

RESEARCH ARTICLE

Organizational Management Control Framework for Information System Auditing

Pham Quang Huy

Faculty of Economics, Vietnam National University, Hanoi, Vietnam

Le Thu Ha

Department of Business Management, Foreign Trade University, Hanoi, Vietnam

VOLUME: Vol.06 Issue10 2026

PAGE: 01-06

Copyright © 2026 Journal of Management and Economics, this is an open-access article distributed under the terms of the Creative Commons Attribution-Noncommercial-Share Alike 4.0 International License. Licensed under Creative Commons License a Creative Commons Attribution 4.0 International License.

Abstract

Information systems have become integral to organizational decision-making, operational continuity, financial administration, information processing, and managerial control. Consequently, information system auditing has evolved beyond a narrow assessment of technical compliance toward a broader examination of whether organizational controls adequately protect information assets and support institutional objectives. This research examines the role of organizational management controls in information system auditing and develops a conceptual management control framework integrating governance, risk management, authorization, access control, monitoring, compliance, and corrective mechanisms. The study adopts a qualitative conceptual methodology based exclusively on a structured synthesis of five provided references concerning information system auditing and control. The analysis indicates that effective information system auditing requires alignment between technological controls and organizational management practices. Technical safeguards may reduce specific operational risks, but their effectiveness depends substantially on managerial authorization, accountability, segregation of responsibilities, monitoring, and continuous review. The proposed framework positions management controls as an interconnected system rather than a collection of isolated audit procedures. The findings further indicate that an effective audit framework should combine preventive, detective, and corrective controls while maintaining organizational independence and accountability. The study contributes a structured conceptual perspective for organizations seeking to strengthen information system audit effectiveness through integrated management control mechanisms.

KEY WORDS

Information System Audit, Management Controls, Internal Control, Information Systems Governance, Audit Framework, Risk Management, Access Control, Compliance, Organizational Control, Information Systems Security.

1. INTRODUCTION

Information systems increasingly function as fundamental organizational infrastructures through which operational, administrative, financial, and managerial activities are

performed. The growing dependence on computerized information processing creates a corresponding need for systematic mechanisms that assess whether information

systems are properly controlled, reliable, accountable, and aligned with organizational objectives. Information system auditing therefore represents not merely a technical examination of computing environments but an organizational process through which the adequacy of controls surrounding information systems can be evaluated.

The distinction between information system controls and broader organizational management controls is particularly important. A technically secure system may nevertheless generate organizational risk when management responsibilities are poorly defined, authorization procedures are inadequate, employees possess excessive privileges, or audit findings are not translated into corrective action. Weber's treatment of information systems control and audit emphasizes the importance of examining controls systematically rather than treating technological mechanisms as independent safeguards (Weber, 2002). From this perspective, auditing should evaluate the relationship between information technology, control structures, organizational responsibilities, and managerial oversight.

Practical approaches to information system auditing similarly indicate that audit activity must be connected with organizational processes and control requirements (Mehta, 2024). Doshi and Patel (2022) provide an accessible foundation for understanding information system audit as a structured examination of information-system-related controls, while Namuduri (2013) emphasizes the importance of moving beyond a narrow compliance orientation. Shah (2021), by examining the role of management accountants in information system audit, further illustrates the organizational and managerial dimensions of control assessment.

The central problem addressed in this research is that information system auditing can become fragmented when technological controls, managerial controls, and compliance activities are evaluated separately. Such fragmentation may prevent auditors and managers from identifying how weaknesses in one control area influence other organizational processes. Accordingly, this study develops a conceptual framework that integrates organizational management controls into information system auditing.

The primary objective is to examine the theoretical and functional relationship between management controls and information system auditing. A second objective is to identify the principal control dimensions required for an integrated audit framework. A third objective is to analyze how

preventive, detective, and corrective mechanisms can operate collectively to strengthen organizational information-system governance. The study is conceptual and applies specifically to organizations in which information systems support significant operational or managerial activities.

2. LITERATURE REVIEW

The provided literature collectively establishes information system auditing as a multidisciplinary control activity involving technology, management, accountability, and organizational governance. Weber (2002) provides the strongest conceptual foundation for understanding information systems control and audit as an interconnected control environment. His work supports the proposition that information-system auditing should examine whether controls are capable of reducing organizational exposure to risks associated with information processing and system operation.

