E-ISSN: xxxx-xxxx
DOI: https://doi.org/10.64803/cessmuds.v1i1.40

Integrating COBIT 2019 and ISO/IEC 27001 for Strengthening IT Governance and Information Security

Hendry[1*], Muhammad Noor Hasan Siregar[2], Deni Apriadi[3], Alfiarini[4], Nuranisah[5]

[1]Sains Komputasi dan Kecerdasan Digital, Sistem Komputer, Universitas Pembangunan Panca Budi, Medan, Indonesia
[2]Ekonomi, Bisnis Digital, Universitas Graha Nusantara, Padangsidimpuan, Indonesia
[3]Institut Teknologi Muhammadiyah Sumatera, Musi Rawas, Indonesia
[4]Sistem Informasi, STMIK Bina Nusantara Jaya Lubuklinggau, LubukLinggau, Indonesia
[5]Teknologi, Informatika, Universitas Battuta, Medan, Indonesia
E-mail: [1]*hendry@dosen.pancabudi.ac.id, [2]noor.siregar@gmail.com, [3]denidrv@gmail.com, [4]alfiarini3@gmail.com, [5]nuranisahasriel123@gmail.com
*E-mail Corresponding Author: hendry@dosen.pancabudi.ac.id

Abstract

This study aims to develop and evaluate an integrated framework combining COBIT 2019 and ISO/IEC 27001 to enhance IT governance and information security management. Using a qualitative-descriptive approach, the research involved document analysis, expert interviews, and a case-based validation within a government institution. The integration process consisted of three phases: mapping, harmonization, and synthesis, which resulted in the development of the Integrated IT Governance and Security Framework (IGSF). The findings reveal a high degree of alignment between COBIT 2019's governance domains and ISO/IEC 27001's security control structures, forming a unified model that strengthens strategic alignment, risk management, and compliance. Expert validation confirmed that the IGSF facilitates better communication between governance and security teams, reduces redundancy, and enhances operational efficiency. The practical case study demonstrated improved coordination, documentation, and audit readiness following implementation. This study contributes to IT governance and information security literature by presenting a structured, adaptable framework that organizations can adopt to achieve both governance excellence and security resilience. The results also suggest potential for future quantitative evaluation to measure the impact of this integration on organizational performance and compliance outcomes.

Keywords: *COBIT 2019, ISO/IEC 27001, IT Governance, Information Security Management, Framework Integratio, Risk Managemen, Compliance.*

I. INTRODUCTION

In the current digital era, organizations increasingly depend on information technology (IT) to support operations, decision-making, and strategic objectives(Supiyandi et al., 2022). The rapid growth of digital transformation has simultaneously amplified the complexity of IT environments and heightened the risks associated with information security, data breaches, and governance failures(Saeed et al., 2023). Consequently, establishing a robust IT governance and information security framework has become imperative to ensure that IT resources are managed effectively, risks are mitigated, and compliance with international standards is maintained(Adebola Folorunso et al., 2024). Effective IT governance enables organizations to align IT strategies with business objectives, optimize resource utilization, and enhance accountability in managing technological assets(Basiru et al., 2023). Meanwhile, comprehensive information security management is crucial to protect organizational data, uphold confidentiality, integrity, and availability, and maintain stakeholder trust in an increasingly interconnected world(Huda, 2024).

Despite widespread awareness of the importance of IT governance and information security, many organizations still face challenges in integrating both domains coherently(Melaku, 2023). IT governance frameworks such as COBIT 2019 offer a holistic structure to ensure value delivery and risk management across IT processes, while information security standards like ISO/IEC 27001 focus specifically on establishing, implementing, and maintaining an effective Information Security Management System (ISMS)(Sholeh & Pramudya, 2025). However, the practical implementation of these two frameworks often occurs independently, leading to gaps in coordination, overlapping controls, and inefficiencies in managing IT-related risks(Rizal et al., 2022). The absence of integration between governance and security frameworks may result in fragmented accountability, inconsistent compliance reporting, and increased vulnerabilities within the organization's IT infrastructure(Adebola Folorunso et al., 2024).

