

Information system audit and organizational performance: an integrative review of governance, controls, and implementation

ARTICLE INFORMATION

Umi Devina*

Master of Management Science
Study Program, Universitas Borneo
Tarakan, Jalan Amal Lama No. 1,
Kelurahan Pantai Amal, Kecamatan
Tarakan Timur, 77115, Tarakan,
North Kalimantan, Indonesia,
umidevina@gmail.com

Turni Azizah

Master of Management Science
Study Program, Universitas Borneo
Tarakan, Jalan Amal Lama No. 1,
Kelurahan Pantai Amal, Kecamatan
Tarakan Timur, 77115, Tarakan,
North Kalimantan, Indonesia,
turniazizah@gmail.com

* Corresponding author

Received : 13 August 2026

Accepted: 12 September 2026

ABSTRACT

Information system auditing has become a strategic assurance activity as organizations increasingly depend on digital systems for financial reporting, operational processes, managerial decision-making, and risk management. Although prior studies generally associate information technology (IT) governance, IT controls, internal auditing, and organizational capabilities with performance outcomes, the literature remains fragmented regarding the mechanisms through which information system audit activities generate organizational value. This study develops an integrative review of peer-reviewed literature to explain how information system audit effectiveness can contribute to organizational performance. The review synthesizes evidence across four mechanisms: information reliability and security, internal control and risk management, IT governance and strategic alignment, and implementation of audit recommendations. Evidence from empirical and conceptual studies indicates that audit effectiveness is better understood as an organizational process than as a stand-alone assurance output. IT governance capability can improve IT performance and subsequently business performance; weaknesses in IT internal controls are associated with adverse performance consequences; and internal-audit IT knowledge and competencies strengthen IT governance processes and IT controls. The review further identifies management support, board-level IT competence, governance maturity, and organizational readiness as important enabling conditions. On this basis, the study proposes an implementation-centered framework in which audit effectiveness influences organizational performance through governance and control mechanisms, with implementation acting as a critical transmission channel. The contribution of this study is to integrate information system auditing with accounting information systems and IT governance research and to specify mechanisms and boundary conditions that can be tested in future empirical studies.

Keywords: *Information system audit; IT governance; internal control; IT controls; audit effectiveness; organizational performance.*

INTRODUCTION

Digital transformation has changed the role of information systems from a supporting infrastructure into an organizational capability that influences reporting, operations, customer interaction, strategic decision-making, and risk management. The increasing dependence on information technology also increases organizational exposure to system failures, inaccurate information, unauthorized access, cybersecurity incidents, ineffective controls, and technology-related compliance failures. Such incidents frequently stem from socio-organizational factors, such as weak security awareness and non-compliant employee behavior, rather than purely technical deficiencies (Alkalbani et al., 2016). In accounting-intensive environments, these risks can affect the reliability of financial and managerial information and, ultimately, the quality of organizational decisions.

Information system auditing is therefore no longer appropriately viewed as a narrow technical examination. It is part of the broader assurance and governance architecture through which organizations evaluate whether technology resources are controlled, risks are managed, information is reliable, and IT activities support organizational objectives. The governance perspective is consistent with the classic IT governance literature, which emphasizes decision rights, accountability, organizational structures, processes, and relational mechanisms as foundations for realizing value from IT (Weill & Ross, 2004; Peterson, 2004; Van Grembergen et al., 2004).

From an accounting information systems perspective, the relevance of IT controls is particularly strong because accounting processes increasingly depend on automated applications, databases, interfaces, access

controls, system-generated evidence, and continuous data flows (Hall, 2021). Weaknesses in IT controls can therefore become organizational liabilities rather than isolated technical deficiencies. Empirical evidence by Stoel and Muhanna (2011) shows that firms reporting material IT internal control weaknesses had lower accounting performance, while more recent research continues to examine how IT general controls influence organizational and market outcomes.

At the same time, information system audit should not be assumed to have a direct and automatic effect on organizational performance. An audit report is an intermediate output. Performance improvements occur only when identified weaknesses are prioritized, assigned to responsible parties, corrected, monitored, and embedded in organizational routines. This implementation perspective is consistent with the IT business-value literature, which argues that technology creates value through complementary organizational resources, capabilities, and processes rather than through technology investment alone (Melville et al., 2004; Bharadwaj, 2000).

