Integrated System and Management Technology

E-ISSN: 3123-9811

Research Article

Examining the Role of Information Technology Governance in Enhancing Risk Management Performance and Regulatory Compliance in Multinational Digital Enterprises

Gunawan Prayitno [1*], Ronaldo Aprili [2]

1 Sekolah Tinggi Manajemen Informatika dan Komputer Pesat Nabire, Indonesia; email: binaanakpapua@gmail.com
2 Universitas Sains dan Teknologi Komputer, Indonesia
* Corresponding Author : Gunawan Prayitno

Abstract: This study investigates the role of Information Technology (IT) governance in enhancing risk management performance and ensuring regulatory compliance within multinational digital enterprises. As digital transformation continues to reshape the global business landscape, organizations face increasing challenges in managing technological risks and complying with complex regulatory requirements across various jurisdictions. The study adopts a quantitative approach, using a survey methodology to collect data from senior IT and compliance managers in multinational digital enterprises. The survey focuses on how IT governance frameworks, such as COBIT 2019 and ISO 27000, are utilized to align IT strategies with business objectives, mitigate risks, and maintain regulatory compliance. The findings indicate that organizations with well-established IT governance structures are better positioned to proactively identify and mitigate risks, ensuring greater consistency in meeting regulatory requirements. These organizations demonstrate improved risk management effectiveness, especially concerning cybersecurity, data privacy, and compliance with global regulations like GDPR. In contrast, organizations with ad hoc or decentralized governance structures struggle with fragmented risk management and compliance efforts. The study further highlights the importance of integrating IT governance frameworks with internal audit functions, specifically the Chief Audit Executive (CAE), to enhance cybersecurity resilience and ensure compliance with global standards. This research contributes to the literature by providing empirical evidence on the integration of IT governance, risk management, and regulatory compliance in multinational enterprises. It also highlights the need for a structured and systematic approach to IT governance to improve organizational performance in managing risks and ensuring consistent regulatory adherence. The study offers practical insights for organizations looking to optimize their IT governance structures in the face of rapid digital transformation.

Keywords: IT governance; risk management; regulatory compliance; digital enterprises; multinational organizations.

Received: November 20, 2025
Revised: Desember 30, 2025
Accepted: January 14, 2026
Published: January 19, 2026
Curr. Ver.: January 19, 2026

1. Introduction

The rapid advancement of digital technologies has fundamentally transformed the global business environment, creating both unprecedented opportunities and significant challenges for multinational enterprises (MNEs). One of the primary challenges MNEs face is managing the increasing complexity of technological risks while ensuring compliance with a highly fragmented and evolving regulatory landscape [1]. These risks-ranging from cybersecurity threats to the complexities of cross-border data privacy regulations-demand robust risk management mechanisms and compliance frameworks. Furthermore, the dynamic nature of global digital markets, influenced by geopolitical tensions and the ongoing digital

transformation, requires a comprehensive approach to governance that integrates technology, risk management, and compliance mechanisms [2].

As MNEs become increasingly interdependent through digital technologies, new vulnerabilities arise. Cybersecurity risks, for example, are exacerbated by emerging technologies like Artificial Intelligence (AI), the Internet of Things (IoT), and Cloud Computing, which introduce unprecedented threats to organizational data and infrastructure [3]. These technologies, while transformative, also necessitate advanced risk assessment strategies to protect against cascading failures and cyberattacks. Similarly, data privacy concerns are compounded by the complex web of regulations governing cross-border data flows. With stringent regulations like the European Union's General Data Protection Regulation (GDPR), MNEs are required to develop proactive strategies such as data mapping, continuous monitoring, and risk assessments to remain compliant [4].

Moreover, the ongoing global economic shifts, exacerbated by events like the COVID-19 pandemic, have highlighted the vulnerabilities in MNEs' global value chains. This environment has made it even more crucial for enterprises to adopt adaptable risk management practices that can withstand crises and geopolitical tensions (Chatterjee et al., 2024). The pandemic underscored the need for resilience, pushing companies to rethink how they manage risks and ensure compliance across multiple jurisdictions [5].

The regulatory landscape in which MNEs operate is also marked by increasing scrutiny and complexity. As digital platforms continue to proliferate, regulators around the world are tightening their grip on online operations. The European Union, for example, has introduced stringent regulations aimed at digital platforms to foster a safer, more transparent online environment [6]. These regulatory complexities require MNEs to implement effective governance mechanisms that can navigate various legal requirements while safeguarding their digital operations.

To effectively address these challenges, MNEs must integrate advanced Information Technology (IT) governance structures into their overall risk management and compliance strategies. IT governance frameworks, such as COBIT and ITIL, can provide the necessary structures to assess, monitor, and mitigate risks while ensuring compliance with regulatory standards [7]. Furthermore, integrating Corporate Social Responsibility (CSR) with Enterprise Risk Management (ERM) practices has proven to enhance stakeholder relationships and improve overall risk mitigation efforts, especially in the context of digital transformation [8].

