International Journal of Advances in Data and Information Systems
Vol. 7, No. 2, August 2026, pp. 645~655
ISSN: 2721-3056, DOI: 10.25008/ijadis.v7i2.1507

Evaluating Access Management Effectiveness for SOX-Driven IT General Controls Using NIST SP 800-53

Irwan Shofwan[1], Muhammad Hafizhuddin Hilman[2], Raden Trimanadi[3,4]
[1,2,3] Faculty of Computer Science, University of Indonesia, Indonesia
[4] Faculty of Computer Science, Esa Unggul University, Indonesia

Article Info

Article history:
Received Jan 01, 2026
Revised Apr 20, 2026
Accepted Apr 28, 2026

Keywords:
Access Management
IT General Controls
Sarbanes–Oxley Compliance
NIST SP 800-53
Fintech Security Governance

ABSTRACT

Access control failures including delayed account deactivation, unauthorized privilege escalation, and gaps in privileged session oversight represent a primary risk pathway to financial reporting integrity failures and SOX-reportable material weaknesses, making effective access management one of the most consequential components of IT General Controls (ITGC) in fintech organizations operating within SOX-oriented governance frameworks. Despite formal compliance efforts, access management controls are often implemented in a procedural manner that may not fully reflect their operational effectiveness. This study evaluates the effectiveness of access management controls in a fintech organization using NIST Special Publication 800-53 Revision 5 as a technical evaluation framework. The research adopts a qualitative evaluative case study approach, combining document review, system observation, and semi-structured interviews to assess selected access management controls. A structured control mapping and gap analysis process is applied to compare existing practices against NIST-defined control requirements, followed by a risk-based interpretation of identified gaps. The results indicate that while foundational access management mechanisms are in place, several controls are only partially effective due to reliance on manual processes, delayed account deactivation, limited privileged access monitoring, and periodic log reviews. These gaps reduce the consistency and timeliness of access enforcement and weaken overall ITGC effectiveness. This study contributes a practical and technically grounded evaluation model that bridges SOX-driven internal control expectations with standardized security controls. The findings provide actionable insights for organizations seeking to strengthen access management governance and improve control effectiveness in regulated digital environments.

This is an open access article under the CC BY-SA license.

Corresponding Author:
Irwan Shofwan,
Department of Information Technology,
Faculty of Computer Science,
University of Indonesia,
UI Depok Campus, Jalan Margonda Raya, Pondok Cina, Beji, Depok, West Java, Indonesia.
Email: irwan.shofwan@ui.ac.id

1. INTRODUCTION

Information technology (IT) governance is widely viewed as a key enabler for ensuring the reliability, security, and integrity of organizational information systems, especially in environments where digital processes directly influence business outcomes and reporting quality [1], [2]. In fintech organizations, where transaction processing and data services are delivered primarily through IT-enabled platforms, weaknesses in IT controls may increase exposure to operational failures and reporting risks that can escalate into compliance issues [2], [3].

The Sarbanes–Oxley Act (SOX) has reinforced the importance of internal control over financial reporting and stimulated extensive research on how control weaknesses affect firm risk and market outcomes [3], [4]. Empirical evidence indicates that internal control deficiencies are associated with higher firm risk and cost of equity, emphasizing that control effectiveness is not merely a procedural requirement but a material risk factor for organizations [4]. Studies also suggest that firms with more effective internal controls may benefit from SOX related mechanisms, further motivating organizations to strengthen controls supporting financial reporting processes [5]. From an audit perspective, stronger IT controls have been linked to audit outcomes such as audit fees, underscoring the economic relevance of control quality in assurance contexts [6]. Consistent with this perspective, empirical research shows that regulatory oversight through PCAOB inspection programs contributes to improvements in the quality of internal control audits, reinforcing the importance of effective ICFR and ITGC evaluation within the SOX framework [7].