Empirical evidence increasingly supports this more nuanced interpretation. Lunardi et al. (2014) found that firms adopting IT governance mechanisms improved their performance relative to a control group, particularly profitability. Wu et al. (2024), using data from 414 Taiwanese internal auditors, found positive relationships between IT knowledge, internal-audit roles, IT-audit competencies, IT governance processes, and IT control effectiveness. Turel et al. (2019) demonstrated that board IT governance should be understood in conjunction with IT operating capabilities, while Caluwe et al. (2024) emphasized the need for IT governance to become an integral part of corporate governance. More recent work has also connected IT governance process capability to IT performance and business performance (Pereira et al., 2022) and examined how audit digitalization can reduce internal control weaknesses through digital governance (Shi & Zhang, 2025).

Despite these developments, the literature remains dispersed across several research traditions. Information system auditing research often focuses on assurance, control objectives, maturity, and audit frameworks. IT governance research focuses on decision rights, strategic alignment, capabilities, board involvement, and value creation. Internal auditing research emphasizes audit competence, assurance quality, and control effectiveness. Accounting research frequently examines the consequences of IT control weaknesses for reporting quality and firm performance. The absence of an integrated mechanism-based synthesis makes it difficult to explain precisely how these streams connect.

This study addresses that problem by developing an integrative review around three research questions. RQ1 asks: How does information system auditing contribute to organizational performance? RQ2 asks: Through what organizational mechanisms are audit activities translated into performance outcomes? RQ3 asks: What organizational conditions strengthen or weaken the realization of audit benefits? These questions deliberately move beyond a simple positive-versus-negative classification of prior findings and focus on mechanisms, boundary conditions, and implementation.

Building on this overall contribution, the review advances three specific points. First, it integrates information system auditing, IT governance, internal controls, and organizational performance into a single explanatory framework. Second, it identifies implementation of audit recommendations as a critical transmission mechanism between assurance and performance. Third, it identifies auditor IT competence, management support, board-level IT competence, governance maturity, and organizational readiness as boundary conditions that help explain variation in audit outcomes. The framework is intended to provide a stronger conceptual foundation for future empirical research in accounting information systems and management.

LITERATURE REVIEW

Information System Audit as an Organizational Assurance Mechanism

Information system auditing evaluates whether information systems and related controls are designed and operating in a manner consistent with organizational objectives, risk tolerance, reporting requirements, and security expectations. The audit perspective encompasses access management, change management, system development, data integrity, business continuity, application controls, IT general controls, and governance processes. The COBIT tradition is especially relevant because it connects IT control objectives with enterprise governance and assurance rather than treating technology as an isolated technical function (Tuttle & Vandervelde, 2007; De Haes & Van Grembergen, 2009b).

The effectiveness of information system audit depends on more than technical procedures. Auditor competence, access to relevant evidence, organizational independence, communication with management, and

the capacity to understand business processes influence whether audit work produces useful assurance. The internal-audit perspective is particularly important because internal auditors operate at the intersection of governance, risk management, internal control, and organizational improvement. Wu et al. (2024) demonstrate that IT knowledge and IT-audit competencies are associated with stronger IT governance processes and IT controls, providing empirical support for the capability dimension of audit effectiveness.

IT Internal Controls and Organizational Performance

IT internal controls are mechanisms designed to protect information and systems, preserve confidentiality, integrity, and availability, support reliable processing, and reduce the likelihood or impact of technology-related failures. Their organizational value extends beyond compliance. Stoel and Muhanna (2011) conceptualize IT internal control weaknesses as organizational liabilities and find that firms with reported material IT control weaknesses exhibit lower accounting performance. This evidence is important because it provides a direct empirical link between IT control quality and organizational performance rather than treating controls merely as regulatory requirements.

The control perspective is reinforced by Li et al. (2008), who examine internal and external influences on IT control governance and show that senior management, board characteristics, and IT leadership are relevant to the quality of IT control governance. Such evidence indicates that IT controls are embedded in organizational structures. Control quality is therefore partly a governance outcome, not simply a technical design outcome.