The digital transformation of enterprises has significantly altered the landscape of global business, introducing new risks and complexities, particularly in the realms of risk management and regulatory compliance. The increasing interdependence of digital systems, coupled with the rapid pace of technological advancements, makes it essential for organizations to integrate effective IT governance frameworks. These frameworks ensure that risk management practices are aligned with organizational objectives and regulatory requirements, thus improving overall performance in risk mitigation and compliance [9].

IT governance structures are fundamental in aligning technology with business goals, particularly in multinational enterprises (MNEs). These governance mechanisms are essential for embedding risk management practices into organizational processes, thereby enhancing the capacity to identify, assess, and mitigate risks. According to [10], governance frameworks such as COBIT 2019 are designed to assess the effectiveness of IT governance, helping organizations align IT strategies with business objectives. This alignment is critical for mitigating risks, especially in environments characterized by rapidly evolving technologies like artificial intelligence (AI) and cloud computing.

Furthermore, robust IT governance ensures that risk management is not treated as a separate function but is integrated into every aspect of the organization’s operations. This integration enables businesses to continuously adapt to new risks while maintaining operational efficiency [11]. It is particularly important for enterprises to integrate Corporate Social Responsibility (CSR) and Enterprise Risk Management (ERM) frameworks, which can enhance compliance efforts and improve organizational resilience in the face of technological disruptions [12].

The increasing complexity of global regulatory frameworks poses a significant challenge for organizations. As digital enterprises expand, they must navigate a maze of regulations across different jurisdictions, which makes compliance both challenging and costly. Data governance, a subset of IT governance, plays a crucial role in ensuring data security, integrity, and compliance with regulations such as GDPR, HIPAA, and CCPA [13]. Effective IT governance structures embed compliance into daily business processes, ensuring that organizations meet regulatory requirements consistently and efficiently [14].

The integration of governance, risk management, and compliance (GRC) frameworks is crucial for organizations to meet regulatory demands while maintaining operational efficiency. These frameworks provide a structured approach that enables companies to continuously monitor and adapt to evolving regulatory requirements, ensuring compliance across the organization [15]. Moreover, continuous monitoring of IT governance practices is essential to maintain compliance and respond to new regulatory changes [16].

In a digital enterprise setting, effective IT governance is crucial for addressing the myriad challenges associated with technological risks and regulatory compliance. As organizations undergo digital transformations, they encounter new risks that necessitate continuous updates to their governance frameworks. Advanced technologies such as AI and machine learning can enhance risk management capabilities, but they also require strong governance to manage their ethical and regulatory implications [16]. Effective IT governance structures help organizations navigate these complexities by ensuring that risk management practices are aligned with the evolving technological landscape and regulatory requirements.

Beyond cybersecurity and risk management aspects, multinational organizations must also address regulatory compliance challenges related to digital governance and information security. Organizations operating across multiple countries must comply with different legal frameworks, particularly those related to data protection, digital transactions, and information management. Studies have shown that blockchain-based infrastructures can enhance regulatory compliance by ensuring transparency, traceability, and the integrity of digital records [17]. In addition, the implementation of IoT-based monitoring systems requires appropriate governance and security mechanisms to ensure compliance with operational standards and technological regulations [18].

Given the increasing complexity of digital ecosystems, the integration of IT governance, risk management, and regulatory compliance has become a critical issue for multinational digital enterprises. Effective IT governance can provide strategic direction and control mechanisms that enable organizations to manage technological risks, maintain system security, and ensure compliance with regulatory requirements. Therefore, examining the role of IT governance in enhancing risk management performance and regulatory compliance is essential to understand how digital enterprises can effectively address technological challenges while maintaining secure and compliant digital operations.

2. Literature Review

Overview of IT Governance Frameworks

COBIT is one of the most widely used frameworks for IT governance. It offers a comprehensive model that helps organizations align IT with business objectives, manage risks, and ensure compliance [19]. The latest version, COBIT 2019, emphasizes governance and management objectives, aligning IT strategies with organizational goals to effectively mitigate risks. COBIT is often used in conjunction with other capability maturity models, such as CMMI and SPICE, to enhance its governance capabilities [20]. By focusing on strategic alignment, COBIT enables businesses to implement efficient and effective IT governance structures that reduce risk exposure.

ITIL is primarily focused on IT service management (ITSM), providing a process-oriented approach to managing IT services [21]. It ensures that IT services are aligned with business needs and helps organizations optimize their IT operations. ITIL's emphasis on service quality and continuous improvement allows organizations to proactively manage risks associated with IT services, such as downtime or service disruptions, which can have significant operational impacts.

ISO 38500 is an international standard that provides principles for the governance of IT within organizations. It emphasizes the evaluation, direction, and monitoring (EDM) of IT use to ensure that it meets business needs [22]. By offering a model for effective corporate IT governance, ISO 38500 ensures that IT governance practices align with business objectives and provide an oversight structure to manage risks related to IT use and integration.