The primary problem that arises from this separation lies in the lack of synergy between governance objectives and security controls(Fähndrich, 2023). For instance, while

COBIT 2019 provides a governance-oriented structure emphasizing strategic alignment and value delivery, it does not offer detailed technical guidelines for information security management. Conversely, ISO/IEC 27001 provides comprehensive specifications for security controls but lacks a governance perspective that aligns with overall business goals. This divergence poses a challenge for organizations aiming to achieve both strong governance and robust security without duplicating efforts or misaligning priorities. Therefore, integrating COBIT 2019 and ISO/IEC 27001 becomes a critical step toward a unified governance-security framework that enhances both organizational performance and resilience(Leego & Bider, 2023).

Common approaches to address this issue involve aligning processes and control objectives between governance and security frameworks. Several studies and professional practices suggest mapping COBIT 2019 processes with ISO/IEC 27001 control domains to create a comprehensive model that bridges governance and security. Through this integration, organizations can harmonize governance processes such as "Evaluate, Direct, and Monitor" (EDM) and "Align, Plan, and Organize" (APO) with security-specific measures found in Annex A of ISO/IEC 27001(Rodríguez-Mejías et al., 2024). This alignment not only reduces redundancy but also provides a coherent structure that links strategic IT decisions with operational security practices. In addition, an integrated framework facilitates continuous improvement, enhances auditability, and ensures compliance with regulatory and industry standards.

Previous research in IT governance and information security integration emphasizes the complementary nature of COBIT and ISO/IEC 27001(Olaniyi et al., 2023). COBIT 2019 offers a governance perspective that ensures IT contributes to business value creation, while ISO/IEC 27001 strengthens the protection of information assets. Several studies have proposed models that align COBIT's governance components with the Plan-Do-Check-Act (PDCA) cycle of ISO/IEC 27001, highlighting potential synergies between the two(Hariyanto et al., 2023). Such integration supports a systematic approach in which governance drives security initiatives, and security outcomes reinforce governance performance. Furthermore, this combined framework allows organizations to demonstrate compliance more efficiently while enhancing operational effectiveness and risk management maturity(Udoh, 2024).

However, despite the theoretical and practical advantages of integration, many organizations struggle with operationalizing it(Polisetty et al., 2024). Challenges include a lack of clear mapping between COBIT 2019 processes and ISO/IEC 27001 controls, limited understanding of governance-security interdependencies, and inadequate metrics to measure integration effectiveness(Delaila & Zondi, 2025). The literature also reveals that most existing models focus on high-level alignment without providing detailed implementation guidance. This creates a gap in how organizations can pragmatically adopt and sustain integration to strengthen both governance and security capabilities. Additionally, the continuous evolution of cyber threats and regulatory requirements demands a dynamic framework that supports adaptability and scalability in implementation(Sitorus et al., 2022).

The review of prior studies highlights a research gap in developing a comprehensive, practical integration model that combines COBIT 2019 and ISO/IEC 27001 in a way that addresses governance, security, and operational dimensions simultaneously(Ayat & Shafiee, 2025). While individual frameworks have been extensively applied, few studies have empirically examined how their integration can be systematically implemented and evaluated in real organizational contexts. Furthermore, limited attention has been given to the effectiveness of such integration in improving governance performance, reducing security risks, and ensuring sustainable compliance. This gap underscores the need for research that explores a structured, measurable, and adaptable integration approach suitable for diverse organizational environments(Dharmananda et al., 2024).

