuous auditing, real-time monitoring, and data analytics enables auditors to identify emerging risks proactively rather than retrospectively. ISACA (2024) argues that organizations relying solely on periodic audits face heightened exposure to cyber incidents and compliance failures, particularly in environments characterized by rapid system changes and third-party dependencies.

Empirical evidence suggests that organizations with higher IT audit maturity demonstrate stronger risk visibility, faster remediation cycles, and improved alignment with enterprise risk management (ERM) frameworks (De Haes et al., 2023). These findings support the argument that IT risk auditing is no longer a support function but a critical component of organizational governance and strategic oversight.

2.2 Regulatory Compliance in a Complex Digital Environment

Regulatory compliance has become increasingly challenging due to the convergence of digital technologies, globalization, and sector-specific regulatory regimes. Regulations such as GDPR, SOX, HIPAA, PCI-DSS, and emerging AI governance frameworks impose stringent requirements on data protection, system security, and accountability (OECD, 2024). Failure to comply with these requirements can result in significant financial penalties, reputational damage, and operational disruptions.

Von Solms and Van Niekerk (2022) contend that most regulatory failures stem from weak information security governance rather than deliberate non-compliance. This perspective is supported by recent empirical studies showing that organizations with fragmented IT governance structures experience higher rates of regulatory violations and audit findings (PwC, 2024). Furthermore, the increasing reliance on third-party service providers and cloud vendors has amplified compliance risks related to vendor oversight and data sovereignty (European Commission, 2024).

Scholars have also highlighted the regulatory implications of emerging technologies such as AI and automated decision-making systems. These technologies introduce new compliance challenges related to transparency, explainability, and ethical use of data, which traditional audit frameworks may not adequately address (OECD, 2024; ISACA, 2024). As a result, regulators increasingly expect organizations to demonstrate robust IT risk governance and audit capabilities.

2.3 IT Governance Frameworks and Audit Effectiveness

IT governance frameworks provide structured guidance for managing and auditing digital risks. COBIT 2019, ISO/IEC 27001, and the NIST Cybersecurity Framework are widely adopted standards that support risk-based auditing and regulatory alignment (ISACA, 2023). Research indicates that organizations adopting these frameworks experience improved audit consistency, clearer accountability, and stronger compliance outcomes (De Haes et al., 2023).

However, several studies caution that adopting the framework alone does not guarantee effectiveness. Kraus et al. (2023) found that organizations often implement frameworks in a compliance-driven manner without integrating them into daily operational processes. This superficial adoption limits IT audits' ability to detect and mitigate emerging risks. Effective IT risk auditing, therefore, requires not only framework alignment but also cultural support, executive sponsorship, and technological enablement.

2.4 Empirical Evidence Linking IT Risk Audit and Regulatory Compliance

While conceptual literature strongly supports a positive relationship between IT risk auditing and regulatory compliance, empirical validation remains limited. PwC (2024) reports that organizations with mature IT audit functions experience fewer regulatory incidents and faster remediation of audit findings. However, such industry reports often lack rigorous statistical testing and peer-reviewed validation.

Recent academic studies have begun to address this gap. Bada and Nurse (2022) demonstrate that audit maturity positively correlates with cybersecurity posture, while Almeida et al. (2023) find that digital risk management effectiveness improves with stronger audit involvement. Nevertheless, few studies explicitly test the impact of IT risk audit maturity on regulatory compliance outcomes using multivariate statistical models.

2.5 Research Gap and Alignment with Study Hypotheses

The reviewed literature reveals a clear gap in empirical research examining the direct relationship between IT risk audit maturity and regulatory compliance effectiveness in challenging digital environments. Existing studies either focus on conceptual frameworks or examine related constructs such as cybersecurity maturity and governance effectiveness. This study addresses this gap by empirically testing the influence of IT risk audit maturity, audit automation, and continuous auditing on regulatory compliance outcomes.