The ISO 27000 series focuses on information security management systems (ISMS), providing guidelines to protect information assets from threats [23]. It is often integrated with other frameworks like COBIT and ITIL to enhance overall IT governance by ensuring that security risks are addressed in a systematic and structured manner. This integration is essential

for organizations to maintain compliance with data protection regulations like GDPR and HIPAA, as well as to ensure the integrity and security of their digital assets.

While the integration of multiple frameworks can lead to redundancies and complexity, research suggests that harmonizing these frameworks through metamodelling can reduce inconsistencies and improve efficiency [24]. This approach allows organizations to leverage the strengths of various frameworks while minimizing overlap and ensuring that all aspects of IT governance, risk management, and compliance are effectively addressed.

Risk Management in Digital Enterprises

The shift towards digital transformation has introduced a host of new risks that require a robust and adaptable governance framework. IT governance structures play a critical role in mitigating these risks by aligning IT initiatives with organizational goals, ensuring that risk management practices are effectively integrated into business processes [25]. Effective governance mechanisms help organizations identify, assess, and mitigate risks associated with digital transformation, such as cybersecurity threats, data breaches, and compliance violations.

Digital transformation introduces new risks related to the adoption of emerging technologies, such as cloud computing, AI, and machine learning [16]. These technologies offer significant opportunities for organizations but also introduce complex risks, including data privacy concerns, system vulnerabilities, and regulatory challenges. As digital transformation accelerates, organizations must enhance their IT governance structures to address these risks and ensure that internal controls are aligned with the evolving technological landscape.

The shift to cloud computing has changed the scope of IT governance, necessitating new control mechanisms to manage security and privacy risks [23]. Cloud environments require specialized governance frameworks like COBIT and ISO 27000 to ensure that organizations can manage the risks associated with data storage, access control, and regulatory compliance in cloud platforms.

IT governance frameworks such as COBIT and ISO 38500 support Enterprise Risk Management (ERM) by providing structured processes and controls to manage IT-related risks [20]. ERM frameworks help organizations integrate IT risk management into their broader risk management strategies, ensuring that all aspects of digital transformation are considered in risk mitigation efforts.

IT governance mechanisms, including organizational structures, processes, and relational mechanisms, are essential for managing risks in digital enterprises [9]. These mechanisms help organizations ensure that IT is aligned with business objectives, that risks are identified and mitigated effectively, and that compliance is maintained across various digital and regulatory landscapes.

Regulatory Compliance in Digital Organizations

In addition to security aspects, digital organizations must also ensure that the information technology systems they use comply with applicable regulations, particularly those related to data protection, information security, and digital system governance. In the context of multinational organizations, regulatory compliance challenges become increasingly complex due to differences in legal standards and technology policies across countries.

The utilization of blockchain technology can contribute to improving compliance with digital regulations through transparent and immutable transaction recording mechanisms. Blockchain-based systems enable organizations to conduct data audits more efficiently and ensure the integrity of information stored within digital systems [26]. Furthermore, the implementation of Internet of Things (IoT) technology also requires effective system management to ensure security and compliance with information technology operational standards [26].

The development of IoT- and sensor-based security systems also highlights the importance of integrating technology with access control mechanisms and continuous system monitoring to maintain organizational information security [18]. Through integrated monitoring and control systems, organizations can enhance their level of compliance with security policies as well as applicable information technology operational standards.

Role of IT Governance in Meeting Regulatory Requirements

IT governance frameworks, such as COBIT 2019, are essential for aligning IT strategies with organizational goals and ensuring that risk management practices are integrated into the business processes. For example, in public sector organizations and state-owned enterprises (SOEs), IT governance plays a critical role in IT master planning, investment management, and risk mitigation [13]. Effective IT governance ensures that IT initiatives support the broader organizational goals, helping to mitigate risks associated with digital transformations, such as cybersecurity vulnerabilities and data privacy issues [27].

One of the primary functions of IT governance is to ensure compliance with external regulations, which is particularly important in highly regulated industries such as healthcare. IT governance frameworks help organizations maintain compliance with relevant laws by embedding compliance into day-to-day business processes. For instance, in healthcare settings, effective IT governance prioritizes compliance with regulations such as HIPAA in the U.S. and the General Data Protection Regulation (GDPR) in Europe, while also focusing on continuous IT performance monitoring to improve both patient care and operational efficiency [28]. The use of frameworks like COBIT ensures that compliance efforts are systematic and integrated into the organization's governance structures.