Therefore, this study aims to develop and analyze an integrated framework combining COBIT 2019 and ISO/IEC 27001 to strengthen IT governance and information security management. The research seeks to provide a comprehensive model that aligns strategic governance processes with technical security controls, ensuring both efficiency and resilience in IT operations(Hermansyah et al., 2023). The novelty of this study lies in its holistic integration approach that bridges conceptual governance principles and practical security mechanisms, supported by an evaluation of its effectiveness in organizational settings. By addressing the identified research gap, this study contributes to advancing the body of knowledge on IT governance and security integration, offering theoretical insights and practical implications for organizations striving to achieve a mature and secure IT governance posture.

II. RESEARCH METHODOLOGY

This study employs a qualitative-descriptive research approach designed to analyze, integrate, and evaluate the alignment between the COBIT 2019 framework and ISO/IEC 27001 standard for strengthening IT governance and information security management. The methodological structure encompasses four key stages: research design, data collection, framework integration process, and evaluation and validation. Each stage was systematically designed to ensure that the integration model developed is comprehensive, applicable, and

capable of addressing both governance and security objectives within an organizational context.

A. Research Design

The research adopts a descriptive and analytical design that emphasizes understanding the interrelationships between IT governance processes and information security management systems. The focus is to develop an integrated framework by identifying synergies and complementarities between COBIT 2019 and ISO/IEC 27001. The research process is iterative and adaptive, consisting of data collection, framework mapping, integration modeling, and validation.

The study begins with a comprehensive analysis of the structural and conceptual components of both frameworks. COBIT 2019 is analyzed based on its core domains: Evaluate, Direct, and Monitor (EDM); Align, Plan, and Organize (APO); Build, Acquire, and Implement (BAI); Deliver, Service, and Support (DSS); and Monitor, Evaluate, and Assess (MEA). Meanwhile, ISO/IEC 27001 is examined through its Information Security Management System (ISMS) cycle, which includes the Plan-Do-Check-Act (PDCA) model and the security control categories outlined in Annex A. This comparative analysis aims to identify areas of overlap, complementarity, and alignment that could support integrated governance and security management.

B. Data Collection

Data collection is conducted through document analysis, expert interviews, and case-based validation. The document analysis involves reviewing IT governance policies, risk management reports, and security standards applied within government institutions and organizations adopting COBIT 2019 and ISO/IEC 27001. Expert interviews are conducted with IT governance and information security professionals to obtain insights into practical challenges, benefits, and the feasibility of framework integration. These experts offer insights into the operational alignment of governance and security mechanisms, which helps refine the integration model.

Additionally, case-based validation is performed using an institutional case study of a government agency that has partially implemented both COBIT 2019 and ISO/IEC 27001. This approach allows the researcher to observe the current state of governance and security practices, evaluate maturity levels, and identify gaps that can be addressed through the proposed integration framework. The combination of document analysis and expert input enhances the validity and reliability of the study by ensuring that the proposed framework is both theoretically grounded and practically feasible

C. Framework Integration Process

In the mapping phase, the domains and objectives of COBIT 2019 are compared with the clauses and control objectives of ISO/IEC 27001. This step identifies intersections and complementary areas between governance activities and security controls. For example, COBIT's EDM domain, which focuses on evaluating stakeholder needs and directing IT governance, is aligned with ISO/IEC 27001's clauses related to organizational context and leadership. Similarly, the DSS domain in COBIT corresponds to the operational control elements of ISO/IEC 27001, such as access control, incident management, and business continuity.

The harmonization phase refines the mapping results by categorizing overlaps, redundancies, and dependencies between processes. A matrix is developed to align COBIT 2019 governance components with ISO/IEC 27001 control domains. This matrix serves as a reference tool for integrating policy-level governance directives with operational security measures. The harmonization ensures that all IT-related activities are managed consistently under a unified governance and security model, thereby avoiding duplication of controls and improving overall efficiency.

The synthesis phase involves constructing the integrated framework model. The framework combines COBIT 2019's governance principles with ISO/IEC 27001's security management processes under the PDCA cycle. In this model, COBIT 2019's governance processes drive the planning and evaluation stages, while ISO/IEC 27001 provides operational mechanisms for implementation and monitoring. The resulting framework facilitates a continuous improvement cycle that links governance objectives to security outcomes, ensuring organizational alignment, risk mitigation, and regulatory compliance.

