e-ISSN:
JURNAL SISTEM DAN TEKNOLOGI INFORMASI
The Journal of Information System and Technology
https://journal.uhamka.ac.id/index.php/sistekinfo/

UHAMKA PRESS

Volume 2 • Number 1 • June 2025 • 10 - 20

Optimizing IT System Audits with AI Assistance: A Comparative Review of COBIT, ISO 27001, and NIST Frameworks

Rifqi Favian Hibatullah[1] , Muhamad Sadam Rivaldi[2], Muhammad Yurizard Laksono[3], Lantip Sidik[4]
[1]Informatics Engineering, Muhammadiyah Prof. Dr. Hamka University, Jakarta, Indonesia
[2]Informatics Engineering, Muhammadiyah Prof. Dr. Hamka University, Jakarta, Indonesia
[3]Informatics Engineering, Muhammadiyah Prof. Dr. Hamka University, Jakarta, Indonesia
[4]Informatics Engineering, Muhammadiyah Prof. Dr. Hamka University, Jakarta, Indonesia

Received: June 8, 2025 Accepted: June 8, 2025 Published: June 8, 2025

Abstract

In an increasingly complex digital landscape, auditing information technology (IT) systems demands adaptive and intelligent approaches. This study aims to compare three major IT audit frameworks—COBIT, ISO 27001, and NIST—while exploring how artificial intelligence (AI) can effectively support the audit process. With AI-assisted literature analysis and framework comparison, this research provides deeper insights into the efficiency, flexibility, and risk focus of each framework. The results reveal that AI integration can accelerate risk assessments, enhance audit recommendation accuracy, and assist organizations in selecting or combining the most suitable frameworks based on strategic and operational needs.

Keywords: Information Technology Audit, Information Security, Cybersecurity Risk Management

INTRODUCTION

In today's digital era, information technology (IT) has become the backbone of operational activities and business strategies across a wide range of sectors. Enhanced IT performance helps businesses to grow, gain a competitive edge, and strengthen the management and oversight of their IT strategies. This becomes increasingly crucial as organisational structures and the technologies they employ grow more complex. As such, IT audits must be guided by frameworks grounded in principles that foster appropriate behaviour and decision-making (Rusman et al., 2022).

At its core, an audit serves as a tool for organisations to monitor and evaluate their operational activities while safeguarding the rights and interests of managers, employees, customers, and investors (Nugroho, 2020). In practice, a number of frameworks have been developed to support this audit process, most notably COBIT, ISO/IEC 27001, and the NIST Cybersecurity Framework. Each of these offers a distinct approach and emphasis in managing and auditing IT systems.

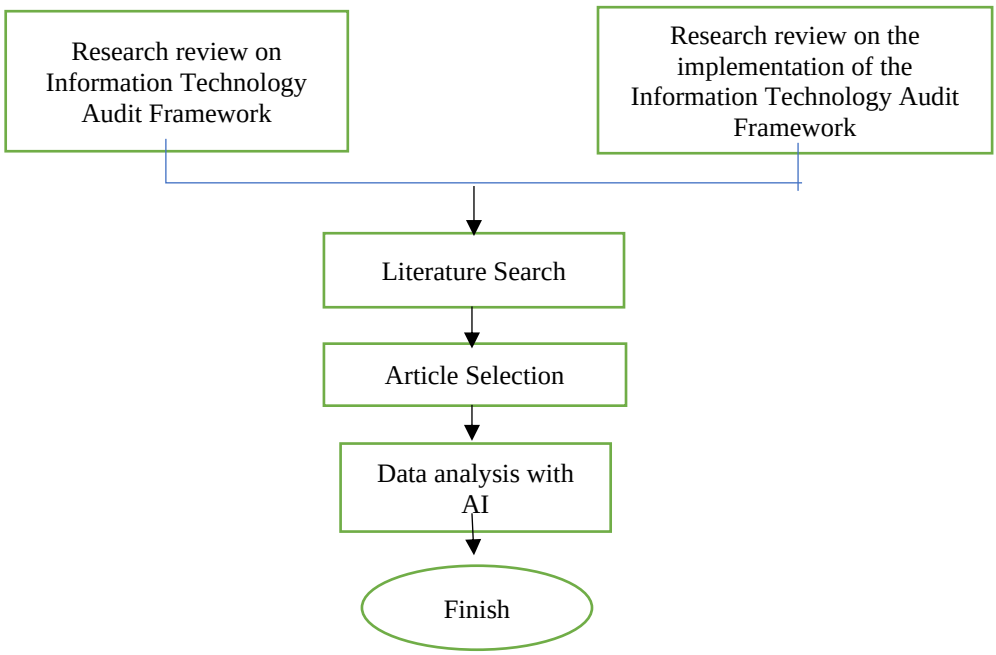
COBIT, developed by ISACA, focuses on IT governance and management that aligns with organisational objectives. It offers a comprehensive process model designed to ensure that IT contributes effectively to the achievement of business goals (McIntosh et al., 2024). Meanwhile, ISO/IEC 27001 is an international standard centred around Information Security Management Systems (ISMS), with the primary aim of safeguarding the confidentiality, integrity, and availability of information (Culot et al., 2021). On the other hand, the NIST Cybersecurity Framework, developed by the National Institute of Standards and Technology, takes a risk-based approach to managing and enhancing an organisation's cybersecurity posture (Mataracioglu & Ozkan, 2011).