Despite these motivations, organizations frequently operationalize compliance through documentation and formal control descriptions that may not fully reflect the technical effectiveness of implemented safeguards. Although governance-level frameworks such as the COSO Internal Control–Integrated Framework define fundamental principles and components for effective internal control design [8], their implementation in practice often remains focused on policy articulation rather than consistent operational enforcement. This limitation becomes more critical when cybersecurity incidents are considered, as they are frequently intertwined with underlying internal control weaknesses. Recent accounting information systems research shows that cyber breach reports may carry signals about underlying internal control deficiencies, implying that formal compliance does not automatically translate into effective control operation [9]. Similarly, evidence from security research suggests that SOX-related disclosures can be informative in predicting security breaches, supporting the view that IT control quality and cybersecurity outcomes are closely connected [10]. Governance-oriented studies further emphasize that control frameworks implemented primarily at a formal or policy level, without consistent operational enforcement mechanisms, may fail to achieve effective risk mitigation in dynamic organizational environments [11]. Prior research has also cautioned organizations to move “beyond compliance” to address security risks that may persist even after baseline compliance requirements are formally satisfied [12].

In response to this challenge, standardized security control frameworks can provide measurable and technically grounded criteria for assessing access management controls, which are central to preventing unauthorized access, limiting excessive privileges, and enabling accountability through monitoring and auditability [13]. NIST Special Publication 800-53 (Revision 5) provides a comprehensive catalog of security and privacy controls, including controls relevant to account management, access enforcement, least privilege, auditing, and continuous monitoring, making it suitable as a technical reference for evaluating access management practices [14], [15]. Prior work discussing regulatory compliance implications of evolving NIST guidance also highlights the relevance of NIST based control structures as a bridge between compliance expectations and technical implementations [16].

However, although research has examined SOX related internal control weaknesses and cybersecurity outcomes, limited empirical work has systematically applied a NIST SP 800-53-based evaluation approach to assess access management effectiveness in fintech organizations within the context of SOX driven internal control expectations [9], [10], [14]. This gap indicates the need for an evaluation approach that integrates accounting information systems insights about internal control effectiveness with a technical control framework that supports structured assessment and actionable improvement planning.

This study sits at the intersection of three bodies of knowledge that have each addressed aspects of access control effectiveness independently, but which have not been systematically integrated for the SOX-fintech evaluation context. The accounting information systems (AIS) literature contributes the internal control effectiveness construct and empirical evidence that ITGC deficiencies carry material consequences for firm risk and audit outcomes [4], [9], [10]. The IT governance literature contributes ITGC design principles and the organizational context for

compliance-oriented control evaluation [7], [8], [18]. The cybersecurity literature, anchored by NIST SP 800-53, contributes technically measurable control criteria that can be verified at the system level [14], [15], [16]. No prior study has integrated all three into a unified, structured evaluation model suited to the fintech-SOX context. This gap distinguishes the present study from related work that either examines SOX compliance at the governance level [8], [11] or applies security frameworks outside the SOX ITGC context [13], [14], and motivates the evaluation approach developed here.

This study addresses the gap by conducting a structured evaluation and gap analysis of access management controls in a fintech organization using NIST SP 800-53 Revision 5 as the primary evaluation reference. By comparing current access management practices against recommended control requirements, the study identifies control deficiencies, assesses their implications for control effectiveness, and proposes improvement directions that are technically measurable and audit-relevant. The contribution of this research lies in providing a practical evaluation model that strengthens the linkage between SOX motivated internal control effectiveness and standardized security controls, supporting fintech organizations and practitioners in improving access management governance and operational security.

2. RESEARCH METHOD

2.1. Research Design

This study adopts a qualitative evaluative research design using a case study approach. The case study focuses on a fintech organization that is subject to SOX-driven internal control requirements, with particular emphasis on access management practices within the scope of IT General Controls (ITGC). A qualitative approach is selected to enable an in-depth examination of control implementation, operational procedures, and system-level configurations that cannot be adequately captured through quantitative metrics alone, which is consistent with prior research emphasizing the suitability of case study methods for investigating complex organizational control environments [17].

The evaluation is conducted as a control-based assessment rather than a system performance measurement. Accordingly, the research does not aim to test system efficiency or user behavior, but to evaluate the adequacy and effectiveness of access management controls in relation to established security control requirements, as commonly adopted in internal control and IT audit-oriented studies [18]. Figure 1 illustrates the research flow adopted in this study, outlining the evaluation stages from scope definition to risk-based interpretation of access management controls.