IT Governance, Decision Rights, and Strategic Alignment

IT governance concerns how organizations direct and control IT-related decisions and resources, an issue long framed as a matter of multiple contingencies rather than a single universal arrangement (Sambamurthy & Zmud, 1999). Weill and Ross (2004) emphasize decision rights and accountability as central mechanisms, while Peterson (2004) and Van Grembergen et al. (2004) conceptualize governance through structures, processes, and relational mechanisms. De Haes and Van Grembergen (2009a) further show that mature combinations of IT governance practices are associated with higher business/IT alignment maturity. These perspectives explain why an information system audit can have limited strategic value if its findings are disconnected from decision rights, organizational priorities, and resource allocation.

The relationship between IT governance and performance has received substantial empirical attention. Lunardi et al. (2014) report improved performance among firms adopting IT governance mechanisms. Zhang et al. (2016) show that IT governance is an antecedent of IT capability and that IT capability contributes to firm performance. Hamdan et al. (2019) provide evidence from Saudi Arabia that IT governance is positively related to operational performance, although not all performance dimensions respond equally. Pereira et al. (2022) further show that IT governance process capability improves IT performance, which then contributes to business performance. These findings suggest a mediated pathway rather than a simplistic direct effect.

IT Capability and the Business Value of Technology

The resource-based view provides a theoretical explanation for why governance and audit mechanisms can influence performance. Bharadwaj (2000) conceptualizes IT capability as the ability to mobilize and deploy IT resources together with human and organizational resources and finds that superior IT capability is associated with firm performance. Melville et al. (2004) similarly argue that IT business value depends on complementary organizational resources and the broader competitive environment. Thus, audit findings may create value when they improve the organizational capabilities that enable technology to support business processes.

Ilmudeen (2024) extends this logic by linking IT governance mechanisms to IT-enabled dynamic capabilities, business process agility, innovation capability, and firm performance. Dynamic-capability reasoning is useful for information system auditing because it emphasizes the ability to sense, respond, reconfigure, and continuously improve rather than merely comply with static control requirements.

Board-Level IT Governance and Corporate Governance

As organizations become more digitally dependent, IT governance increasingly intersects with corporate governance. Li et al. (2008) show that senior-management and board characteristics are associated with IT control governance. Turel et al. (2019) argue that board IT governance and IT operating capabilities should be

considered jointly, while Caluwe et al. (2024) identify board roles and IT competence as important for embedding IT governance within corporate governance. This stream of research implies that information system audit findings concerning technology risk may require board-level attention when risks affect strategy, reporting, resilience, or enterprise value.

COBIT and Structured IT Governance

COBIT is widely used to structure governance and management objectives, assess capability, identify control gaps, and organize improvement actions (ISACA, 2019; De Haes et al., 2019). Tuttle and Vandervelde (2007) empirically examine COBIT as an internal control framework for information technology, while De Haes and Van Grembergen (2009b) discuss COBIT as a framework for enterprise governance and IT assurance. Later editions and applications of COBIT have expanded its relevance to enterprise governance, risk, value, and performance. However, the framework should not be interpreted as a universal causal mechanism. COBIT provides structure; organizational capabilities determine whether that structure produces effective implementation.

Digitalization, DevOps, and Changing IT Control Environments

Contemporary information system auditing must also respond to changes in how technology is developed and operated. Plant et al. (2022) argue that DevOps environments combine manual and automated controls and require new approaches to IT governance and auditing. This development is important because traditional periodic audit approaches may be insufficient where systems change continuously and control activities are embedded in automated pipelines. Audit effectiveness therefore increasingly requires technical competence, continuous monitoring, and understanding of automated control environments.

Information Quality and Decision Usefulness

Information quality is an important intermediate mechanism connecting IT governance and organizational performance. Saragih et al. (2024) examine IT governance and internal information quality and their relationship with corporate tax savings, showing that governance and information quality can jointly shape organizational outcomes. This supports the argument that audit value is partly realized through better information rather than through audit activity itself.

Recent Digital Governance Evidence

Recent evidence strengthens the implementation-centered perspective. Shi and Zhang (2025) find that audit digitalization decreases the occurrence and number of internal control weaknesses and facilitates corporate IT governance. Benaroch (2025) develops and empirically validates a model of IT general-control pervasiveness and shows that investors attach value relevance to deficiencies that are more pervasive and connected to cyber incidents. These studies indicate that the organizational consequences of IT controls are increasingly visible through both internal governance outcomes and external valuation responses.