Although these three frameworks have been widely adopted by organisations worldwide, selecting and implementing the most suitable one can pose significant challenges. This is largely due to differences in focus, structure, and methodology offered by each framework. It is therefore essential for organisations to develop a thorough understanding of the characteristics, strengths, and limitations of each framework prior to adoption.

This study aims to analyse existing literature related to these three IT audit frameworks. By reviewing a range of previous studies and scholarly publications, the research seeks to provide a deeper insight into the effectiveness, challenges, and best practices associated with the implementation of COBIT, ISO/IEC 27001, and the NIST Cybersecurity Framework.

METHODS

This study was conducted using a literature review method with a descriptive-comparative approach. In literature-based research, the key characteristic lies in the researcher's direct interaction with a wide range of previously published sources (Suryadewi et al., 2024). The data were gathered through Google Scholar, academic publications, and official framework documents provided by ISACA, ISO, and NIST, with an emphasis on relevant years of publication. The research design presented in this study follows a structured sequence, as illustrated in the diagram below:



The schematic design of this study serves as a guideline for conducting the research, which is carried out through a series of stages:

Literature Collection and Curation
Literature was gathered from reputable academic sources such as Google Scholar, ScienceDirect, and official documentation from ISACA, ISO, and NIST. To improve the efficiency and relevance of the data collection process, an AI-based natural language processing (NLP) model was used to automatically filter and extract high-quality and relevant publications.

AI-Assisted Comparative Analysis
The selected frameworks were then analyzed through a comparative lens, supported by AI to identify patterns, conceptual similarities, and differences across key audit dimensions: primary focus, core principles, risk management approach, scope of application, and target users. This AI integration enabled a faster and more accurate mapping of similarities and distinctions between frameworks.

Recommendation Mapping and Strategic Synthesis
In the final stage, AI was utilized to synthesize a strategic recommendation model based on organizational needs. Variables such as industry sector, organizational size, IT maturity level, and cybersecurity risk exposure were taken into consideration to generate a dynamic, data-driven framework selection guide. This guide can assist decision-makers in selecting or combining frameworks that best align with their strategic and operational goals.

FINDINGS AND DISCUSSION
Understanding Information Systems/Technology Audit

In today's digital landscape, information systems and technology have become integral to organisational operations, decision-making, and competitive advantage. However, this widespread reliance on Information Technology (IT) introduces significant risks, including data loss, processing errors, cyberattacks, and non-compliance with applicable regulations. To address these challenges and ensure the effective, secure, and efficient utilisation of IT

assets, Information Systems/Technology Audits (IS/IT Audits) have emerged as a critical function. They are no longer optional but essential for organisations to meet increasingly stringent IT Governance requirements.

Over time, the role of IT audits has undergone a profound transformation, shifting from a specialised technical function to a strategic imperative. Early descriptions of IT audits may have indicated a sole focus on technical controls or financial transaction integrity, even as "part of a broader financial audit." However, more recent and comprehensive sources, such as various journals and professional organisations, highlight much broader objectives. These include asset protection, data integrity assurance, achievement of organisational goals, efficient resource utilisation, compliance, and, most importantly, support for overall IT governance.

This shift indicates that the increasing complexity and criticality of IT in modern business operations have naturally expanded the scope and heightened the urgency of IT audits. They are no longer merely about ensuring financial accuracy or preventing basic errors but about contributing to overall organisational resilience, strategic alignment, and building digital trust. This transformation positions IT audits as a core component of enterprise risk management and corporate governance, transcending technical or compliance roles to actively contribute to strategic business objectives and ensure the reliability and security of an organisation's digital foundation. The explicit assertion that IT audits are a "necessity" for IT Governance underscores this strategic and irreplaceable role.