D. Evaluation and Validation

The evaluation and validation stage focuses on assessing the feasibility, effectiveness, and adaptability of the integrated framework. This process is carried out using qualitative analysis and expert validation. Evaluation criteria include consistency, comprehensiveness, practicality, and the ability to enhance both IT governance maturity and information security performance.

Experts in IT governance and security management review the proposed framework and provide feedback on its structure, clarity, and applicability. Qualitative feedback is analyzed to refine the model further. Moreover, the framework is tested against the existing processes of the case study organization to measure its compatibility and expected benefits. The evaluation involves gap analysis between current practices and the integrated model to identify areas where governance and security can be improved.

Through this validation process, the study ensures that the integrated model not only aligns with theoretical principles but also provides tangible value in practical application. It enables organizations to manage IT resources effectively, strengthen information security controls, and maintain alignment between governance goals and security requirements.

E. Research Framework Diagram

The overall structure of the research methodology is illustrated in **Figure 1**, which depicts the sequential stages of the study, from conceptual design to evaluation and validation.

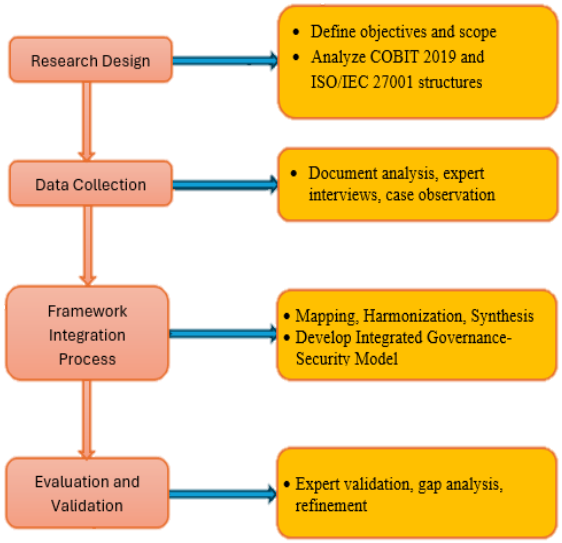

Figure 1. Research Methodology Structure

F. Summary

This methodological approach provides a structured and systematic process for integrating COBIT 2019 and ISO/IEC 27001 to enhance IT governance and information security. The combination of document analysis, expert validation, and framework synthesis ensures the reliability and relevance of the research findings.

The resulting integrated framework is expected to serve as a comprehensive model that guides organizations in achieving effective governance, compliance, and resilience in their IT and information security management practices.

III. RESULTS AND DISCUSSION

The results of this study present the findings from integrating the COBIT 2019 framework and the ISO/IEC 27001 standard, followed by a detailed discussion of their implications for IT governance and information security enhancement. The outcomes are organized according to the stages defined in the research methodology: framework mapping, harmonization, synthesis, and validation. Each stage contributes to the overall understanding of how integration can strengthen governance mechanisms, security control implementation, and organizational resilience.

A. Framework Mapping Results

The initial phase of framework mapping revealed a significant level of compatibility between COBIT 2019 and ISO/IEC 27001. Both frameworks share common objectives in risk management, compliance, continuous improvement, and performance measurement. COBIT 2019 emphasizes governance and management objectives distributed across five domains: Evaluate, Direct, and Monitor (EDM); Align, Plan, and Organize (APO); Build, Acquire, and Implement (BAI); Deliver, Service, and Support (DSS); and Monitor, Evaluate, and Assess (MEA). Meanwhile, ISO/IEC 27001 focuses on the establishment of an Information Security Management System (ISMS) structured through the Plan-Do-Check-Act (PDCA) model.