A robust internal audit function, particularly the role of the Chief Audit Executive (CAE), is crucial for enhancing cybersecurity quality. IT governance frameworks, through mechanisms like private CAE-AC meetings and IT audit expertise, significantly improve cybersecurity resilience. These mechanisms help organizations align with global cybersecurity standards, such as the GDPR and NIST [29]. The increasing complexity of cybersecurity risks, especially with the integration of emerging technologies like cloud computing, requires that IT governance frameworks continuously evolve to address new security challenges and regulatory expectations.

Gaps in Research

While much of the existing research on IT governance focuses on specific sectors or national contexts, such as small banks in Croatia or public-listed companies in India, there is a notable gap in empirical studies examining IT governance within multinational digital enterprises. These enterprises face unique challenges in integrating IT governance, risk management, and compliance across various jurisdictions with different regulatory landscapes [30]. Future research should focus on exploring the integration of IT governance within multinational organizations, addressing the complexities of cross-border regulations and ensuring consistent compliance across different regions.

The integration of IT governance frameworks, such as COBIT 2019, into organizational processes presents practical challenges, especially in developing countries with complex and fragmented regulatory environments. Research highlights the need for more practical implementation strategies to optimize the use of these frameworks for regulatory compliance and operational efficiency [31]. These challenges underscore the importance of developing context-specific strategies that can facilitate the smooth implementation of IT governance frameworks in diverse regulatory settings.

The integration of emerging technologies, particularly Artificial Intelligence (AI), into IT governance frameworks presents significant challenges. These include data sovereignty issues, regulatory compliance in AI applications, and ensuring transparency in automated decision-making processes [32]. As AI continues to evolve, there is a need for more research into how IT governance can support the adoption of AI technologies while ensuring compliance with existing regulations and maintaining ethical standards in business operations [28].

3. Proposed Method

This study adopts a quantitative approach using a survey to collect data from senior IT and compliance managers in multinational digital enterprises. The survey will capture insights into their IT governance practices, risk management strategies, and regulatory compliance efforts, focusing on frameworks like COBIT and ISO 27000. Structural Equation Modeling (SEM) will be used to analyze the relationships between IT governance, risk management, and compliance. The sample will consist of 100 to 150 senior managers from various industries, ensuring a diverse and representative data set for reliable statistical analysis.

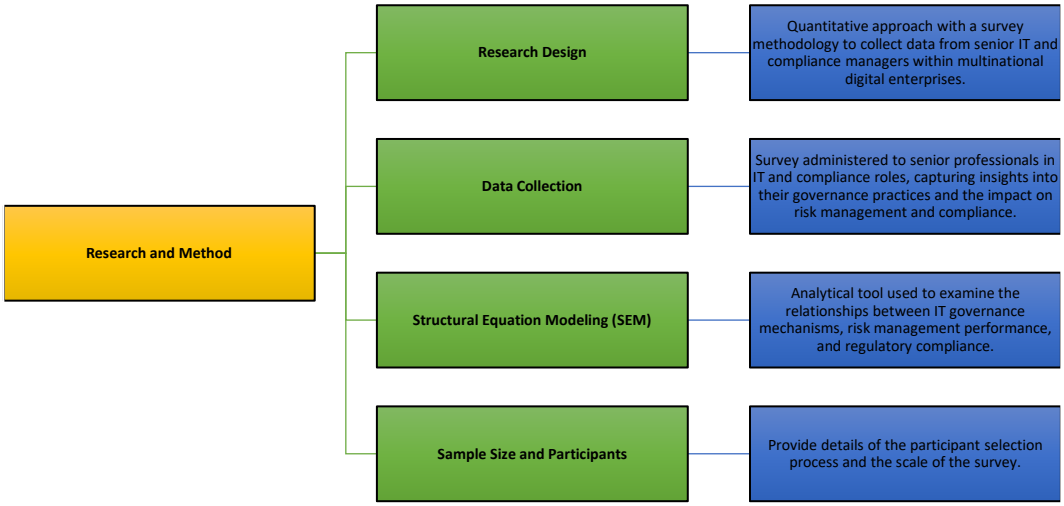

Figure 1. Flowchart structure.

Research Design

This study adopts a quantitative approach using a survey methodology to collect data from senior IT and compliance managers within multinational digital enterprises. A quantitative approach allows for objective, statistically analyzable data collection that can provide valuable insights into the relationship between IT governance mechanisms, risk management performance, and regulatory compliance. The survey methodology is ideal for capturing the perspectives and experiences of senior professionals who play a direct role in the implementation and management of IT governance frameworks. By focusing on senior IT and compliance managers, this study seeks to gather data from individuals who are actively involved in integrating IT governance practices with business objectives to manage risks and ensure compliance.

Data Collection

The data collection process will involve administering a structured survey to senior IT and compliance managers across multinational digital enterprises. These professionals were chosen because of their extensive experience and direct involvement in overseeing IT governance, risk management, and regulatory compliance within their organizations. The survey will consist of questions designed to capture insights into the participants' governance practices, challenges in managing risks, and strategies used to maintain compliance with regulatory requirements. The questions will focus on the integration of IT governance frameworks, such as COBIT and ISO 27000, into the organization's processes and their impact on risk management and regulatory compliance. The responses will provide valuable data to understand how governance structures influence risk mitigation and compliance performance.