Objectives and Benefits of IT System Audits

A core objective of IT audit is to identify potential security risks and assess the overall performance of IT systems. This includes evaluating the security of both hardware and software to prevent evolving cyber threats. Security audits specifically focus on assessing various IT security aspects, including policies, procedures, access controls, data encryption, authentication methods, user authorisation, and intrusion detection systems. The goal is to evaluate how effectively an organisation's IT infrastructure can protect information and valuable assets from both internal and external threats. Furthermore, audits examine how data is collected, stored, and managed—referred to as Data Management Audits—to ensure its accuracy and security throughout its lifecycle.

IT systems audits also aim to evaluate the effectiveness and efficiency of the applications in use and assess how well information technology supports personnel management information systems (Enggar Novianto, 2023). This involves assessing the extent to which IT investments deliver added value, expected benefits, and optimal results for the organisation. In addition, application performance audits specifically evaluate the speed, scalability, and efficiency of applications used in organisational operations, ensuring that these applications support business workflows smoothly.

COBIT (Control Objectives for Information and Related Technologies)

COBIT is an IT governance framework developed by ISACA (Information Systems Audit and Control Association). Its objective is to assess the effectiveness of information systems implementation within production areas, ensure systems function optimally, and evaluate overall system integration and security mechanisms (Fernandes Andry et al., 2022). COBIT is designed to align IT objectives with overall business goals, enhance cyber security, and comprehensively improve organisational governance systems. COBIT 5 is based on five essential principles that form the foundation of effective IT governance: meeting stakeholder needs, covering the enterprise end-to-end, applying a single integrated framework, enabling a holistic approach, and separating governance from management (Kuryanti et al., 2023). The COBIT 2019 version further introduces dynamic governance

principles tailored to the specific needs of organisations, demonstrating the framework's adaptability to evolving business and technological environments.

One of COBIT's key features is the Goals Cascade, which links stakeholder needs to enterprise goals, which are then translated into IT-related goals and enabler goals. This process ensures that every stakeholder requirement is translated into specific and measurable actions (Kulkarni, 2017). This structure supports the prioritisation of governance goals based on enterprise goal priorities. For IT auditors, the Goals Cascade is a highly useful tool for identifying key IT-related areas posing risks to enterprise objectives, thereby assisting in IT audit planning and risk prioritisation. As such, COBIT serves as a bridge between business strategy and IT audit.

COBIT also includes seven enablers that are crucial to the success of organisational IT processes. These enablers include principles, policies, and frameworks; processes; organisational structures; culture, ethics, and behaviour; information; services, infrastructure, and applications; and people, skills, and competencies (3_185610007_BAB_II - Nururri Aji Maruf - Aji Maruf, n.d.). By providing a common language for IT professionals, auditors, and business executives, along with structured mechanisms such as the Goals Cascade, COBIT fundamentally redefines the role of IT audit. Auditing no longer solely inspects technical or operational compliance in isolation. Instead, auditors can use COBIT to evaluate the extent to which IT supports and contributes to the achievement of organisational strategic goals. This allows auditors to speak the "language of business" and provide recommendations that are more strategically relevant, directly correlating with business value.

COBIT enables IT auditing to become a more strategic and value-adding function, rather than one purely focused on compliance. It facilitates improved communication and alignment between IT teams, audit functions, and senior management, ensuring that IT investments and audit efforts are aligned with the organisation's overall vision, mission, and strategy. This alignment is crucial to ensure that IT not only functions effectively but also delivers maximum value to the organisation.

ISO 27001 (Information Security Management System)

ISO 27001 is the international standard for Information Security Management Systems (ISMS). Implementing ISO 27001 entails adopting a comprehensive framework to identify, manage, and mitigate various threats to organisational information (Rutanaji et al., 2017). This standard significantly enhances information security across three primary dimensions: confidentiality, integrity, and availability. Confidentiality ensures that sensitive information, such as customer data or intellectual property, is protected from unauthorised access. Integrity involves the accuracy and completeness of data, ensuring that only authorised changes are permitted. Availability ensures that information is accessible to authorised users and systems whenever required.

Additional benefits of ISO 27001 include reduced financial costs associated with data breaches, the ability to attract new business and talent, strengthened security through comprehensive risk assessments, reduction in human errors via effective employee training, and increased trust from various stakeholders.