Research Framework

The literature supports an implementation-centered pathway in which information system audit effectiveness influences organizational performance through four mechanisms: information reliability and security; internal control and risk management; IT governance and strategic alignment; and implementation of audit recommendations. Auditor IT competence, management support, governance capability, and organizational readiness operate as enabling conditions.

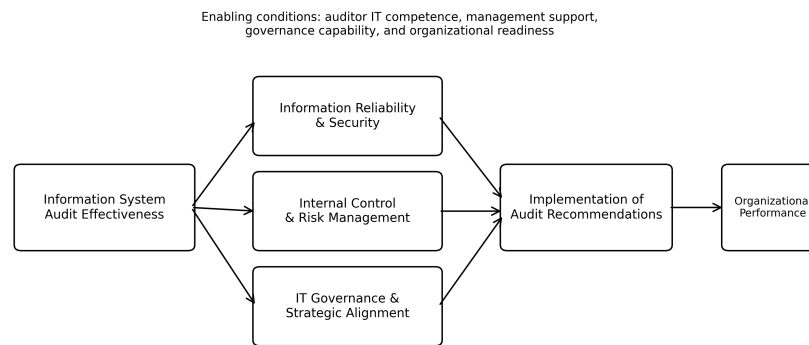


Figure 1. Implementation-centered framework linking information system audit effectiveness to organizational performance.

METHODOLOGY

Research Design

This study uses an integrative literature review rather than a fully reproducible systematic literature review. The distinction is deliberate: an integrative review synthesizes conceptual and empirical evidence around a defined set of research questions, whereas a systematic review additionally requires documented search records, database-specific counts, explicit screening decisions, complete study metadata, and risk-of-bias assessments (Snyder, 2019; Tranfield et al., 2003). Because these elements are outside the scope of the present study, systematic-review status is not claimed. The present review instead synthesizes verified peer-reviewed evidence and explicitly identifies this methodological boundary.

Search Orientation and Eligibility

The literature was oriented around combinations of the following concepts: information system audit, IT audit, IT governance, internal audit, IT controls, COBIT, information quality, IT capability, organizational performance, firm performance, risk management, and digital governance. Priority was given to peer-reviewed journal articles and authoritative scholarly books or professional frameworks that directly informed the conceptual development. Seminal sources were retained where they established foundational constructs, while recent studies were emphasized for contemporary evidence.

Analytical Procedure

Each source was assessed against four analytical questions: what audit or governance mechanism is examined; what organizational outcome is reported; what mechanism connects the governance or control activity to the outcome; and what contextual or organizational conditions influence the relationship. The evidence was then synthesized thematically. Because the studies differ substantially in constructs, samples, methods, and outcomes, statistical meta-analysis was not attempted.

Quality and Transparency

The review follows the transparency principles of literature-review methodology but does not claim PRISMA-complete reporting. Systematic-review terms such as "eligibility" and "PRISMA" are used here only as reference points to make the review's methodological boundary explicit, not to imply that a full systematic-review protocol was followed. PRISMA 2020 requires explicit reporting of eligibility criteria, information sources, search strategies, study-selection procedures, and other review processes (Page et al., 2021). A future systematic extension should therefore document exact search strings, database dates, duplicate removal, title/abstract screening, full-text exclusions, quality appraisal, and a PRISMA flow diagram.

RESULTS

RQ1: How Does Information System Auditing Contribute to Organizational Performance?

The evidence indicates that information system auditing contributes to performance primarily through improvements in organizational control and governance rather than through the audit report itself. The strongest direct evidence concerns IT control quality. Stoel and Muhanna (2011) find that material IT internal control weaknesses are associated with lower accounting performance, indicating that poor IT controls can impose an organizational liability. As with most evidence reviewed in this study, this relationship is correlational; the underlying research designs do not establish the direction of causality between IT-control quality and organizational performance. Even so, it provides an important performance rationale for auditing IT controls.