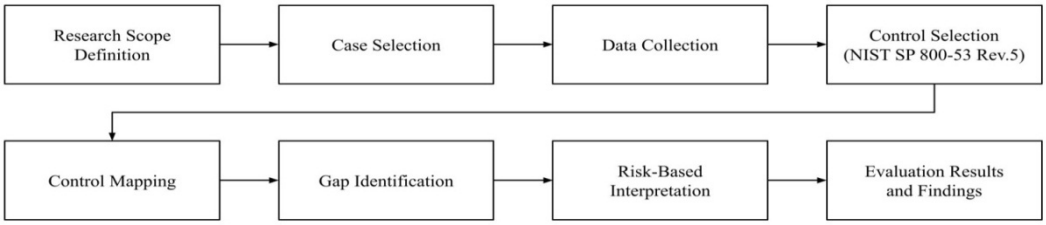


Figure 1. Research Flow for Access Management Evaluation Based on NIST SP 800-53 Rev.5

2.2. Evaluation Framework

NIST Special Publication 800-53 Revision 5 is used as the primary evaluation framework in this study due to its comprehensive and operationally detailed structure for assessing security and privacy controls. Specifically, this research focuses on the Access Control (AC) control family, which provides a structured basis for evaluating access management practices at the system level, including account management, access enforcement, least privilege, session control, and remote access controls [14].

The selection of NIST SP 800-53 is motivated by its ability to translate regulatory and compliance expectations into technically measurable control requirements that can be directly mapped to system configurations and operational procedures. Unlike high-level governance frameworks, NIST SP 800-53 defines control expectations in an explicit and implementable

manner, making it suitable for evaluating access management effectiveness in regulated environments such as fintech organizations subject to SOX-driven internal control requirements [16]. o ensure comprehensive coverage while maintaining analytical clarity, all 25 base controls within the AC family (AC-1 to AC-25) are included in the scope of this evaluation and grouped into logical categories based on their primary control objectives, as summarized in Table 1.

Table 1. Grouping of NIST SP 800-53 Access Control (AC) Controls Evaluated in This Study

Category	NIST AC Controls	Control Focus
Policy & Governance	AC-1	Access control policy and procedures
Account Lifecycle Management	AC-2	Account creation, modification, disabling, and removal
Access Enforcement & Authorization	AC-3, AC-4	Enforcement of access decisions and information flow control
Separation & Least Privilege	AC-5, AC-6	Separation of duties and restriction of excessive privileges
Session & Logon Control	AC-7, AC-8, AC-9	Unsuccessful logon attempts, system use notification, session termination
Concurrent & Contextual Access	AC-10, AC-11, AC-12	Concurrent sessions, device lock, session termination
Remote & Network-Based Access	AC-17, AC-18, AC-20	Remote access, wireless access, and external system access
Access Constraints & Attributes	AC-14, AC-16	Permitted actions without identification, security attributes
Mobile, Cloud & Special Access	AC-19, AC-21, AC-22, AC-23	Mobile devices, information sharing, public content, data mining protection
Advanced & Privileged Access Controls	AC-24, AC-25	Access control decisions, reference monitor

2.3. Scope of Evaluation

The scope of the evaluation is limited to access management controls that support ITGC objectives in the context of SOX compliance. The assessed control areas include account lifecycle management, user access provisioning and deprovisioning, privileged access control, access enforcement mechanisms, and monitoring of access-related activities. These control areas are widely recognized as critical components of effective access management and internal control effectiveness [18], [4].

Business process controls, financial transaction controls, and non-access-related ITGC domains such as change management and IT operations are excluded from the scope to maintain focus and analytical depth. This scoping decision ensures that the evaluation remains aligned with the research objective of assessing access management effectiveness without diluting analytical rigor.

2.4. Data Collection Techniques

Data collection is conducted using multiple qualitative techniques to support triangulation and improve assessment reliability. The primary techniques include document review, system observation, and semi-structured interviews with personnel responsible for access management operations, a combination commonly used in qualitative control evaluations to strengthen evidence validity [17], [19].

Document review covers access control policies, standard operating procedures, user access records, and audit-related documentation. System observation involves examining identity management systems, access control configurations, and logging mechanisms to understand how controls are implemented in practice. Semi-structured interviews are conducted with system administrators responsible for identity and access management operations to clarify operational workflows, control responsibilities, and exception handling practices.

2.5. Control Mapping and Gap Analysis Procedure

The evaluation process follows a structured control mapping and gap analysis procedure. First, selected NIST SP 800-53 control requirements are identified and translated into assessment criteria. Second, existing access management practices are mapped against these criteria to determine the level of implementation and control coverage, following established approaches for control-based assessments [14], [9].