Within the context of IT auditing, ISO 27001 demonstrates that information security is not merely about "technical security" but also about "security as a business differentiator." Standardised and verifiable information security, through ISO 27001 certification supported by audits, directly leads to a reduction in security incident risks (e.g., data breaches, cyber-attacks). This risk reduction, in turn, builds strong trust among customers, business partners, and investors. This trust is not merely a sentiment; it becomes a significant intangible asset, distinguishing the organisation in a competitive market and directly contributing to long-term business growth and reputation. Audits based on ISO 27001 help organisations not only meet legal and industry standards but also build a

reputation as responsible and trustworthy entities in data management. This clearly shows that IT audits, through standards like ISO 27001, directly contribute to brand value, competitiveness, and the financial sustainability of organisations. (Beyond Defense: The Business Benefits of ISO 27001 Certification, n.d.)

NIST (National Institute of Standards and Technology)

The National Institute of Standards and Technology (NIST) is a United States federal agency that plays a pivotal role in the development of standards, guidelines, and best practices to improve the security and resilience of information systems. While originally established to promote innovation and industrial competitiveness, NIST has become globally recognised for its contributions to cybersecurity frameworks, particularly within the realm of information technology governance and audit (Security and Privacy Controls for Information Systems and Organizations, 2020).

One of NIST's most influential contributions is the NIST Cybersecurity Framework (CSF), which provides a structured, risk-based approach for organisations to assess and enhance their cybersecurity posture. The framework is composed of five core functions: Identify, Protect, Detect, Respond, and Recover, which together form a comprehensive lifecycle for managing cybersecurity risk. These functions are further divided into categories and subcategories that guide organisations in establishing appropriate controls, policies, and procedures.

For IT auditors, the NIST CSF offers a valuable reference point when evaluating the maturity and effectiveness of an organisation's cybersecurity strategies. It allows auditors to benchmark existing practices against industry-accepted standards, identify gaps in implementation, and propose improvements that align with broader organisational goals. Moreover, NIST provides detailed Special Publications, such as NIST SP 800-53 and SP 800-171, which offer granular controls and security requirements tailored for federal information systems and contractors but are increasingly adopted by private sector entities as well (Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018).

NIST's approach is inherently flexible and scalable, making it suitable for organisations of varying sizes and industries. Importantly, it emphasises a risk-based philosophy, where controls and resources are prioritised based on the likelihood and impact of threats. This aligns closely with contemporary IT governance practices, which advocate for proportionate and adaptive security measures that reflect the dynamic threat landscape.

Comparative Analysis

COBIT 5 / COBIT 2019

COBIT 2019 presents a highly flexible and adaptive framework tailored to align with organisational needs. Its primary focus lies in the governance and management of information technology, structured across several key domains: Align, Plan and Organise (APO); Build, Acquire and Implement (BAI); Deliver, Service and Support (DSS); and Monitor, Evaluate and Assess (MEA) (Simamora, 2025). The framework provides a comprehensive model for aligning IT processes with business objectives, ensuring the delivery of value from IT investments while maintaining control over risks. COBIT's strength lies in its structured yet adaptable approach, enabling organisations to tailor governance mechanisms to their specific context and strategic direction.

ISO 27001

ISO 27001 is an internationally recognised framework for information security management, initially introduced in 2005 and later revised in 2013, replacing the earlier ISO 27001:2009 version. It adopts the foundational principles of an Information Security Management System (ISMS), employing the PDCA (Plan-Do-Check-Act) model to promote continual improvement. Widely accepted beyond the United States, ISO 27001 enjoys global recognition due to its practical and scalable structure for organisations of varying sizes and

industries. As stated by Sama et al. (2021), ISO 27001 encompasses seven core requirements:

1. Context of the organisation
2. Leadership
3. Planning
4. Support
5. Operation
6. Performance evaluation
7. Improvement

These requirements form the backbone of a systematic approach to managing information security risks, promoting a culture of proactive risk identification, compliance, and continuous improvement.

NIST Cybersecurity Framework

In general, the NIST framework is organised into five key functions known as the *Core*, which serve as high-level guidance for understanding and improving an organisation's cybersecurity posture. These five functions—Identification, Protection, Detection, Response, and Recovery—represent the fundamental pillars of a robust and comprehensive cybersecurity programme. They enable organisations to visualise their cybersecurity risk management efforts clearly, support strategic decision-making, and facilitate communication among technical and non-technical stakeholders alike.