IT governance studies provide a second stream of evidence. Lunardi et al. (2014) find that adoption of IT governance mechanisms is associated with improved organizational and financial performance. Pereira et al. (2022) show that IT governance process capability improves IT performance, which then improves business performance. Zhang et al. (2016) similarly demonstrate the role of IT governance in developing IT capability and firm performance. Together, these findings suggest that governance and control mechanisms can affect performance when they improve the organization's ability to deploy IT resources effectively.

The contribution of information system audit is therefore best conceptualized as assurance-enabled organizational improvement. Audit identifies weaknesses and risks; governance determines accountability and resource allocation; management implements corrective actions; and organizational capabilities determine whether the changes are sustained. The audit is a critical input into this chain but not the final outcome.

RQ2: Through What Mechanisms Are Audit Activities Translated into Performance?

Four mechanisms recur across the evidence. The first is information reliability and security. Effective controls improve the integrity, availability, and reliability of information used for reporting and decision-making. The second is internal control and risk management. Audit findings identify weaknesses and help management prioritize mitigation. The third is IT governance and strategic alignment. Governance structures ensure that technology decisions are connected to organizational objectives and accountability. The fourth is implementation of audit recommendations. This mechanism transforms assurance findings into actual process and control changes.

The importance of mediation is consistent with IT business-value theory. Melville et al. (2004) argue that IT creates value through complementary organizational resources, while Bharadwaj (2000) emphasizes organizational IT capability. Consequently, an audit can influence performance only if its findings strengthen the complementary resources and capabilities through which IT creates value.

RQ3: What Conditions Strengthen or Weaken Audit Benefits?

Auditor competence is a central enabling condition. Wu et al. (2024) find that IT knowledge and IT-audit competencies are positively associated with IT governance processes and control effectiveness. Management and board involvement are also important. Li et al. (2008) show that senior-management and board characteristics are associated with IT control governance, while Caluwe et al. (2024) emphasizes board roles and IT competence in integrating IT governance into corporate governance.

Organizational maturity and capability also matter. De Haes and Van Grembergen (2009a) show that organizations using a combination of mature governance practices exhibit higher business/IT alignment maturity. Pereira et al. (2022) demonstrate that IT governance process capability is linked to business performance through IT performance. These findings suggest that the same audit recommendation may have different effects across organizations depending on their capacity to implement and institutionalize change.

Table 1. Evidence Synthesis

RQ	Mechanism	Main evidence	Boundary condition	Research implication
RQ1	Control and governance improvement	IT control weaknesses are associated with lower performance (Stoel & Muhanna, 2011); IT governance adoption/capability is associated with improved IT or business performance (Lunardi et al., 2014; Pereira et al., 2022).	Governance maturity and organizational capability.	Audit effects should be evaluated through downstream organizational outcomes.
RQ2	Information quality; internal control; IT governance; implementation	Evidence converges on indirect pathways from audit/control to	Management follow-through and resource availability.	Recommendation implementation should be modeled as a mediator.

		performance (Melville et al., 2004; Bharadwaj, 2000).		
RQ3	Competence, leadership, board involvement, governance capability	Internal-audit IT competence and board/management IT capabilities strengthen governance and controls (Wu et al., 2024; Li et al., 2008).	Organizational readiness and context.	Future studies should test moderation and contingency effects.

DISCUSSION

The central finding is that information system audit should be conceptualized as an implementation-dependent governance capability. This interpretation differs from a compliance-centered model in which audit success is measured primarily by the completion of audit procedures or the number of findings issued. Under an implementation-centered model, audit quality is necessary but not sufficient. Organizational value depends on whether findings are understood, prioritized, assigned, corrected, monitored, and integrated into governance routines.

This finding also explains why the empirical literature does not always show uniform relationships between IT governance and performance. Hamdan et al. (2019) find a positive effect on operational performance but not necessarily across all performance dimensions. Permatasari (2025), in an Indonesian manufacturing setting, reports no significant effect of IT governance implementation on firm performance. Because this finding is drawn from a single-country, single-industry setting, it should be read as evidence that context and implementation maturity condition outcomes rather than as a direct contradiction of the broader cross-country evidence reported by Lunardi et al. (2014) and Pereira et al. (2022). Such differences should not automatically be treated as contradictions. They may reflect differences in governance maturity, measurement, implementation period, industry context, and the organization's ability to convert governance practices into capabilities.

