Jurnal TRANSFORMATIKA
Vol.22, No.2, Januari 2025, pp. 73 - 80
P-ISSN: 1693-3656, E-ISSN: 2460-6731
https://journals.usm.ac.id/index.php/transformatika/

Comparative Study of Information System Governance Frameworks: Foundations for IT Risk Management Using COBIT 2019 and ITIL

Moch. Badrus Sholeh[1], Naufal Daffa Pramudya[2]
[1]Universitas Diponegoro, Magister Sistem Informasi
Jl. Imam Bardjo SH No.5, Semarang, 024-8449610, e-mail: badrus@students.undip.ac.id
[2]Universitas Diponegoro, Magister Sistem Informasi
Jl. Imam Bardjo SH No.5, Semarang, 024-8449610, e-mail: naufaldaffapramudya1@students.undip.ac.id

ARTICLE INFO

History of the article :
Received 27 Mei 2024
Received in revised form 12 Maret 2025
Accepted 6 Maret 2025
Available online 24 Maret 2025

Keywords:

I-BGP, *failover*, *routing*, jaringan lokal, Mikrotik

*** Correspondece:**

Telepon:
+62817240742

E-mail:
agushartanto@usm.ac.id

ABSTRACT

In this study, COBIT 2019 and ITIL V4 are compared in the context of managing IT risk. Through systematic literature review (SLR), the theoretical and practical foundations of both frameworks are evaluated. COBIT 2019 offers a structured approach, while ITIL emphasizes adaptive operational practices. Analysis of strengths and weaknesses helps organizations choose an approach that aligns with their strategic objectives. With this understanding, organizations can enhance their ability to manage IT risks and achieve business goals effectively.

1. INTRODUCTION

In the digital era, managing information technology (IT) risks has become crucial for organizations across various sectors. IT risks can significantly impact operational sustainability, data security, and organizational reputation. Strong frameworks for governing information systems are needed to effectively identify, evaluate, and manage these risks. Two commonly used frameworks for IT system governance and risk management are COBIT (Control Objectives for Information and Related Technology) and ITIL (Information Technology Infrastructure Library). These frameworks offer different yet complementary approaches to optimizing IT value and minimizing related risks.

The implementation of information technology has become a critical element in companies due to its effectiveness and efficiency, which accelerates every operation, thereby influencing a more financially and network-wise competitive edge. Information technology has something very important for companies [1]. Information is something that is important for a company or organization, in this case it influences the achievement of the vision and mission. Companies or organizations need to study information well in order to avoid threats and various challenges in achieving their goals [2]. In the implementation of information technology, various issues regarding company assets arise due to the lack of proper management of IT assets in institutions/companies.

IT assets must be dependable to ensure that IT Asset Management activities align with business requirements. The goal of IT Asset Management within an institution or company is to plan and oversee the asset life cycle, as well as to anticipate potential future risks [1].

Due to these issues, the need for IT governance arises to help organizations support their goals. IT governance can be defined as “the decision-making process regarding IT investments. including how it is made and who is responsible, as well as how the results of the decision are measured and implemented.” [3]. IT governance is a crucial aspect of corporate governance that focuses on aligning IT strategy with business objectives, ensuring IT investments contribute to organizational goals, effectively managing risks, and delivering value [4].

By utilizing the COBIT framework, it helps a company or organization in directing their goals, vision and mission. This COBIT framework framework has the benefit of the doubt and is open to various references. This can help organizations and companies focus on information technology [5]. Conversely, ITIL serves as a framework offering guidance on managing IT infrastructure, development, and operations within IT services. Frequently used as a reference for implementing IT service management (ITSM), ITIL effectively integrates IT with an organization's strategy [1]. IT services are managed with the understanding that frameworks in the IT field can be enhanced or developed to meet organizational and research objectives. This assessment can be done using ITIL, which can be used as a service management to support organizational goals, and with a service-oriented approach, ITIL helps organizations improve operational efficiency and customer satisfaction while reducing operational risks.

By understanding the frameworks of both COBIT 2019 and ITIL V4, and considering their strengths and weaknesses, organizations can analyze the theoretical and practical foundations of these frameworks. In developing and adopting both frameworks, organizations have the flexibility to choose and implement approaches that best suit their needs and strategic goals.

RESEARCH METHODS

This research utilized the systematic literature review (SLR) method, consisting of three main stages: planning, execution, and reporting [6]. In the planning stage, the primary focus was on determining the research questions (RQ) for this SLR. The main research questions posed were:

- RQ1: How can the COBIT 2019 and ITIL frameworks be used for risk management?
- RQ2: What are the strengths and weaknesses of the COBIT 2019 and ITIL frameworks in risk management?