Each control is then evaluated by comparing the observed condition with the expected condition defined by NIST SP 800-53. Gaps are identified when control requirements are partially implemented, inconsistently applied, or not implemented. The identified gaps are documented along with supporting evidence obtained from documents, system observations, and interviews, ensuring traceability between findings and evaluation criteria.

2.6. Risk-Based Assessment Consideration

To support prioritization, identified gaps are further analyzed using a risk-based perspective. Gaps are classified based on their potential impact on access control effectiveness and their likelihood of contributing to unauthorized access or compliance issues. This approach aligns with prior studies emphasizing the importance of risk-based interpretation when assessing internal control weaknesses [4], [10].

The risk-based assessment does not introduce a separate risk model but serves as an analytical lens to interpret evaluation results and support decision-making related to access management enhancement.

2.7. Validity and Reliability Considerations

To enhance validity, the study applies data triangulation by cross-verifying findings across multiple data sources and collection techniques, a widely accepted practice in qualitative case study research [17]. Reliability is supported by using a consistent evaluation framework and standardized assessment criteria derived from NIST SP 800-53. The structured mapping process ensures that control assessments are repeatable and traceable to specific evaluation criteria.

2.8. Research Output and Analysis Artifacts

The output of this research consists of an evaluation report presenting the assessed access management controls, identified gaps, and their implications for control effectiveness. The findings are synthesized in a gap analysis matrix that highlights discrepancies between current practices and recommended control requirements, providing a structured basis for discussion and improvement planning, as commonly reported in framework-based control evaluation studies [9].

3. RESULTS AND DISCUSSION

3.1. Overview of Access Management Evaluation Results

The evaluation results indicate that the fintech organization has implemented fundamental access management controls to support IT General Controls (ITGC) objectives. Core mechanisms such as user authentication, role assignment, and access approval workflows are formally defined and operational, thereby providing a baseline level of protection against unauthorized access and supporting basic compliance requirements [18], [20]. A high-level summary of the implementation status across key access management control areas is presented in Table 2.

However, the evaluation also reveals that several access management controls are implemented in a partially effective manner. Although relevant policies and procedures are in place, their execution relies heavily on manual processes and periodic reviews rather than continuous or automated enforcement. Similar conditions have been reported in prior studies, where documented access control mechanisms did not necessarily translate into effective operational control [12], [9]. This reliance on manual execution limits the organization's ability to enforce access controls consistently and in a timely manner, particularly in environments characterized by frequent personnel changes and dynamic system usage.

Table 2. Overview of Access Management Evaluation Results

Category	AC Controls	Control Focus	Summary of Findings
Access Control Policy & Governance	AC-1	Implemented	Access control policies and responsibilities are formally defined and communicated, providing baseline governance support.
Account Lifecycle Management	AC-2	Partially Implemented	Account provisioning and deprovisioning are documented but rely on manual processes and periodic reviews.
Access Enforcement	AC-3	Partially Implemented	Role-based access restrictions are defined, but enforcement consistency varies across systems.

Category	AC Controls	Control Focus	Summary of Findings
Separation of Duties	AC-5	Implemented	Segregation of roles is established at a procedural level to reduce conflict of interest risks.
Least Privilege	AC-6	Partially Implemented	Least-privilege principles are stated but lack strong technical enforcement and continuous review.
Privileged Access Management	AC-6, AC-17	Partially Implemented	Privileged access exists with limited session logging and monitoring of high-risk activities.
Access Monitoring & Review	AC-7, AC-9	Partially Implemented	Logging is enabled; however, reviews are periodic and not supported by automated alerting mechanisms.

3.2. Results of NIST SP 800-53-Based Gap Analysis

The gap analysis, conducted by mapping existing access management practices against selected NIST SP 800-53 Revision 5 controls, identifies multiple discrepancies between expected and actual control conditions [14]. The most significant gaps are observed in control areas related to account lifecycle management, privileged access management, and continuous monitoring domains that are widely recognized as high-risk in access control evaluations [21], [22]. A summary of the key access management gaps identified through this evaluation is presented in Table 3.