Doshi and Patel (2022) approach information system auditing from a foundational perspective and provide a basis for understanding the audit as an organized evaluation of information systems and their associated controls. Their contribution is particularly relevant to the present framework because organizational management controls cannot be evaluated effectively without understanding the underlying audit process. The implication is that auditing must connect system-level observations with organizational responsibilities and managerial expectations.

Mehta (2024) presents a practical orientation to information systems auditing. This practical emphasis complements Weber's broader control perspective by highlighting the operational nature of audit examination. The relationship between the two perspectives suggests that an effective audit framework must be both conceptually sound and practically implementable. A control that exists formally but is not consistently applied cannot be regarded as an effective organizational safeguard.

Namuduri (2013) provides an important conceptual direction by emphasizing information systems auditing beyond compliance. A compliance-oriented audit can determine whether prescribed requirements have been followed, but compliance alone does not necessarily establish whether controls are effective. An organization may satisfy a formal requirement while retaining weaknesses in authorization, monitoring, accountability, or risk response. The broader perspective proposed by Namuduri therefore supports the

development of an audit model concerned with control effectiveness rather than documentation alone.

Shah (2021) contributes a managerial perspective by examining the role of management accountants in information system audit. This perspective demonstrates that information-system controls have consequences extending beyond information technology departments. Financial reporting, managerial decision-making, resource allocation, and organizational accountability may all depend upon the reliability and integrity of information systems.

Across the literature, a common theme emerges: information system auditing is most effective when control evaluation is integrated with organizational management. Weber (2002) particularly supports the view that information systems control should be understood as part of a broader organizational control structure. However, the provided literature does not explicitly present a unified framework that integrates governance, risk assessment, authorization, access management, monitoring, compliance, and corrective action into a single organizational management control model.

This constitutes the conceptual gap addressed by the present study. Rather than treating the individual contributions as separate audit techniques, the proposed framework synthesizes their common principles into an integrated organizational control architecture. The theoretical positioning of the study is therefore based on the proposition that information system audit effectiveness depends on the interaction among technological controls, managerial oversight, organizational accountability, and continuous monitoring.

3. METHODOLOGY

3.1 Research Design

This study adopts a qualitative conceptual research design based exclusively on structured analysis and synthesis of the five references provided. Because the study does not employ a primary organizational dataset, interviews, surveys, or experimental observations, the methodology focuses on theoretical interpretation and framework development. The objective is not to statistically test relationships but to construct a coherent model explaining how organizational management controls can strengthen information system auditing.

The methodological approach follows three analytical stages.

First, the literature was examined to identify recurring concepts concerning information system auditing and control. Second, these concepts were grouped into functional control dimensions. Third, the dimensions were integrated into a conceptual organizational management control framework.

3.2 Conceptual Framework Development

The proposed framework consists of six interconnected dimensions: governance and accountability, risk assessment, authorization and access control, operational control, monitoring and audit assurance, and corrective action.

Governance and accountability constitute the foundation of the framework. Management must establish responsibility for information systems, define authority, and ensure that control objectives are aligned with organizational objectives. Without clear accountability, weaknesses identified during auditing may not result in managerial action. Weber (2002) provides a foundation for viewing information-system control as an organizational responsibility rather than an exclusively technical function.

Risk assessment represents the second dimension. Information system auditing should identify potential risks affecting confidentiality, integrity, availability, reliability, and organizational operations. A hypothetical organization introducing a centralized financial information system, for example, may face risks associated with unauthorized access, inaccurate data modification, system interruption, or inappropriate user privileges. The audit process should therefore evaluate controls in relation to the organization's specific risk exposure rather than applying identical control expectations to every system.

Authorization and access control form the third dimension. Organizational management must determine who can access information, what activities users may perform, and under what circumstances access should be modified or withdrawn. Effective authorization reduces the possibility that users can perform activities beyond their legitimate responsibilities. In this respect, information system auditing must examine not only whether access restrictions technically exist but also whether management procedures support appropriate authorization.

The fourth dimension concerns operational controls. These include procedures governing system use, information processing, change management, data handling, backup processes, and continuity-related activities. Operational

controls translate management expectations into repeatable organizational practices. Their effectiveness depends on consistency between formally established procedures and actual employee behavior.