The temporal dimension is especially important. Lunardi et al. (2014) report that performance improvements become more evident after adoption, while Pereira et al. (2022) identify a sequential pathway from governance process capability to IT performance and then business performance. This suggests that audit and governance interventions may require organizational learning and process adaptation before performance effects become visible. A cross-sectional design may therefore underestimate long-term benefits.

The findings also reinforce the importance of integrating IT governance with corporate governance. Technology-related risks increasingly affect financial reporting, business continuity, cybersecurity, regulatory exposure, and strategic investment. Caluwe et al. (2024) argues that IT governance should become an integral component of corporate governance, while Li et al. (2008) provides evidence that board and senior-management characteristics are associated with IT control governance. Audit committees and boards therefore have a role in ensuring that significant IT audit findings are treated as enterprise risks when appropriate.

COBIT remains valuable as a governance and assurance structuring mechanism, but the evidence does not support treating framework adoption as a sufficient condition for performance. COBIT can clarify objectives, responsibilities, capability levels, and improvement priorities; however, implementation depends on people, decision rights, resources, organizational culture, and management commitment. The practical implication is that organizations should evaluate COBIT-based audit programs by the extent to which identified gaps are closed and organizational capabilities improve, rather than by maturity scores alone.

The changing technology environment also requires audit methodologies to evolve. Plant et al. (2022) demonstrate that DevOps environments alter the control environment by combining automated and manual controls. Shi and Zhang (2025) show that audit digitalization can reduce internal control weaknesses and facilitate digital governance. Benaroch (2025) further demonstrates that the pervasiveness of IT general-control deficiencies matters for market value. Together, these studies indicate that future information system auditing will increasingly require continuous, risk-based, data-enabled approaches.

6.1 Theoretical Implications

The study contributes theoretically by connecting three streams that are often separated: information system audit, IT governance, and IT business value. The proposed framework treats audit effectiveness as an upstream assurance capability and organizational performance as a downstream outcome. Information quality, internal control, risk management, governance alignment, and recommendation implementation serve as mechanisms, while organizational capabilities serve as boundary conditions. This structure provides a basis for future mediation and moderation testing.

6.2 Practical Implications

Organizations should broaden the evaluation of information system audit effectiveness. In addition to audit completion and finding counts, management should monitor remediation rates, time to close high-risk findings, recurrence of control weaknesses, changes in residual risk, information-quality indicators, control automation, and evidence that IT investments remain aligned with organizational priorities. Audit committees should require formal ownership and deadlines for material recommendations and should monitor unresolved issues through governance mechanisms.

For internal-audit functions, the evidence suggests that investment in IT knowledge is strategically important. Auditors need sufficient understanding of IT governance, cybersecurity, data architecture, automated controls, cloud environments, and system development to evaluate technology risks credibly. The objective is not to turn every internal auditor into a software engineer but to ensure that the audit function has the collective competence required to assess technology-dependent business processes.

6.3 Limitations and Future Research

The main limitation is methodological scope. Because this study does not provide a complete reproducible systematic-search record, it cannot claim the comprehensiveness of a PRISMA systematic review or statistical meta-analysis. The evidence base is also heterogeneous in terms of countries, industries, constructs, research methods, and performance measures. Accordingly, the findings should be interpreted as an integrative synthesis rather than as estimates of a universal causal effect.

Future research should conduct a fully reproducible systematic review using Scopus, Web of Science, ScienceDirect, and relevant accounting and information-systems databases. The protocol should specify exact search strings, publication windows, eligibility criteria, duplicate removal, screening, full-text exclusion reasons, and quality appraisal. Empirical research should then test the proposed model using longitudinal or panel data where possible. In particular, future studies should examine whether implementation of audit recommendations mediates the relationship between audit quality and organizational performance and whether auditor IT competence, management support, governance maturity, and board IT competence moderate the relationship.

CONCLUSION

This study reviewed the literature on information system auditing, IT governance, internal controls, IT capabilities, and organizational performance and developed an implementation-centered framework for explaining how audit activities can create organizational value. The evidence indicates that information system audit is most valuable when it strengthens information reliability, internal control, risk management, and IT governance and when findings are translated into corrective action.