Table 3. Summary of Key Access Management Gaps Identified

Category	AC Controls	Control Focus	Summary of Findings	Gap Description
Account Lifecycle Management	AC-2	Account provisioning and deprovisioning rely on manual and periodic reviews	Automated and timely account lifecycle enforcement	Delayed account revocation increases risk of orphaned and excessive access
Privileged Access Management	AC-6, AC-17	Privileged activities are not consistently logged or reviewed	Continuous monitoring and logging of privileged sessions	Limited visibility over high-risk privileged actions
Access Monitoring & Audit	AC-7, AC-9	Log reviews conducted periodically without automated alerting	Continuous monitoring with automated detection	Delayed detection of access violations and policy deviations

In the area of account lifecycle management, the evaluation indicates that user account provisioning and deprovisioning processes are formally documented but largely manual in execution. Account deactivation following role changes or employee separation relies on periodic access reviews rather than real-time triggers, thereby increasing the risk of orphaned or excessive access. Prior research has shown that delayed account revocation is a recurring source of access control weaknesses and contributes to elevated organizational risk [23]. This condition reflects partial alignment with NIST account management requirements, which emphasize automated, timely, and event-driven enforcement mechanisms [14].

For privileged access management, the organization enforces role-based access restrictions; however, monitoring of privileged activities remains limited. Privileged sessions are not consistently logged or subject to systematic review, reducing visibility into high-risk actions performed by users with elevated permissions. This gap between formal access restrictions and effective oversight has been widely recognized in the literature as a critical weakness in access control implementations, particularly in regulated and high-risk environments [24], [25].

Limitations are also evident in the continuous monitoring and auditing of access-related activities. Although logging mechanisms are enabled, log review processes are conducted on a periodic basis and are not integrated with automated alerting or anomaly detection capabilities. Consequently, access violations or policy deviations may remain undetected until after scheduled reviews, weakening both preventive and detective control functions. Similar shortcomings associated with periodic monitoring approaches have been reported in prior internal control and cybersecurity studies [10], [26].

3.3. Risk-Based Interpretation of Identified Gaps

From a risk-based perspective, the identified gaps vary in their potential impact on access control effectiveness. Gaps related to delayed account deactivation and insufficient privileged access monitoring are classified as higher-risk issues due to their direct association with

unauthorized access and fraud scenarios. Empirical evidence indicates that access-related internal control deficiencies are strongly associated with increased firm risk and weakened assurance outcomes [4], [5]. The relative prioritization of these gaps based on their assessed impact and likelihood is illustrated in Figure 3.

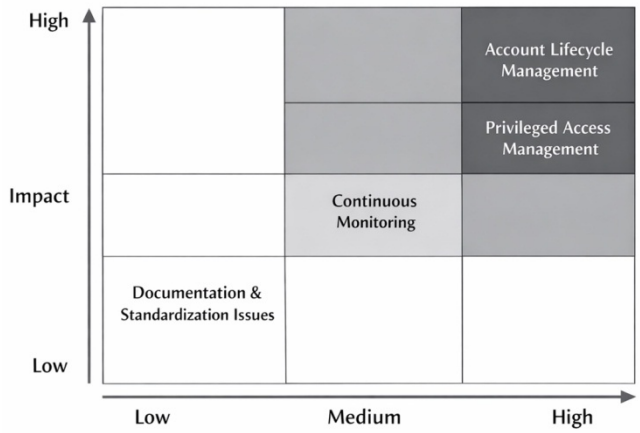


Figure 2. Risk-Based Classification of Identified Access Management Gaps

Lower-risk gaps are primarily associated with documentation inconsistencies and limited standardization across systems. While these issues do not immediately compromise access control effectiveness, prior studies suggest that persistent weaknesses in documentation and standardization may contribute to gradual control degradation over time [12], [27]. Overall, the risk-based interpretation highlights the importance of prioritizing remediation efforts toward controls that directly affect access enforcement and monitoring capabilities. In Figure 3, darker grayscale shading indicates higher-risk gaps resulting from a combination of higher impact and likelihood, whereas lighter shading represents lower-risk conditions.

3.4. Discussion: Implications for ITGC and SOX-Oriented Control Effectiveness

The results of this evaluation reinforce the critical distinction between formal compliance and operational control effectiveness within SOX-oriented IT General Controls (ITGC). Although the organization demonstrates procedural alignment with ITGC requirements through documented access management policies and defined workflows, the identified gaps indicate that these controls are not yet optimized to support continuous, consistent, and proactive enforcement. This finding is consistent with prior studies showing that internal control weaknesses may persist despite documented compliance, particularly when control execution relies heavily on manual and periodic processes rather than automated mechanisms [12].