Monitoring and audit assurance constitute the fifth dimension. Controls cannot be assumed to remain effective indefinitely. Changes in technology, organizational structure, personnel responsibilities, and business processes can create new vulnerabilities. Continuous or periodic monitoring allows management to identify control deterioration and determine whether corrective measures are necessary. Namuduri's (2013) emphasis on going beyond compliance supports the argument that monitoring should evaluate actual control effectiveness rather than merely confirm the existence of documented procedures.

The sixth dimension is corrective action. Audit findings have organizational value only when weaknesses are addressed. Corrective controls should identify the responsible authority, establish an appropriate response, and determine whether the response has resolved the underlying weakness. A recurring audit finding, for example, may indicate not simply an isolated employee error but a structural weakness in management supervision.

3.3 Functional Relationship Among Controls

The framework is designed as an interconnected cycle rather than a linear sequence. Governance determines accountability; risk assessment identifies areas requiring attention; authorization and operational controls reduce identified risks; monitoring evaluates control performance; and corrective action addresses weaknesses. Results from corrective action subsequently influence governance and future risk assessment.

This cyclical relationship is significant because isolated controls may create a false perception of security. For example, an organization may possess technically sophisticated access restrictions while failing to review whether former employees' accounts have been removed. The technical control exists, but the management process governing the control is ineffective. Therefore, auditing should evaluate the entire control relationship.

Mehta (2024) supports the practical orientation required to examine information systems systematically, while Doshi and Patel (2022) provide a foundational basis for understanding the audit process. Together, these perspectives support a

framework in which control assessment connects formal requirements with actual organizational practice.

4. RESULTS

The conceptual analysis produces five principal findings regarding organizational management controls and information system auditing.

First, management accountability emerges as a foundational condition of effective information system control. Information systems cannot be controlled effectively when responsibility for authorization, monitoring, risk response, and corrective action is fragmented or ambiguous. The audit function should therefore examine whether management has established identifiable responsibility for system-related controls. This finding is consistent with the broader control orientation identified by Weber (2002), in which information systems control is connected with organizational processes rather than isolated technological mechanisms.

Second, the analysis indicates that control effectiveness is more significant than formal compliance. An organization may maintain policies and documented procedures while failing to implement them consistently. Consequently, an audit framework focused exclusively on documentation may overlook operational weaknesses. Namuduri (2013) is particularly relevant to this finding because the concept of going beyond compliance implies an evaluation of whether controls actually support organizational objectives.

Third, access and authorization controls should be evaluated as management processes as well as technical functions. User privileges represent organizational decisions concerning responsibility and authority. An inappropriate privilege may therefore reflect a weakness in managerial authorization rather than simply a technical configuration error. Effective auditing should consequently assess whether access rights correspond with current job responsibilities and whether changes in organizational roles trigger appropriate control responses.

Fourth, monitoring and corrective action determine whether the control system remains adaptive. Information systems and organizational structures continuously change, meaning that controls that were adequate at one point may become insufficient. A mature audit framework therefore requires recurring assessment and documented responses to identified weaknesses. Shah's (2021) discussion of the managerial role in information system auditing reinforces the importance of

connecting audit information with organizational decision-making.

Fifth, the findings indicate that an integrated framework provides stronger analytical value than isolated control assessments. Governance, risk assessment, access control, operations, monitoring, and corrective action are mutually dependent. Weakness in one dimension can reduce the effectiveness of other dimensions. For example, strong technical access restrictions may have limited value when management fails to review authorization requirements after employees change roles.

Overall, the findings suggest that information system auditing should be positioned as an organizational control mechanism rather than solely as a technology-focused inspection. The proposed framework provides a structured means of connecting audit activities with managerial responsibility, operational risk, and continuous improvement.

5. DISCUSSION

The findings have important theoretical implications for the understanding of information system auditing. The central theoretical proposition is that information system audit effectiveness depends on the integration of technological and organizational controls. Weber (2002) provides a foundational basis for this interpretation by connecting information systems control with audit processes. The present framework extends this perspective conceptually by emphasizing the interaction among governance, risk assessment, authorization, operations, monitoring, and corrective action.