Structural Equation Modeling (SEM)

To analyze the relationships between IT governance mechanisms, risk management performance, and regulatory compliance, this study will utilize Structural Equation Modeling (SEM). SEM is an advanced statistical technique that allows for the examination of complex relationships between multiple variables. This approach is particularly useful for understanding how various factors of IT governance impact risk management and compliance outcomes. By using SEM, the study can quantify the effects of different IT

governance practices on business outcomes and assess the significance of these relationships. SEM will provide a rigorous and systematic framework for analyzing the data and testing the hypotheses related to IT governance, risk management, and compliance.

Sample Size and Participants

The sample for this study will consist of senior IT and compliance managers working in multinational digital enterprises. Participants will be selected based on their expertise in managing IT governance and compliance activities within global organizations. The survey will target a sample of approximately 100 to 150 senior managers, ensuring that the data collected is both statistically significant and representative of a broad range of multinational digital enterprises. These participants will be selected from various industries to provide a comprehensive view of how IT governance frameworks are implemented and their impact on risk management and compliance. The sample size is chosen to provide sufficient statistical power for the analysis using SEM, ensuring that the results are reliable and meaningful.

4. Results and Discussion

The study highlights the crucial role of IT governance frameworks, such as COBIT 2019 and ISO 27000, in enhancing risk management and ensuring consistent regulatory compliance in multinational digital enterprises. These frameworks align IT strategies with organizational goals, enabling proactive risk identification, efficient mitigation, and better adherence to complex regulatory requirements across multiple jurisdictions. By integrating risk management into daily operations and ensuring compliance through continuous monitoring and risk assessments, organizations can navigate regulatory challenges effectively. Additionally, collaboration between IT governance and internal audit functions strengthens cybersecurity, improving resilience and protecting sensitive data. The findings suggest that robust IT governance structures are essential for organizations to adapt to digital transformation, manage risks, and maintain compliance in a rapidly evolving regulatory landscape.

Results

The study reveals that strong IT governance frameworks significantly impact risk mitigation effectiveness and regulatory compliance consistency in multinational digital enterprises. The survey results indicated that organizations employing comprehensive IT governance structures, such as COBIT 2019 and ISO 27000, were more effective in aligning their IT strategies with organizational goals. This alignment enabled these organizations to proactively identify and address risks, ensuring that risk management practices were consistently integrated into their operations. In particular, organizations with these frameworks experienced greater efficiency in risk mitigation, especially concerning cybersecurity threats, data privacy issues, and regulatory compliance challenges across multiple jurisdictions.

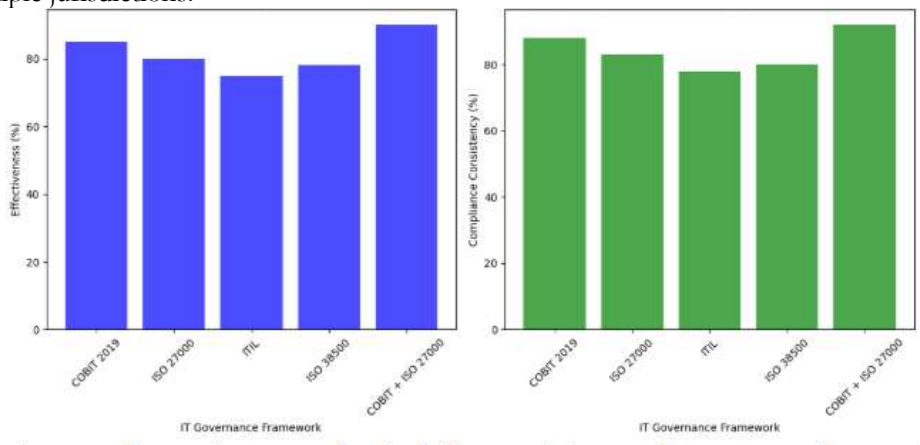

Figure 2. Risk Mitigation Effectiveness by IT Governance Framework and Regulatory Compliance Consistency by IT Governance Framework.

Here are the supporting graphs representing the findings on the impact of IT governance frameworks on risk mitigation effectiveness and regulatory compliance consistency:

a) Risk Mitigation Effectiveness by IT Governance Framework: This bar chart shows the effectiveness of various IT governance frameworks in mitigating risks. As seen, COBIT 2019 and the combination of COBIT + ISO 27000 demonstrate the highest effectiveness in risk mitigation, followed by ISO 27000 and ISO 38500.
b) Regulatory Compliance Consistency by IT Governance Framework: This chart presents the consistency of regulatory compliance across different IT governance frameworks. Again, COBIT 2019 and COBIT + ISO 27000 lead in ensuring consistent compliance, while ITIL shows slightly lower compliance consistency compared to others.