The observed deficiencies in account lifecycle management and privileged access monitoring highlight structural limitations in the organization's access management implementation. Delayed account deactivation and insufficient oversight of privileged activities expose the organization to elevated risks of unauthorized access and misuse, undermining both preventive and detective control objectives. Prior research in accounting information systems and cybersecurity domains has emphasized that such access-related weaknesses are among the most significant contributors to residual compliance and security risks, especially in regulated environments [9], [26].

By applying NIST SP 800-53 Revision 5 as an evaluation reference, this study demonstrates how standardized security control frameworks can be operationalized to translate high-level compliance expectations into measurable and technically enforceable requirements [14], [16]. The findings suggest that strengthening access management effectiveness requires a shift from compliance-oriented control design toward technically integrated solutions that emphasize automation, real-time monitoring, and centralized oversight. Such an approach not only enhances ITGC effectiveness but also improves the organization's ability to demonstrate sustainable compliance and resilience against access-related risks.

3.5. Summary of Findings

Overall, the evaluation indicates that while foundational access management controls are in place, their effectiveness is constrained by limited automation and monitoring capabilities. The gap analysis provides clear evidence that access management remains a critical area requiring improvement to support robust IT General Controls (ITGC) implementation. These findings reinforce prior conclusions that effective access control requires a shift from compliance-oriented control design toward technically enforceable and continuously monitored practices [9], [25], [26]. These observations provide the basis for the concluding section, which summarizes the study's contributions and outlines its practical implications.

4. CONCLUSION

This study evaluates the effectiveness of access management controls in a fintech organization using NIST SP 800-53 Revision 5 as a technical evaluation reference within the context of IT General Controls (ITGC). The evaluation results indicate that while foundational access management mechanisms are formally defined and operational, several controls remain only partially effective due to their reliance on manual processes and periodic reviews. These findings are consistent with prior studies, which emphasize that fragmented security tooling and documentation-driven control implementations, when supported primarily by manual and periodic review mechanisms, are often insufficient to provide consistent and timely enforcement in dynamic organizational environments.

The gap analysis reveals that the most critical deficiencies are concentrated in account lifecycle management, privileged access monitoring, and continuous auditing of access-related activities. Delayed account deactivation and limited visibility into privileged actions increase exposure to unauthorized access and reduce overall control effectiveness. Prior research on centralized security monitoring indicates that the absence of integrated and continuously operated visibility mechanisms may limit an organization's ability to detect misuse and respond to access-related risks in a timely manner, particularly when monitoring practices rely on fragmented tooling and periodic review processes.

By applying NIST SP 800-53 as an evaluation framework, this research demonstrates how standardized security controls can be operationalized to assess access management practices in a structured and technically measurable manner. The findings highlight the value of using detailed control criteria to bridge the gap between compliance expectations and system-level control implementation, particularly in environments subject to SOX-driven internal control requirements.

The contribution of this study lies in providing a practical evaluation approach that integrates insights from accounting information systems and cybersecurity control frameworks. The proposed evaluation model supports organizations in identifying control weaknesses, prioritizing remediation efforts, and strengthening access management governance in a manner that is both audit-relevant and technically actionable.

For accounting information systems researchers, this study provides field evidence that access-related ITGC weaknesses concentrate in predictable structural patterns — account lifecycle management and privileged access monitoring, even in organizations with formally documented compliance programs. This finding extends the proposition of Blakely et al. [9], that cyber breach signals reflect underlying control deficiencies, by identifying the specific control-level mechanisms through which the compliance–effectiveness gap operates, and empirically supports Westland's [10], argument that SOX disclosures carry predictive content about security outcomes.

For IT governance researchers, the partial effectiveness ratings concentrated in lifecycle and monitoring controls suggest that ITGC maturity models should incorporate technical enforcement criteria alongside policy documentation metrics. A control that is formally documented but manually executed should not be assessed at the same maturity level as one that is automated and continuously monitored.