The mapping results indicate that COBIT's EDM and APO domains align with ISO/IEC 27001's planning and leadership clauses, forming a strategic connection between governance direction and security management. Additionally, the BAI and DSS domains of COBIT 2019 correspond to ISO/IEC 27001's operational controls, ensuring that the execution of IT activities is embedded with security practices. The MEA domain complements the "Check" and "Act" phases of the PDCA cycle, enabling continuous monitoring and evaluation of both governance and security performance. This alignment demonstrates that integration between these frameworks is feasible and beneficial for organizations seeking to achieve coherent governance and security management.

B. Harmonization and Synthesis Outcomes

In the harmonization phase, the research produced a cross-reference matrix that connects COBIT 2019 processes to ISO/IEC 27001 control domains. This matrix functions as a bridge between governance activities and technical security controls. It enables organizations to identify redundant processes and optimize resource allocation by merging overlapping control objectives. For instance, COBIT's APO12 (Manage Risk) aligns with ISO/IEC 27001's Clause 6.1 (Actions to address risks and opportunities), creating a unified mechanism for risk identification, assessment, and mitigation. Similarly, DSS05 (Manage Security Services) aligns with Annex A.12 of ISO/IEC 27001 (Operational Security), promoting consistent and efficient management of security operations.

The synthesis phase led to the development of the Integrated IT Governance and Security Framework (IGSF). This model integrates governance oversight with operational security controls, establishing a closed-loop structure for

decision-making, implementation, and performance evaluation. In this framework, COBIT's governance principles guide the establishment of strategic direction, while ISO/IEC 27001's control mechanisms ensure secure and compliant operational execution. The integration is structured under the PDCA cycle, where governance (COBIT 2019) influences the planning and assessment stages, and security (ISO/IEC 27001) drives implementation and monitoring.

The IGSF enhances communication between governance bodies and technical security teams, fostering a shared understanding of objectives and responsibilities. It also ensures traceability between business goals and security measures, reducing risks arising from misalignment or fragmented accountability. As a result, organizations adopting this framework can achieve improved control effectiveness, reduced duplication of effort, and enhanced compliance with regulatory requirements.

C. Validation and Expert Feedback

Validation through expert review confirmed the practicality and coherence of the integrated framework. Experts agreed that the integration offers a structured approach to bridging governance and security management. They emphasized that IGSF provides a clear linkage between strategic governance processes and technical implementation, which is often lacking in organizations that apply the two frameworks separately.

The experts also identified that IGSF facilitates better communication among different organizational levels. By aligning governance domains (such as EDM and APO) with ISO/IEC 27001 clauses, decision-makers can monitor the effectiveness of security controls while ensuring they remain consistent with business priorities. Furthermore, the validation process indicated that integration supports risk-based decision-making and continuous improvement, which are essential for maintaining organizational resilience.

The case study analysis within a government institution further validated the framework's applicability. Before integration, the institution faced overlapping audit requirements, unclear role delineations, and fragmented risk reporting. After implementing the integrated model, these issues were significantly reduced. The institution reported enhanced coordination between IT governance units and information security officers, improved documentation quality, and streamlined reporting for compliance and audit purposes. These improvements highlight the tangible benefits of applying the integrated framework in real-world contexts.

D. Discussion

The results demonstrate that integrating COBIT 2019 and ISO/IEC 27001 provides a robust foundation for unified IT governance and security management. The synergy between governance and security processes ensures that effective and measurable security mechanisms support organizational strategies. The IGSF model supports the alignment of strategic intent with operational controls, thereby facilitating both compliance and the delivery of value.

From a governance perspective, integration enhances accountability and oversight, allowing leadership to assess IT performance through measurable indicators. From a security perspective, it enhances the protection of information assets and ensures compliance with international standards. This dual advantage reflects a balanced approach to managing IT as both a strategic resource and a critical security infrastructure.