Additionally, the data suggested that IT governance frameworks enhanced the consistency of regulatory compliance. Organizations with well-established IT governance structures demonstrated higher adherence to complex regulatory requirements such as GDPR, HIPAA, and other region-specific data protection laws. These organizations were able to manage cross-border compliance more effectively, ensuring that compliance was embedded into daily operations rather than being treated as a separate or secondary function. This led to a significant reduction in non-compliance risks and improved the ability to respond to regulatory changes in a timely manner.

Discussion

The findings of this study highlight the critical role of IT governance frameworks in improving risk management and ensuring consistent regulatory compliance in multinational digital enterprises. By aligning IT strategies with organizational goals, frameworks like COBIT 2019 enable organizations to integrate risk management into all business processes, making it an ongoing concern rather than a reactive measure. This proactive approach helps businesses anticipate potential risks and implement mitigation strategies before these risks escalate, contributing to a more resilient organization. In contrast, organizations lacking such frameworks struggle with ad hoc approaches, which result in fragmented risk management practices that fail to address the complexity and scope of risks associated with digital transformation.

In terms of regulatory compliance, IT governance frameworks ensure that compliance requirements are not merely a checklist but are incorporated into the organization's daily activities. This integrated approach enables multinational digital enterprises to address the regulatory challenges posed by operating in multiple jurisdictions. By using tools such as data mapping, continuous monitoring, and risk assessments, organizations can stay ahead of regulatory changes, ensuring that they remain compliant even as regulations evolve. This is particularly important in industries such as healthcare and finance, where regulatory requirements are stringent and failure to comply can result in significant legal and financial consequences.

Furthermore, the study underscores the importance of collaboration between IT governance and internal audit functions in strengthening cybersecurity measures. The Chief Audit Executive (CAE) plays a pivotal role in ensuring that cybersecurity practices are aligned with global standards like NIST and GDPR. When IT governance and internal audit functions work synergistically, organizations are better equipped to identify vulnerabilities and mitigate risks effectively, resulting in improved cybersecurity resilience. This collaboration enhances the organization's ability to protect sensitive data and maintain the trust of stakeholders, contributing to overall business performance and compliance consistency.

5. Comparison

Organizations with well-established IT governance structures, such as those utilizing frameworks like COBIT 2019 and ISO 27000, significantly outperformed those with ad hoc or decentralized governance practices in terms of risk management and regulatory compliance. The data from this study revealed that businesses with comprehensive IT governance structures were able to proactively identify and mitigate risks, ensuring alignment between IT strategies and organizational goals. This structured approach allowed them to manage risks in a systematic and consistent manner, particularly when navigating complex and evolving regulatory requirements across multiple jurisdictions. In contrast, organizations with decentralized or ad hoc governance structures struggled with fragmented risk

management practices, resulting in inefficiencies, inconsistent compliance efforts, and difficulty adapting to regulatory changes. These organizations often lacked the necessary frameworks to align IT practices with broader business objectives, which led to reactive risk management strategies and an increased likelihood of non-compliance.

When compared with previous research on IT governance and its impact on organizational outcomes, the findings of this study align with existing literature on the importance of formal governance frameworks in enhancing risk management and ensuring compliance. Previous studies have consistently shown that organizations with robust IT governance mechanisms, such as those based on COBIT and ITIL, achieve better results in terms of risk mitigation and compliance (e.g., studies on the financial sector and public institutions). For example, research on state-owned enterprises and public organizations has demonstrated that effective IT governance frameworks lead to improved performance in risk management and regulatory compliance (Lubis et al., 2023). Similarly, studies on multinational companies have highlighted that the integration of IT governance with organizational strategies is critical for maintaining consistent compliance across borders, particularly in industries with stringent regulatory requirements. This study adds to the body of evidence by confirming that the adoption of structured IT governance frameworks is essential for improving both risk management effectiveness and compliance consistency in the context of multinational digital enterprises.

6. Conclusions

This study demonstrated the significant role that well-established IT governance frameworks, such as COBIT 2019 and ISO 27000, play in enhancing risk management performance and ensuring regulatory compliance within multinational digital enterprises. The findings revealed that organizations with robust IT governance structures performed better in proactively identifying, assessing, and mitigating risks compared to those with ad hoc or decentralized governance practices. Furthermore, these organizations exhibited greater consistency in meeting complex and evolving regulatory requirements across multiple jurisdictions. By aligning IT strategies with business objectives, companies were able to embed risk management and compliance processes into their daily operations, leading to improved overall performance.