The study also demonstrates that audit benefits are conditional. Auditor IT competence, management support, board-level IT competence, governance maturity, and organizational readiness influence whether audit findings lead to sustained improvements. The relationship between governance and performance is therefore better understood as a process involving multiple organizational mechanisms rather than as a simple direct effect.

For accounting and management practice, the implication is clear: information system audit should be evaluated not only by the quality of assurance work but also by the organizational consequences of that work. For research, the framework provides testable mechanisms and boundary conditions that can be examined through longitudinal, panel, survey, or mixed-method designs. A future fully documented systematic review and meta-analysis would provide an important next step in establishing the strength and generalizability of these relationships.

REFERENCES

- Alkalbani, A., Deng, H., & Kam, B. (2016). Investigating the role of socio-organizational factors in information security compliance in organizations. *International Journal of Information Management*, 36(6), 947–957.

- Benaroch, M. (2025). Measuring the pervasiveness of IT general controls: A model and empirical validation. *International Journal of Accounting Information Systems*, 56, 100752. <https://doi.org/10.1016/j.accinf.2025.100752>
- Bharadwaj, A. S. (2000). A resource-based perspective on information technology capability and firm performance: An empirical investigation. *MIS Quarterly*, 24(1), 169–196.
- Caluwe, L., Wilkin, C. L., De Haes, S., & Huygh, T. (2024). Board roles required for IT governance to become an integral component of corporate governance. *International Journal of Accounting Information Systems*, 54, 100694. <https://doi.org/10.1016/j.accinf.2024.100694>
- De Haes, S., & Van Grembergen, W. (2009a). An exploratory study into IT governance implementations and its impact on business/IT alignment. *Information Systems Management*, 26(2), 123–137. <https://doi.org/10.1080/10580530902794786>
- De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2019). *Enterprise governance of information technology: Achieving alignment and value in digital organizations*. Springer. <https://doi.org/10.1007/978-3-030-25918-1>
- De Haes, S., & Van Grembergen, W. (2009b). *Enterprise governance of information technology: Achieving strategic alignment and value*. Springer. <https://doi.org/10.1007/978-0-387-84882-2>
- Hamdan, A., Khamis, R., Anasweh, M., Al-Hashimi, M., & Razzaque, A. (2019). IT governance and firm performance: Empirical study from Saudi Arabia. *SAGE Open*, 9(2). <https://doi.org/10.1177/2158244019843721>
- Hall, J. A. (2021). *Accounting information systems* (10th ed.). Cengage.
- Ilmudeen, A. (2024). IT governance mechanism and IT-enabled dynamic capabilities drives firm performance: An empirical study in Sri Lanka. *Information Development*, 40(1), 3–19. <https://doi.org/10.1177/02666669221074259>
- ISACA. (2019). *COBIT 2019 framework: Governance and management objectives*. ISACA.
- Li, C., Lim, J.-H., & Wang, Q. (2008). Internal and external influences on IT control governance. *International Journal of Accounting Information Systems*, 9(4), 225–239. <https://doi.org/10.1016/j.accinf.2007.09.002>
- Lunardi, G. L., Becker, J. L., Maçada, A. C. G., & Dolci, P. C. (2014). The impact of adopting IT governance on financial performance: An empirical analysis among Brazilian firms. *International Journal of Accounting Information Systems*, 15(1), 66–81. <https://doi.org/10.1016/j.accinf.2013.02.001>
- Melville, N., Kraemer, K., & Gurbaxani, V. (2004). Information technology and organizational performance: An integrative model of IT business value. *MIS Quarterly*, 28(2), 283–322.
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, n71. <https://doi.org/10.1136/bmj.n71>
- Pereira, C. M. L., da Silva, M. M., & de Carvalho, J. Á. (2022). Impact of IT governance process capability on business performance: Theory and empirical evidence. *Decision Support Systems*, 153, 113668. <https://doi.org/10.1016/j.dss.2021.113668>
- Permatasari, Y. (2025). The influence of IT governance implementation on firm performance in manufacturing companies. *Journal of Applied Accounting and Taxation*, 10(1), 1–11. <https://doi.org/10.30871/jaat.v10i1.7020>
- Peterson, R. (2004). Crafting information technology governance. *Information Systems Management*, 21(4), 7–22. <https://doi.org/10.1201/1078/44705.21.4.20040901/84183.2>
- Plant, O. H., van Hillegersberg, J., & Aldea, A. (2022). Rethinking IT governance: Designing a framework for mitigating risk and fostering internal control in a DevOps environment. *International Journal of Accounting Information Systems*, 45, 100560. <https://doi.org/10.1016/j.accinf.2022.100560>
- Sambamurthy, V., & Zmud, R. W. (1999). Arrangements for information technology governance: A theory of multiple contingencies. *MIS Quarterly*, 23(2), 261–290.
- Saragih, A. H., Ali, S., Suwardi, E., & Utomo, H. (2024). Finding the missing pieces to an optimal corporate tax savings: Information technology governance and internal information quality. *International Journal of Accounting Information Systems*, 52, 100665. <https://doi.org/10.1016/j.accinf.2023.100665>