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

The literature review directly informs the study's hypotheses by establishing theoretical and empirical justification for examining IT risk audit maturity (H1), audit automation (H2), and continuous auditing practices (H3) as key determinants of regulatory compliance effectiveness.

2.6 Hypotheses Development

Based on the literature, the following hypotheses were formulated:

H1: IT risk audit maturity has a significant positive effect on regulatory compliance effectiveness.

H2: Audit automation positively moderates the relationship between IT risk audit maturity and regulatory compliance effectiveness.

H3: Continuous auditing practices significantly enhance regulatory compliance outcomes in digitally complex environments.

3. METHODOLOGY

3.1 Research Design

A mixed-methods research design was adopted to provide both statistical rigor and contextual depth. Quantitative survey data were complemented by qualitative interviews.

3.2 Sample and Data Collection

The study targeted IT auditors, GRC professionals, and cybersecurity managers in regulated industries, including financial services, healthcare, and technology. Of the 210 distributed questionnaires, 162 valid responses were received (77% response rate). Additionally, 15 semi-structured interviews were conducted with senior IT audit professionals.

3.3 Measurement of Variables

- **IT Risk Audit Maturity (Independent Variable):** Measured using indicators including risk-based planning, audit automation, continuous monitoring, and framework alignment.
- **Regulatory Compliance Effectiveness (Dependent Variable):** Measured using compliance findings, regulatory incidents, and remediation effectiveness.
- **Control Variables:** Organization size, industry sector, and regulatory intensity.

3.4 Data Analysis Techniques

Quantitative data were analyzed using descriptive statistics, Pearson's correlation, and multiple regression. Qualitative data were analyzed through thematic coding.

4. RESULTS

4.1 Reliability and Validity Assessment

To ensure the robustness of the measurement instruments, reliability and validity tests were conducted prior to hypothesis testing. Internal consistency reliability was assessed using Cronbach's alpha, while construct validity was evaluated using the Kaiser–Meyer–Olkin (KMO) measure of sampling adequacy and exploratory factor analysis (EFA).

Table 1

Reliability Statistics (Cronbach's Alpha)

Construct	Number of Items	Cronbach's α
IT Risk Audit Maturity	6	0.89
Audit Automation	4	0.86
Continuous Auditing	4	0.88
Regulatory Compliance Effectiveness	5	0.91

Note. All Cronbach's alpha values exceed the recommended threshold of 0.70, indicating strong internal consistency.

Table 2

KMO and Bartlett's Test of Sphericity

Test	Value
Kaiser–Meyer–Olkin (KMO) Measure	0.82
Bartlett's Test of Sphericity (χ^2)	1246.37

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

Test	Value
df	210
Sig.	< .001

The KMO value exceeds the minimum acceptable threshold of 0.60, and Bartlett's test is statistically significant, confirming the suitability of the data for factor analysis.

Table 3

Exploratory Factor Analysis (Factor Loadings)

Item	IT Audit Maturity	Audit Automation	Continuous Auditing	Compliance Effectiveness
IAM1	0.78	—	—	—
IAM2	0.81	—	—	—
IAM3	0.76	—	—	—
AA1	—	0.84	—	—
AA2	—	0.79	—	—
CA1	—	—	0.82	—
CA2	—	—	0.77	—
CE1	—	—	—	0.85
CE2	—	—	—	0.81

Note. All factor loadings exceed 0.70, demonstrating strong convergent validity and minimal cross-loading concerns.

4.2 Descriptive Statistics and Hypothesis Testing

Table 4

Descriptive Statistics of Key Variables

Variable	Mean	Std. Deviation
IT Risk Audit Maturity	3.87	0.61
Audit Automation	3.54	0.72
Continuous Auditing	3.68	0.66
Regulatory Compliance Effectiveness	3.91	0.58

Table 5

Correlation Matrix

Variable	1	2	3	4
1. IT Risk Audit Maturity	1			
2. Audit Automation	.64**	1		
3. Continuous Auditing	.69**	.61**	1	
4. Compliance Effectiveness	.71**	.66**	.73**	1

Note. p < .01.