This study makes a valuable contribution to the literature by providing empirical evidence on the integration of IT governance with risk management and regulatory compliance in multinational digital enterprises. While previous research has explored the impact of IT governance frameworks in specific sectors or national contexts, this study fills a gap by focusing on multinational organizations operating in a complex global regulatory environment. Additionally, the study highlights the importance of internal audit functions and the role of the Chief Audit Executive (CAE) in enhancing cybersecurity resilience, a crucial aspect of modern IT governance. The findings further underscore the need for organizations to adopt structured governance frameworks to improve risk management, maintain regulatory compliance, and navigate the challenges of digital transformation effectively. This research provides actionable insights for enterprises seeking to optimize their IT governance structures and enhance their risk management capabilities in the context of global operations.

References

[1] Y. Luo, "A general framework of digitization risks in international business," *J. Int. Bus. Stud.*, vol. 53, no. 2, pp. 344 – 361, 2022, doi: 10.1057/s41267-021-00448-9.

[2] F. J. Contractor, J. Cantwell, G. Gereffi, and K. P. Sauvant, "The shift to a more turbulent IB environment, and how MNEs respond to this shift," *Int. Bus. Rev.*, vol. 35, no. 2, 2026, doi: 10.1016/j.ibusrev.2025.102538.

[3] A. Carlo and F. Casamassima, "'Going Digital, Staying Secure: Cyber ERM Activities in a Post-Pandemic Setup,'" in *Proceedings of the International Astronautical Congress, IAC*, 2022.

[4] W. Wang, "Challenges and Strategies for Cross-Border Data Compliance in Enterprise Digital Management," in *Proceedings of 2024 5th International Conference on Computer Science and Management Technology, ICCSMT 2024*, 2025, pp. 972 – 976. doi: 10.1145/3708036.3708196.

[5] E. S. Mandrakov, D. A. Dudina, V. A. Vasiliev, and M. N. Aleksandrov, "Risk Management Process in the Digital Environment," in *Proceedings of the 2022 International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2022*, 2022, pp. 108 – 111. doi: 10.1109/ITQMIS56172.2022.9976622.

[6] M. S. M. Silva, "At the digital crossroads: The attention economy, freedom of expression, and platform regulation — Challenges and prospects for solutions in the European Union," *Comun. e Soc.*, vol. 137, no. 150, 2025, doi: https://doi.org/10.17231/volesp(2025).5496.

[7] E. García-Canal and M. F. Guillén, "The International Expansion of Digital Platforms: A Dynamic Setting for Challenging and Advancing Theories of the Multinational Enterprise," *BRQ Bus. Res. Q.*, 2025, doi: 10.1177/23409444251382952.

[8] C. D. Djakman and S. V. Siregar, "The effect of maturity learn element in Enterprise risk management and corporate social responsibility on the level of digital transformation," *Bus. Strateg. Dev.*, vol. 7, no. 1, 2024, doi: 10.1002/bsd2.346.

[9] J. Zhong, X. Wang, and T. Zhang, "Network Security Governance Policy and Risk Management: Research on Challenges and Coping Strategies," *J. Mach. Comput.*, vol. 4, no. 1, pp. 153 – 169, 2024, doi: 10.53759/7669/jmc202404015.

[10] M. Chergui, A. Chakir, and H. Medromi, "Smart IT governance, risk and compliance semantic model: Business Driven architecture," in *Proceedings of the 3rd World Conference on Smart Trends in Systems, Security and Sustainability, WorldS4 2019*, 2019, pp. 297 – 301. doi: 10.1109/WorldS4.2019.8903997.

[11] S. Nai, A. Rifai, and A. Sadiq, *Data governance, key insights, strategic challenges, and future imperatives*. 2025. doi: 10.4018/979-8-3373-0365-9.ch001.

[12] H. Abdullah, "Analyzing the technological challenges of Governance, Risk and Compliance (GRC)," in *4th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques, ICEECCOT 2019*, 2019, pp. 274 – 282. doi: 10.1109/ICEECCOT46775.2019.9114642.

[13] F. S. Lubis, V. S. Praditha, M. Lubis, H. Fakhrurroja, M. F. Safitra, and A. R. Lubis, "Corporate ICT Governance of Indonesian State-Owned Companies: Governance Structure and Decision Making Archetype," in *2023 IEEE International Conference on Computing, ICOCO 2023*, 2023, pp. 277 – 282. doi: 10.1109/ICOCO59262.2023.10397787.

[14] A. Byrne, "NAVIGATING THE DIGITAL EVOLUTION: UNCOVERING GOVERNANCE CHALLENGES AND STRATEGIES FOR SUCCESSFUL TRANSFORMATION," *EDPACS*, vol. 69, no. 3, pp. 40 – 46, 2024, doi: 10.1080/07366981.2024.2325010.

[15] E. Iveroth, J. Lindvall, and J. Magnusson, *Final words – looking back and ahead*. 2025. doi: 10.4324/9781003540472-24.

[16] X. Wang, N. Wang, W. Sun, A. Xu, and Z. Zhang, "Digital transformation and enterprise violation risk: A 'motivation-opportunity-attitude' framework," *Heliyon*, vol. 10, no. 20, 2024, doi: 10.1016/j.heliyon.2024.e39125.