For cybersecurity practitioners and standard-setters, the findings indicate that the current SOX ITGC compliance framework, which does not mandate reference to technical security standards, may produce a systematic blind spot in access control assessment. Organizations and

regulators may benefit from examining whether ITGC evaluation guidance should formally incorporate technically measurable criteria such as those provided by NIST SP 800-53 as a complement to the existing principles-based COSO framework.

This study is subject to certain limitations. The evaluation is conducted within a single organizational context, which may limit the generalizability of the findings. In addition, the assessment focuses exclusively on access management controls and does not cover other ITGC domains such as change management or IT operations. Interview data were drawn solely from system administrators responsible for access management operations; perspectives from compliance officers, internal auditors, or security operations personnel were not represented, which may limit the completeness of findings related to policy-level and audit-oriented control dimensions. Future research may extend this approach by applying the evaluation model across multiple organizations, incorporating additional control domains, engaging a broader range of organizational stakeholders, or examining the impact of automation and continuous monitoring on long-term control effectiveness.

CONFLICT OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

DATA AVAILABILITY

The data supporting the findings of this study consist of internal access control policies, standard operating procedures, user access records, system configuration observations, and semi-structured interview transcripts obtained from a single fintech organization. Because these materials contain confidential organizational and security-sensitive information, they cannot be made publicly available. The anonymized control mapping and gap analysis matrix derived from these sources is available from the corresponding author upon reasonable request, subject to approval from the participating organization.

AUTHOR CONTRIBUTIONS

Irwan Shofwan: Conceptualization, Methodology, Investigation, Formal analysis, Data Curation, Visualization, Writing - Original Draft. **Muhammad Hafizhuddin Hilman**: Methodology, Validation, Supervision. **Raden Trimanadi**: Methodology, Validation, Supervision.

REFERENCES

[1] P. Weill and J. W. Ross, "IT Governance on One Page," *SSRN Electronic Journal*, 2004, doi: 10.2139/ssrn.664612.

[2] S. Mithas, A. Tafti, I. Bardhan, and J. M. Goh, "Information Technology and Firm Profitability: Mechanisms and Empirical Evidence," *MIS Quarterly*, vol. 36, no. 1, pp. 205–224, Oct. 2012, doi: 10.2307/41410414.

[3] G. P. Lander, "The Sarbanes-Oxley Act of 2002," *Journal of Investment Compliance*, vol. 3, no. 1, pp. 44–53, Jan. 2002, doi: 10.1108/joic.2002.3.1.44.

[4] H. ASHBAUGH-SKAIFE, D. W. COLLINS, W. R. KINNEY JR, and R. LAFOND, "The Effect of SOX Internal Control Deficiencies on Firm Risk and Cost of Equity," *Journal of Accounting Research*, vol. 47, no. 1, pp. 1–43, Mar. 2009, doi: 10.1111/j.1475-679X.2008.00315.x.

[5] P. P. Gupta, H. Sami, and H. Zhou, "Do companies with effective internal controls over financial reporting benefit from Sarbanes–Oxley sections 302 and 404?," *Journal of Accounting, Auditing and Finance*, vol. 33, no. 2, pp. 200–227, 2018, doi: 10.1177/0148558X16663091.

[6] T. Mazza and S. Azzali, "Information Technology Controls Quality and Audit Fees: Evidence From Italy," *Journal of Accounting, Auditing & Finance*, vol. 33, no. 1, pp. 123–146, Jan. 2018, doi: 10.1177/0148558X15625582.

[7] M. L. DEFOND and C. S. LENNOX, "Do PCAOB Inspections Improve the Quality of Internal Control Audits?," *Journal of Accounting Research*, vol. 55, no. 3, pp. 591–627,