1. Identification
   This function involves developing an organisational understanding of the cybersecurity environment, including the identification of systems, assets, data, and capabilities. It lays the foundation for effective risk management by ensuring that critical resources are accounted for and appropriately prioritised.
2. Protection
   Focused on implementing suitable safeguards, this function seeks to reduce the likelihood of cybersecurity incidents. It encompasses access controls, awareness training, data security measures, and protective technologies to ensure continuity of services.
3. Detection
   This function addresses the ability to discover cybersecurity incidents in a timely manner. It involves deploying detection processes and technologies that allow for swift identification and analysis of potential threats.
4. Response
   The response function centres on the planning and execution of appropriate measures to contain the impact of cybersecurity incidents. It involves incident response planning, communication, mitigation, and continuous improvement following incidents.
5. Recovery
   Finally, this function supports resilience and the restoration of capabilities that may have been impaired due to a cybersecurity event. It includes planning for system restoration and incorporating lessons learned to strengthen future defences.

The structured and adaptable nature of the NIST Cybersecurity Framework makes it highly applicable across sectors and especially valuable in environments where aligning IT security with enterprise risk management is a strategic priority.

Table 1. Comparative table

Comparative Dimensions	COBIT	ISO 27001	NIST

Main Focus	Comprehensive Enterprise IT Governance and Management, bridging business risks, control needs and technical issues.	Information security management system (ISMS), ensuring the selection of adequate and proportionate security controls.	Standards and guidelines for the security and resilience of information systems to cyber threats, including risk management. Cybersecurity, and privacy.
Objective	IT manager, compliance auditor, business executive.	Helping organizations build and maintain ISMS, emphasizing the protection of confidentiality, integrity, and availability of information.	Provides a set of standards and guidelines to ensure the security and resilience of information systems, primarily for US federal agencies, but broadly applicable.
Key Principles	Integrate IT risk management into corporate governance, with objectives and metrics.	Commitment to continuous improvement of ISMS, determination of information security objectives, compliance with applicable requirements.	Risk-based, core functions (Identify, Protect, Detect, Respond, Recover), adaptive to changing risks.
Scope	Applicable to organizations of all sizes and sectors, particularly for IT-business alignment, service delivery, and IT risk/compliance management.	Applicable to any organization, regardless of size, type or nature, to establish, implement, maintain and continually improve an ISMS.	Designed for US federal agencies, but its comprehensive and flexible nature makes it widely applicable in the private sector for cybersecurity and risk management.
Target Users	IT manager, compliance auditor, business executive.	Information security professional, risk manager, internal/external auditor.	Cybersecurity professional, risk manager, auditor.
Risk Management Approach	Integrate IT risk management into corporate governance, with objectives and metrics.	Risk-based, identification, assessment and treatment of information security risks as the core of ISMS.	Risk-based, identifying and analyzing risks to the organization's operations, with a core function of managing cyber risk.
Compliance Aspects	Help ensure compliance with regulatory and legal requirements.	Helps meet ever-changing legal and regulatory requirements, preventing fines.	Helping organizations meet cybersecurity standards and guidelines, especially for US federal agencies.

Relevance to IT Audit Stages	Provides guidance for good IT governance and management, helping auditors refer to the principles of effective IT governance.	Provides a framework for managing information security risks, which is the basis for information security audits.	Assess the organization's compliance with cybersecurity standards, evaluate the effectiveness of information security measures, and assess risk assessment processes.

This table provides a highly structured and systematic approach to conducting comparative analysis generated by AI. It ensures that all relevant aspects of each framework are examined consistently against predefined criteria, making the comparison clear, concise, and easily digestible for the reader. This structured approach directly addresses the requirement for a "comparative analysis" as outlined in the user's question and significantly aids in identifying overlaps, unique strengths, and potential gaps among the frameworks. Furthermore, it serves as a visual summary of the key findings, thereby enhancing overall comprehension.

CONCLUSION

This study has conducted a comparative analysis of three major IT audit frameworks—COBIT, ISO 27001, and NIST—through a literature review enhanced with AI-driven analysis. The results indicate that each framework offers unique strengths and focus areas:

- **COBIT** excels in comprehensive IT governance and the alignment of IT with business objectives.
- **ISO 27001** provides a standardized structure for information security management, ideal for organizations handling sensitive data and requiring regulatory compliance.
- **NIST** offers a flexible, risk-based approach that is highly adaptable to the evolving landscape of cybersecurity threats.

The integration of AI throughout the research process accelerated the analysis, enhanced objectivity, and enabled more precise identification of patterns and recommendations. AI also allowed for the dynamic mapping of organizational needs to the most suitable IT audit framework, based on factors such as industry sector, organization size, and IT maturity.