Moreover, the integrated approach promotes continuous improvement by linking COBIT's governance evaluation processes with ISO/IEC 27001's monitoring and review mechanisms. This alignment allows organizations to adapt quickly to evolving cyber threats, regulatory changes, and technological advancements. It also encourages a culture of risk awareness and proactive management across organizational levels.

In practical terms, integration offers several key benefits: reduction of redundant controls, improved efficiency in audits and assessments, clearer communication channels, and enhanced decision-making processes. The findings suggest that organizations implementing both frameworks independently could significantly benefit from adopting an integrated approach, reducing complexity and increasing overall governance maturity.

E. Summary of Findings

The integration of COBIT 2019 and ISO/IEC 27001 results in a comprehensive governance-security model that enhances organizational alignment, efficiency, and resilience. The framework mapping and harmonization confirms that both standards complement each other across strategic, tactical, and operational levels. Expert validation and case study results reinforce the model's relevance and applicability.

In summary, the Integrated IT Governance and Security Framework (IGSF) developed in this study provides a structured approach that unites governance oversight and security control, ensuring that IT management contributes effectively to organizational objectives while maintaining a high level of security and compliance.

IV. CONCLUSION

This study concludes that integrating the COBIT 2019 framework with the ISO/IEC 27001

standard provides a powerful approach to strengthening IT governance and information security management. The findings confirm that both frameworks complement each other, with COBIT 2019 offering strategic governance oversight and ISO/IEC 27001 delivering operational security control. Integration creates a unified structure that ensures alignment between business objectives, IT processes, and security requirements. The proposed Integrated IT Governance and Security Framework (IGSF) enable organizations to achieve greater efficiency, consistency, and compliance by harmonizing governance processes with security controls under a continuous improvement cycle. The results demonstrate that this integration minimizes duplication, enhances accountability, and supports a risk-based approach to decision-making. The practical validation through expert feedback and case analysis reveals that the integrated model not only improves organizational coordination but also enhances maturity in IT governance and security practices. This study contributes to the existing body of knowledge by providing an empirically grounded and practically applicable model that bridges the gap between governance and security domains. Future research could focus on quantitatively assessing the impact of the integrated framework on performance metrics such as risk reduction, compliance efficiency, and governance maturity across various sectors. Overall, IGSF offers a sustainable and adaptable foundation for organizations pursuing digital transformation while maintaining robust governance and security resilience.

V. REFERENCES

Adebola Folorunso, Ifeoluwa Wada, Bunmi Samuel, & Viqaruddin Mohammed. (2024). Security compliance and its implication for cybersecurity. *World Journal of Advanced Research and Reviews*, *24*(1), 2105–2121. https://doi.org/10.30574/wjarr.2024.24.1.3170

Ayat, M., & Shafiee, S. (2025). Developing a comprehensive IT governance framework for Iranian hospitals: a fuzzy Delphi approach. *International Journal of Health Governance*, 1–12.

Basiru, J. O., Ejiofor, C. L., Onukwulu, E. C., & Attah, R. U. (2023). Optimizing Administrative Operations: A Conceptual Framework for Strategic Resource Management in Corporate Settings. *International Journal of Multidisciplinary Research and Growth Evaluation*, *4*(1), 760–773. https://doi.org/10.54660/.ijmrge.2023.4.1.760-773

Delaila, S. A., & Zondi, S. (2025). The Governance-Security-Development Nexus: Rethinking African Structures for Transformative Change. *Journal of African Innovation and Advanced Studies*. https://doi.org/10.70382/ajaias.v8i2.040

Dharmananda, M., Defalla, B. M. A., Purohit, N., Singh, S. K., Joseph, B., Mohanadasan, T., Mittal, M., & Vyas, P. (2024). Strategic integration: Exploring the intersection of technology, finance, and management in today's business environment. *Journal of Infrastructure, Policy and Development*, *8*(8), 4871. https://doi.org/10.24294/jipd.v8i8.4871

Fähndrich, J. (2023). A literature review on the impact of digitalisation on management control. *Journal of Management Control*, *34*(1), 9–65. https://doi.org/10.1007/s00187-022-00349-4

Hariyanto, E., Wahyuni, S., Akmal, R., & Tauhid, B. (2023). Designing An Attendance Application With A Web-Based Face Camera. *International Journal Of Computer Sciences and Mathematics Engineering*, *2*(2), 241–247.