Table 6

Regression Results Predicting Compliance Effectiveness

Predictor	β	t-value	p-value
IT Risk Audit Maturity	0.63	9.12	< .001
Audit Automation	0.28	4.76	< .001
Continuous Auditing	0.31	5.44	< .001
Control Variables	—	—	ns

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

-------|------|----------------|
IT Risk Audit Maturity	3.87	0.61
Audit Automation	3.54	0.72
Continuous Auditing	3.68	0.66
Regulatory Compliance Effectiveness	3.91	0.58

Table 7
Correlation Matrix

Variable	1	2	3	4
1. IT Risk Audit Maturity	1			
2. Audit Automation	.64**	1		
3. Continuous Auditing	.69**	.61**	1	
4. Compliance Effectiveness	.71**	.66**	.73**	1

Note. p < .01.

Table 8
Regression Results Predicting Compliance Effectiveness

Predictor	β	t-value	p-value
IT Risk Audit Maturity	0.63	9.12	< .001
Audit Automation	0.28	4.76	< .001
Continuous Auditing	0.31	5.44	< .001
Control Variables	—	—	ns

5. DISCUSSION

This study set out to empirically examine the role of IT risk audit maturity in enhancing regulatory compliance within challenging digital environments. The findings provide strong support for all proposed hypotheses and offer meaningful contributions to both theory and practice. By integrating empirical evidence with established governance and audit frameworks, this section discusses the results through theoretical and practical lenses.

5.1 Theoretical Implications

From a theoretical perspective, the findings extend the literature on IT governance, risk management, and audit effectiveness in several important ways. First, the strong positive relationship between IT risk audit maturity and regulatory compliance effectiveness provides empirical validation for governance-based theories that position auditing as a core assurance mechanism within enterprise risk management (ERM). Prior studies have largely conceptualized this relationship without rigorous empirical testing (De Haes et al., 2023). This study bridges that gap by demonstrating, through multivariate analysis, that audit maturity is not merely correlated with, but also significantly predictive of, compliance outcomes.

Second, the results support contingency theory in the context of digital risk management. Contingency theory posits that organizational effectiveness depends on the alignment between internal structures and external environmental conditions. In highly digitalized and regulated environments, traditional periodic audits appear insufficient. The significant effects of audit automation and continuous auditing confirm that adaptive audit mechanisms are necessary to cope with technological volatility, regulatory complexity, and real-time risk exposure (Bada & Nurse, 2022; Kraus et al., 2023).

Third, this study contributes to emerging scholarship on continuous assurance and digital auditing by empirically substantiating the theoretical claim that technology-enabled audit practices enhance governance outcomes. While frameworks such as COBIT 2019 and ISO/IEC 27001 advocate continuous monitoring, empirical support has remained limited. The findings reinforce these frameworks by demonstrating that continuous auditing is not only conceptually sound but also empirically effective in strengthening regulatory compliance.

5.2 Practical Implications for Organizations and Regulators

From a practical standpoint, the findings carry important implications for organizations, regulators, and audit professionals. For organizations operating in regulated digital environments, the results highlight the need to move

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

beyond compliance-driven, checklist-based audits toward risk-based, continuous audit models. Organizations with mature IT risk audit functions characterized by automation, real-time monitoring, and strong alignment with governance are better equipped to identify compliance gaps early and reduce remediation delays.

Audit automation emerged as a significant predictor of compliance effectiveness, underscoring the value of data analytics, continuous control monitoring, and integrated GRC platforms. Practitioners should prioritize investments in audit technologies that enable real-time visibility into control performance, particularly in cloud and third-party environments where manual audits are often ineffective. Additionally, the findings suggest that boards and senior management must elevate IT risk auditing to a strategic governance function rather than treating it as a purely operational activity.

For regulators, the study provides empirical support for encouraging or mandating stronger IT governance and audit practices. Regulatory bodies increasingly emphasize governance accountability and continuous risk oversight, particularly in areas such as data protection and cybersecurity. The results suggest that regulatory guidance should explicitly recognize the role of continuous IT auditing and audit automation in achieving sustainable compliance, rather than relying solely on periodic compliance assessments.