Jun. 2017, doi: 10.1111/1475-679X.12151.
[8] Committee of Sponsoring Organizations of the Treadway Commission (COSO), "Internal Control—Integrated Framework," 2013.
[9] B. Blakely, J. Kurtenbach, and L. Nowak, "Exploring the information content of cyber breach reports and the relationship to internal controls," *International Journal of Accounting Information Systems*, vol. 46, no. July, p. 100568, Sep. 2022, doi: 10.1016/j.accinf.2022.100568.
[10] J. C. Westland, "The information content of Sarbanes-Oxley in predicting security breaches," *Computers & Security*, vol. 90, p. 101687, Mar. 2020, doi: 10.1016/j.cose.2019.101687.
[11] J. R. Cohen, J. R. Joe, J. C. Thibodeau, and G. Trompeter, "Audit Partners' Judgments and Challenges in the Audit of Internal Control over Financial Reporting," *SSRN Electronic Journal*, 2020, doi: 10.2139/ssrn.3551763.
[12] P. Foote and T. Neudenberger, "Beyond Sarbanes-Oxley compliance," *Computers and Security*, vol. 24, no. 7, pp. 516–518, 2005, doi: 10.1016/j.cose.2005.07.005.
[13] M. Syafrizal, S. R. Selamat, and N. A. Zakaria, "Analysis of Cybersecurity Standard and Framework Components," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 12, no. 3, pp. 417–432, Apr. 2022, doi: 10.17762/ijcnis.v12i3.4817.
[14] Joint Task Force NIST, "Security and Privacy Controls for Information Systems and Organizations," Gaithersburg, MD, Sep. 2020. doi: 10.6028/NIST.SP.800-53r5.
[15] D. Mittal and M. Damle, "An Appraisal in Internal Control Frameworks Implementation of COSO, ISO 27001 and NIST for Opportunities in Industry 5.0," in *2025 Seventh International Conference on Computational Intelligence andCommunication Technologies (CCICT)*, Apr. 2025, pp. 345–352. doi: 10.1109/CCICT65753.2025.00061.
[16] R. V. Rose, "NEW NIST REVISIONS – WHAT DO THEY MEAN FOR REGULATORY COMPLIANCE?," *EDPACS*, vol. 59, no. 6, pp. 5–13, Jun. 2019, doi: 10.1080/07366981.2019.1642559.
[17] R. K. Yin, *Case Study Research and Applications Sixth Edition*, vol. 6. 2455 Teller Road, Thousand Oaks California 91320 United States: SAGE Publications, Inc., 2018. doi: 10.4135/9781412957397.
[18] B. Tuttle and S. D. Vandervelde, "An empirical examination of CobiT as an internal control framework for information technology," *International Journal of Accounting Information Systems*, vol. 8, no. 4, pp. 240–263, Dec. 2007, doi: 10.1016/j.accinf.2007.09.001.
[19] H. Taherdoost, "Validity and Reliability of the Research Instrument; How to Test the Validation of a Questionnaire/Survey in a Research," *SSRN Electronic Journal*, no. January 2016, 2016, doi: 10.2139/ssrn.3205040.
[20] U. J. Gelinas, R. B. Dull, and P. Wheeler, *Accounting Information Systems*. Cengage Learning, 2011. [Online]. Available: https://books.google.co.id/books?id=cdU8AAAAQBAJ
[21] R. S. Sandhu and P. Samarati, "Access control: principle and practice," *IEEE Communications Magazine*, vol. 32, no. 9, pp. 40–48, Sep. 1994, doi: 10.1109/35.312842.
[22] F. Cai, N. Zhu, J. He, P. Mu, W. Li, and Y. Yu, "Survey of access control models and technologies for cloud computing," *Cluster Computing*, vol. 22, no. S3, pp. 6111–6122, May 2019, doi: 10.1007/s10586-018-1850-7.
[23] C. Li, G. Peters, V. Richardson, and M. Watson, *The Consequences of Information Technology Control Weaknesses on Management Information Systems: The Case of Sarbanes-Oxley Internal Reports.* 2010.
[24] D. F. Ferraiolo, J. F. Barkley, and D. R. Kuhn, "A role-based access control model and reference implementation within a corporate intranet," *ACM Transactions on Information and System Security*, vol. 2, no. 1, pp. 34–64, 1999, doi: 10.1145/300830.300834.
[25] R. Sandhu, D. Ferraiolo, and R. Kuhn, "The NIST model for role-based access control," in *Proceedings of the fifth ACM workshop on Role-based access control*, Jul. 2000, pp. 47–63.

doi: 10.1145/344287.344301.
[26] S. Romanosky, "Examining the costs and causes of cyber incidents," *J. Cybersecur.*, vol. 2, pp. 121–135, 2016, doi: 10.1093/cybsec/tyw001.
[27] M. Benaroch, "International Journal of Accounting Measuring the pervasiveness of IT general controls : A model and empirical validation," *International Journal of Accounting Information Systems*, vol. 56, no. June, p. 100752, Dec. 2025, doi: 10.1016/j.accinf.2025.100752.