[17] D. Danang, M. U. Dewi, and W. Aryani, "Systematic Literature Review on the Application of Blockchain in Enhancing Server Security: Research Methods for Mitigating Ransomware and Malware Attacks," *Int. J. Comput. Technol. Sci.*, vol. 1, no. 4, pp. 27–51, 2024.

[18] E. Muhadi, S. Sulartopo, D. Danang, D. Sasmoko, and N. D. Setiawan, "Rancang bangun sistem keamanan ruang persandian menggunakan RFID dan sensor PIR berbasis IoT," *Router J. Tek. Inform. dan Terap.*, vol. 2, no. 1, pp. 8–20, 2024.

[19] H. Wu and Y. Wang, "Digital transformation and corporate risk taking: Evidence from China," *Glob. Financ. J.*, vol. 62, 2024, doi: 10.1016/j.gfj.2024.101012.

[20] R. Mulyana, L. Rusu, and E. Perjons, "IT governance mechanisms influence on digital transformation: A systematic literature review," in *27th Annual Americas Conference on Information Systems, AMCIS 2021*, 2021.

[21] C. Espinoza-Aguirre and D. Pillo-Guanoluisa, "IT governance model for public institutions with a focus on higher education; [Modelo de Gobierno de TI para Instituciones Públicas con enfoque en la Educación Superior]," in *Iberian Conference on Information Systems and Technologies, CISTI*, 2018, pp. 1 – 14. doi: 10.23919/CISTI.2018.8399248.

[22] V. Hotti and H. Meriläinen, "Framework-based ICT governance and survey in Northern Savonia," *Commun. Comput. Inf. Sci.*, vol. 636, pp. 193 – 206, 2016, doi: 10.1007/978-3-319-44672-1_16.

[23] N. Kazemargi and P. Spagnoletti, "Cloud Sourcing and Paradigm Shift in IT Governance: Evidence from the Financial Sector," in *Lecture Notes in Information Systems and Organisation*, 2020, pp. 47 – 61. doi: 10.1007/978-3-030-47355-6_4.

[24] J. H. Ortiz and S. Bayona-Oré, "Framework for it governance in a financial institution; [Implementación de un Marco para el Gobierno TI en una Entidad Financiera]," *RISTI - Rev. Iber. Sist. e Tecnol. Inf.*, vol. 2019, no. E23, pp. 220 – 232, 2019.

[25] N. Xu, W. Lv, and J. Wang, "The impact of digital transformation on firm performance: a perspective from enterprise risk management," *Eurasian Bus. Rev.*, vol. 14, no. 2, pp. 369 – 400, 2024, doi: 10.1007/s40821-024-00264-9.

[26] D. Danang, N. D. Setiawan, and E. Siswanto, "Pemanfaatan Teknologi Internet of Things untuk Monitoring Kualitas Air Sungai di Wilayah Perkotaan," *J. New Trends Sci.*, vol. 2, no. 1, pp. 23–34, 2024.

[27] T. Wulyatiningsih and J. Y. Mambu, "IT Governance Maturity and Business Alignment: A COBIT 2019 Evaluation at RSUD ODSK," *Int. J. Eng. Sci. Inf. Technol.*, vol. 5, no. 2, pp. 248 – 255, 2025, doi: 10.52088/ijesty.v5i2.822.

[28] G. Benneh Mensah *et al.*, "Assessing the role Ghana's Public Health Act, 2012 (Act 851) can play in oversight of artificial intelligence healthcare systems to prevent medical errors and improve patient safety," *Babylonian J. Artif. Intell.*, pp. 24–32, 2023, doi: https://doi.org/10.58496/BJAI/2023/006.

[29] A. Alzeban, K. Al-Hajaya, N. Sawan, H. Chammaa, and S. Foster, "The quality of cybersecurity audits: do synergies among the chief audit executive, IT governance and internal audit functions matter?," *Manag. Audit. J.*, pp. 1 – 27, 2025, doi: 10.1108/MAJ-05-2025-4825.

[30] F. U. Begum, O. M. J. Popoola, and M. Z. Ghazali, "Unveiling the Determinants of Effective IT Governance: A Conceptual Framework for India's Public Listed Companies," *Pap. Asia*, vol. 40, no. 6b, pp. 415 – 428, 2024, doi: 10.59953/paperasia.v40i6b.297.

[31] A. A. Odejide, A. E. van der Poll, and J. A. van der Poll, "Towards a Conceptual IT Governance Framework for Developing Countries," *Stud. Big Data*, vol. 170, pp. 439 – 449, 2025, doi: 10.1007/978-3-031-83915-3_35.

[32] F. A. Almaqtari, "The Role of IT Governance in the Integration of AI in Accounting and Auditing Operations," *Economies*, vol. 12, no. 8, 2024, doi: 10.3390/economies12080199.