5.3 Implications for the IT Audit Profession

The findings also have significant implications for the IT audit profession. The demonstrated importance of audit maturity and automation highlights the growing need for auditors to possess advanced skills in cybersecurity, data analytics, cloud architecture, and emerging technologies. Traditional audit competencies alone may no longer suffice in digitally complex environments. Professional bodies and training institutions should therefore update certification curricula and continuous professional development programs to reflect these evolving requirements (ISACA, 2024).

Moreover, the results reinforce the shifting role of IT auditors from a role as retrospective assurance providers to proactive risk advisors. By leveraging continuous auditing tools and analytics, IT auditors can provide forward-looking insights that support regulatory compliance and strategic decision-making. This evolution aligns with recent calls in the literature for repositioning the IT audit function as a value-adding component of organizational governance rather than a cost center.

5.4 Synthesis of Theory and Practice

Overall, the expanded discussion demonstrates strong alignment between theoretical expectations and practical realities. Theoretical models advocating risk-based, continuous, and technology-enabled auditing are empirically supported by the study's findings, while practical recommendations are grounded in robust statistical evidence. This synthesis strengthens the study's contribution by showing that advances in IT audit theory can be successfully operationalized to address real-world regulatory challenges in digital environments.

5.6 Conclusion

This study demonstrates that mature IT risk audit practices are essential for achieving effective regulatory compliance in challenging digital environments. Empirical results confirm that IT risk audit maturity, audit automation, and continuous auditing significantly enhance compliance effectiveness. As organizations face increasing digital complexity and regulatory scrutiny, the evolution of IT audit functions from periodic assurance providers to continuous governance partners becomes imperative.

5.7 Limitations and Future Research

Despite its contributions, this study has several limitations. First, the use of self-reported survey data may introduce response bias. Second, the cross-sectional design limits the ability to infer causality between IT risk audit maturity and compliance effectiveness. Third, the sample focused primarily on regulated industries, which may limit generalizability to less regulated sectors.

Future research should adopt longitudinal designs to examine causal relationships over time and expand the sample to include small and medium-sized enterprises and public-sector organizations. Additionally, future studies could explore the role of emerging technologies such as artificial intelligence, blockchain, and continuous control monitoring systems in reshaping IT risk auditing and regulatory compliance.

5.8 Recommendations

Organizations should invest in audit automation tools, adopt continuous auditing models, strengthen IT governance structures, and provide advanced training for IT auditors. Regulators should also provide clearer guidance on auditing emerging technologies such as AI and cloud systems.

REFERENCES

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

1) Almeida, F., Santos, J., & Monteiro, J. (2023). Digital transformation and cybersecurity risk management: An organizational perspective. *Journal of Information Security, 14*(2), 85–101.
2) Bada, M., & Nurse, J. R. C. (2022). Developing cybersecurity audit maturity models. *Computers & Security, 114*, 102588.
3) De Haes, S., Van Grembergen, W., & Joshi, A. (2023). Enterprise governance of information technology. *MIS Quarterly Executive, 22*(1), 1–15.
4) ISACA. (2023). *COBIT 2019 framework*. ISACA.
5) ISACA. (2024). *State of IT audit and assurance*. ISACA Research.
6) Kraus, S., Breier, M., & Dasi-Rodriguez, S. (2023). Digital auditing and continuous assurance. *Technological Forecasting and Social Change, 189*, 122372.
7) OECD. (2024). *Digital security risk management and regulatory compliance*. OECD Publishing.
8) PWC. (2024). Global Economic Crime Survey 2024. Retrieved from//efaidnbmnnnibpcajpcglclefindmkaj/https://www.pwc.dk/da/publikationer/2024/2024-global-economic-crime-survey.pdf
9) Von Solms, R., & Van Niekerk, J. (2022). Information security governance. *Computers & Security, 112*, 102516.