Based on these findings, it is recommended that organizations avoid relying on a single framework in isolation. Instead, they should consider combining elements from multiple frameworks to build a more comprehensive, responsive, and resilient IT audit and risk management system tailored to the demands of today’s digital era.

REFERENCES

3_185610007_BAB_II - Nururri Aji Maruf - Aji Maruf. (n.d.).

Beyond defense: The business benefits of ISO 27001 certification. (n.d.).

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. In TQM Journal (Vol. 33, Issue 7, pp. 76–105). Emerald Group Holdings Ltd. https://doi.org/10.1108/TQM-09-2020-0202

Enggar Novianto. (2023). AUDIT SISTEM INFORMASI PADA APLIKASI SISTEM INFORMASI MANAJEMEN KEPEGAWAIAN (SIMPEG) MENGGUNAKAN MODEL FRAMEWORK COBIT 4.1. Jurnal Manajemen Informatika & Sistem Informasi (MISI), 6(1). https://doi.org/10.36595/misi.v5i2

Fernandes Andry, J., Sakti Lee, F., Darma, W., Rosadi, P., Ekklesia, R., & Studi Sistem, P. (2022). AUDIT SISTEM INFORMASI MENGGUNAKAN COBIT 5 PADA PERUSAHAAN PENYEDIA LAYANAN INTERNET. Jurnal Ilmiah Rekayasa Dan Manajemen Sistem Informasi, 8(1), 14430.

Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (2018). https://doi.org/10.6028/NIST.CSWP.04162018

Kulkarni, G. (2017). Applying the Goals Cascade to the COBIT 5 Principle Meeting Stakeholder Needs.

Kuryanti, S. J., Adiwihardja, C., Suryadi, A., & Ambarsari, D. A. (2023). Penerapan Framework COBIT Untuk Peningkatan Tata Kelola TI. Journal of Students' Research in Computer Science, 4(2), 189–198. https://doi.org/10.31599/jsrcs.v4i2.2964

MATARACIOGLU, T., & OZKAN, S. (2011). GOVERNING INFORMATION SECURITY IN CONJUNCTION WITH COBIT AND ISO 27001.

McIntosh, T. R., Susnjak, T., Liu, T., Watters, P., Nowrozy, R., & Halgamuge, M. N. (2024). From COBIT to ISO 42001: Evaluating Cybersecurity Frameworks for Opportunities, Risks, and Regulatory Compliance in Commercializing Large Language Models. https://doi.org/10.1016/j.cose.2024.103964

Nugroho, H. (2020). A Review on Information System Audit Using COBIT Framework. IJAIT (International Journal of Applied Information Technology), 46. https://doi.org/10.25124/ijait.v3i02.2114

Rusman, A., Nadlifatin, R., & Subriadi, A. P. (2022). Information System Audit Using COBIT and ITIL Framework: Literature Review. SinkrOn, 7(3), 799–810. https://doi.org/10.33395/sinkron.v7i3.11476

Rutanaji, D., Suning Kusumawardani, S., Wahyu Winarno, W., & Teknik Elektro dan Teknologi Informasi, J. (2017). Prosiding Seminar Nasional XII "Rekayasa Teknologi Industri dan Informasi.

Sama, H., Licen, L., Saragi, J. S. D., Erline, M., Kelvin, K., Hartanto, Y., Winata, J., & Devalia, M. (2021). Studi Komparasi Framework Nist Dan Iso 27001 Sebagai Standar Audit Dengan Metode Deskriptif Studi Pustaka. Rabit : Jurnal Teknologi Dan Sistem Informasi Univrab, 6(2), 116–121. https://doi.org/10.36341/rabit.v6i2.1752

Security and Privacy Controls for Information Systems and Organizations. (2020). https://doi.org/10.6028/NIST.SP.800-53r5

Simamora, G. (2025). Analisis Tata Kelola Teknologi Informasi Menggunakan Metode Cobit 5 (Studi Kasus : Koperasi Simpan Pinjam Graha Arsindi Bumiayu). 12(2), 2660–2668.

Suryadewi, D., Manuaba, I. B. G., & Jasa, L. (2024). Literature Review: Evaluasi Keefektifan Framework Audit Teknologi Informasi pada Perguruan Tinggi. Majalah Ilmiah Teknologi Elektro, 23(1), 177. https://doi.org/10.24843/mite.2024.v23i01.p19