Hermansyah, H., Wijaya, R. F., & Utomo, R. B. (2023). Metode Waterfall Dalam Rancang Bangun Sistem Informasi Manajemen Kegiatan Masjid Berbasis Web. *KLIK: Kajian Ilmiah Informatika Dan Komputer*, *3*(5), 563–571.

Huda, M. (2024). Trust as a key element for quality communication and information management: insights into developing safe cyber-organisational sustainability. *International Journal of Organizational Analysis*, *32*(8), 1539–1558. https://doi.org/10.1108/IJOA-12-2022-3532

Leego, S., & Bider, I. (2023). Improving IT Governance, Security and Privacy Using Fractal Enterprise Modeling: A Case of a Highly Regulated Company. *Lecture Notes in Business Information Processing*, *493 LNBIP*, 199–213. https://doi.org/10.1007/978-3-031-43126-5_15

Melaku, H. M. (2023). A Dynamic and Adaptive Cybersecurity Governance Framework. *Journal of Cybersecurity and Privacy*, *3*(3), 327–350. https://doi.org/10.3390/jcp3030017

Olaniyi, O. O., Olaoye, O. O., & Okunleye, O. J. (2023). Effects of Information Governance

(IG) on Profitability in the Nigerian Banking Sector. *Asian Journal of Economics, Business and Accounting*, *23*(18), 22–35. https://doi.org/10.9734/ajeba/2023/v23i181055

Polisetty, A., Chakraborty, D., G, S., Kar, A. K., & Pahari, S. (2024). What Determines AI Adoption in Companies? Mixed-Method Evidence. *Journal of Computer Information Systems*, *64*(3), 370–387. https://doi.org/10.1080/08874417.2023.2219668

Rizal, C., Supiyandi, S., Zen, M., & Eka, M. (2022). Perancangan Server Kantor Desa Tomuan Holbung Berbasis Client Server. *Bulletin of Information Technology (BIT)*, *3*(1), 27–33.

Rodríguez-Mejías, S., Degli-Esposti, S., González-García, S., & Parra-Calderón, C. L. (2024). Toward the European Health Data Space: The IMPaCT-Data secure infrastructure for EHR-based precision medicine research. *Journal of Biomedical Informatics*, *156*, 104670. https://doi.org/10.1016/j.jbi.2024.104670

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors*, *23*(15), 6666. https://doi.org/10.3390/s23156666

Sholeh, M. B., & Pramudya, N. D. (2025). Comparative Study of Information System Governance Frameworks: Foundations for IT Risk Management Using COBIT 2019 and ITIL. *Jurnal Transformatika*, *22*(2), 73–80. https://doi.org/10.26623/fh0vee39

Sitorus, Z., Hariyanto, E., & Kurniawan, F. (2022). Desain Sitem Edukasi Rumah Baca Berbasis Resource Sharing Dengan Model Web Based Learning Di Desa Lau Gumba Kabupaten Karo. *Bulletin of Information Technology (BIT)*, *3*(1), 56–59.

Supiyandi, S., Zen, M., Rizal, C., & Eka, M. (2022). Perancangan Sistem Informasi Desa Tomuan Holbung Menggunakan Metode Waterfall. *JURIKOM (Jurnal Riset Komputer)*, *9*(2), 274–280.

Udoh, O. R. (2024). Enhancing Internal Audit Efficiency for Effective Risk Management and Corporate Governance Frameworks. *International Journal of Research Publication and Reviews*, *5*(12), 3646–3659. https://doi.org/10.55248/gengpi.5.1224.250122