- Shi, W., & Zhang, Z. (2025). Exploring the role of digital governance: The effect of audit digitalization on firms' internal control weaknesses in China. *International Journal of Accounting Information Systems*, 56, 100756. <https://doi.org/10.1016/j.accinf.2025.100756>
- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339. <https://doi.org/10.1016/j.jbusres.2019.07.039>
- Stoel, M. D., & Muhanna, W. A. (2011). IT internal control weaknesses and firm performance: An organizational liability lens. *International Journal of Accounting Information Systems*, 12(4), 280–304. <https://doi.org/10.1016/j.accinf.2011.06.001>
- Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management*, 14(3), 207–222. <https://doi.org/10.1111/1467-8551.00375>
- Turel, O., Liu, P., & Bart, C. (2019). Is board IT governance a silver bullet? A capability complementarity and shaping view. *International Journal of Accounting Information Systems*, 33, 32–46. <https://doi.org/10.1016/j.accinf.2019.03.002>
- Tuttle, B., & Vandervelde, S. D. (2007). An empirical examination of CobiT as an internal control framework for information technology. *International Journal of Accounting Information Systems*, 8(4), 240–263. <https://doi.org/10.1016/j.accinf.2007.09.001>
- Van Grembergen, W., De Haes, S., & Guldentops, E. (2004). Structures, processes and relational mechanisms for IT governance. In W. Van Grembergen (Ed.), *Strategies for information technology governance* (pp. 1–36). IGI Global. <https://doi.org/10.4018/978-1-59140-140-7.ch001>
- Weill, P., & Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business School Press.
- Wu, T.-H., Huang, S.-Y., Chiu, A.-A., & Yen, D. C. (2024). IT governance and IT controls: Analysis from an internal auditing perspective. *International Journal of Accounting Information Systems*, 52, 100663. <https://doi.org/10.1016/j.accinf.2023.100663>
- Zhang, P., Zhao, K., & Kumar, R. (2016). Impact of IT governance and IT capability on firm performance. *Information Systems Management*, 33(4), 291–302. <https://doi.org/10.1080/10580530.2016.1220218>

APPENDIX

This appendix outlines a proposed search and reporting protocol for extending the present integrative review into a fully reproducible systematic review. A future systematic extension should register this protocol before screening begins. Suggested databases are Scopus, Web of Science, ScienceDirect, and selected accounting and information-systems indexes. A search string may combine: ("information system audit" OR "IT audit" OR "information systems assurance") AND ("IT governance" OR COBIT OR "internal control" OR "IT controls") AND ("organizational performance" OR "firm performance" OR efficiency OR "business value"). The review should report database coverage, search dates, exact strings, filters, duplicate removal, screening decisions, full-text exclusion reasons, quality assessment, extraction fields, and a PRISMA 2020 flow diagram.

Recommended extraction fields include publication year, country, industry, sample size, research design, audit construct, governance construct, IT-control construct, mediator, moderator, performance measure, main findings, limitations, and theoretical perspective. Quality appraisal should assess construct validity, sampling adequacy, measurement reliability, analytical transparency, and risk of bias. Where studies provide comparable effect sizes, a meta-analysis can be considered; otherwise, a structured qualitative synthesis should be retained