The distinction between compliance and effectiveness is particularly important. Compliance can provide evidence that an organization has established formal requirements, but it does not necessarily establish that those requirements are functioning as intended. Namuduri (2013) provides the strongest basis among the supplied literature for this broader interpretation. From a management perspective, the relevant question is therefore not merely whether a control exists but whether the control reduces meaningful organizational risk.

The framework also demonstrates the importance of managerial involvement. Information system auditing can be weakened when responsibility is assigned exclusively to technical specialists. Technology professionals may identify system vulnerabilities, but management determines organizational priorities, allocates resources, establishes accountability, and decides how identified risks should be

addressed. Shah (2021) is relevant in this respect because the role of management-oriented professionals demonstrates the broader organizational significance of information system audit.

A major practical implication is that organizations should avoid designing audit programs around isolated technical checkpoints. Instead, auditors should examine relationships between control objectives and actual organizational practices. For instance, evaluating user access should involve consideration of authorization responsibilities, employee roles, monitoring practices, and procedures for correcting inappropriate access. Such an approach provides a more meaningful assessment than simply verifying the presence of password or authentication mechanisms.

The framework also involves trade-offs. Stronger controls may increase security and accountability but can simultaneously increase administrative complexity. Excessively restrictive authorization mechanisms may reduce operational flexibility, while insufficient restrictions may increase organizational risk. Consequently, effective management control requires proportionality between risk exposure and control intensity. The purpose of auditing should not be to maximize controls indiscriminately but to determine whether controls are appropriate for organizational circumstances.

Another limitation concerns the conceptual nature of the present study. Because the framework is derived exclusively from the five supplied references, it does not empirically test control effectiveness across specific industries or organizational sizes. The proposed relationships should therefore be interpreted as a theoretically grounded framework rather than a statistically validated model. Future empirical research could examine whether organizations applying the framework demonstrate measurable improvements in audit quality, control effectiveness, risk reduction, or management responsiveness.

The literature also suggests that practical implementation is essential. Mehta (2024) emphasizes the practical orientation of information systems auditing, while Doshi and Patel (2022) provide a foundational perspective on audit practice. Accordingly, the framework should be translated into organization-specific audit procedures rather than adopted as a rigid universal checklist. Different organizations will possess different systems, risks, governance structures, and regulatory environments.

Despite these limitations, the integrated perspective offers a useful conceptual contribution. It shifts attention from individual controls toward relationships among controls and management responsibilities. This is particularly important because information-system risk frequently emerges from interactions between technical weaknesses and organizational practices. An integrated audit therefore provides greater potential for identifying systemic weaknesses and supporting informed managerial decisions.

6. CONCLUSION

Information system auditing is increasingly significant because organizational activities depend heavily on reliable, secure, and appropriately controlled information systems. This study examined the relationship between organizational management controls and information system auditing and developed a conceptual framework integrating governance and accountability, risk assessment, authorization and access control, operational controls, monitoring, and corrective action.

The analysis demonstrates that effective information system auditing extends beyond technical inspection and formal compliance. Management accountability, risk-oriented evaluation, appropriate authorization, continuous monitoring, and corrective action are essential components of an effective organizational control environment. The framework further demonstrates that these components should operate as an interconnected cycle rather than as independent audit activities.

The principal contribution of the study is the integration of organizational management principles into a structured information system audit framework. The approach provides a conceptual basis for evaluating whether controls are not only formally established but also practically effective and organizationally aligned. It also emphasizes the importance of connecting audit findings with managerial responsibility and corrective action.

The study is limited by its conceptual methodology and reliance exclusively on the provided literature. Future research should empirically test the proposed framework across different organizational environments and examine its relationship with audit effectiveness, information-system reliability, risk reduction, and organizational performance. Such research could further refine the framework and establish measurable indicators for evaluating management

control maturity.

REFERENCES

1. Doshi H, Patel H. The Beginner's Guide to Information System Audit. Notion Press, Chennai, 2022.
2. Mehta AM. Auditing Information Systems- A Practical Approach. Conestoga Open Learning, Kitchener, 2024.
3. Namuduri K. Information Systems Auditing- Going Beyond Compliance. International Journal of Auditing Technology, 2013;1(1):45-51.
4. Shah S. Information System Audit-Role of CMAs. The Management Accountant, 2021;56(9):45-47.
5. Weber R. Information Systems Control and Audit. Pearson Education India, Noida, 2002.