Next, in the execution stage, the researcher conducted article searches in various digital libraries such as Scopus, ScienceDirect, Springer Link, and Google Scholar. Keywords used in the search included "COBIT 2019", "ITIL", and "Risk Management" with a publication date range from 2020 to 2024. This process was followed by article extraction based on predefined criteria and research questions, with a focus on the titles and abstracts of the articles. The inclusion criteria for articles were as follows: 1) Articles must be written in English or Indonesian, 2) Articles must be open access, 3) Only article-format works were considered, 4) Abstracts must explicitly explain how a framework can assist companies in addressing challenges in IT risk management and/or achieving organizational goals.

In the reporting stage, all findings related to the utilization of COBIT 2019 and ITIL V4, as well as their strengths and weaknesses, will be documented, and conclusions will be presented in the following section. In summary, the series of SLR stages can be seen in Figure 1.

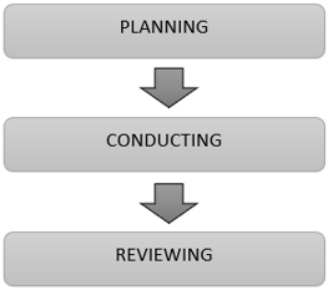

Figure 1. SLR Stages

RESULTS And Analysis

This chapter presents the results and analysis of the research conducted through systematic literature review (SLR). The research findings are divided into three main sections: data sources, the COBIT 2019 and ITIL frameworks in risk management, and the strengths and weaknesses of the COBIT 2019 and ITIL frameworks in risk management.

The first section, data sources, explains the sources obtained from the data extraction process. The second section explains how the COBIT 2019 and ITIL frameworks can assist in risk management. The final section discusses the strengths and weaknesses of each framework. The analysis in this chapter is supported by references from the articles identified and evaluated during the SLR process.

1. Data Hasil Pengujian

After completing the planning and execution stages, a total of 15 articles were successfully identified as relevant to addressing the research questions. Subsequently, significant key sentences from these articles were documented, highlighting the strengths and weaknesses of each framework. The recorded information was then organized into notes, which were later summarized and elaborated upon in the following section. A brief overview of the article search and extraction process can be seen in Figure 2 below.

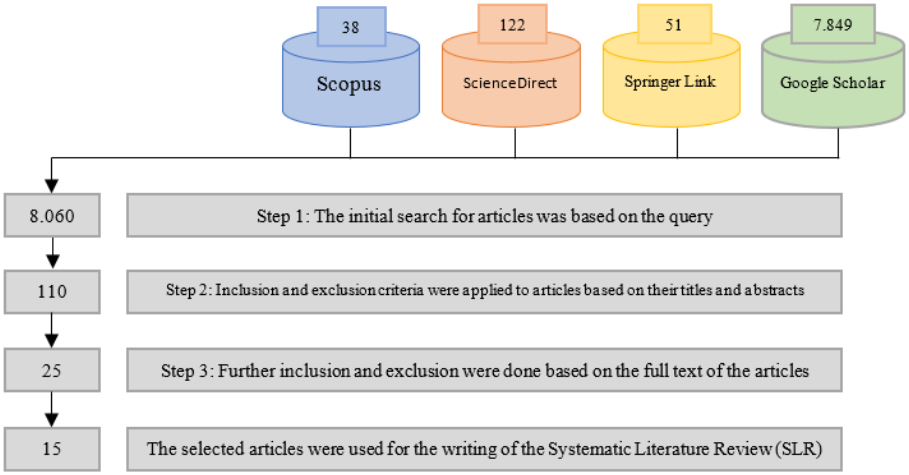

Figure 2. Article Extraction Stages

DOI: https://doi.org/10.26623/fh0vee39

2. COBIT 2019 in Managing Risk

COBIT (Control Objectives for Information and Related Technology) is a framework that sets standards and guidelines for IT operations, aiming to maximize the return on information technology investments and ensure efficient service delivery by offering clear metrics for managing errors. In its application, COBIT offers comprehensive and flexible guidance for IT governance and risk management. Designed to assist organizations in managing IT risks in a structured and integrated manner, COBIT 2019 covers the entire spectrum of IT governance, from strategic planning to day-to-day operations. The goal cascade approach in COBIT 2019 helps connect organizational strategic objectives with IT governance and management objectives, enabling the identification and mitigation of risks that may hinder the achievement of strategic goals. This framework includes several governance and management objectives that provide specific guidance for identifying, evaluating, and managing related risks.

In the concept of performance, COBIT 2019 introduces the concept of performance and maturity, allowing organizations to measure the effectiveness of IT governance in managing risks and identifying areas for improvement. Information security and regulatory compliance are also key focuses, with guidance to ensure that security practices and compliance are integrated into IT governance processes, thereby minimizing security and regulatory-related risks. COBIT 2019 is also designed for integration with other frameworks such as ITIL and ISO 27001, enabling the use of best approaches from various frameworks for a more holistic IT risk management. By emphasizing best principles and practices in IT governance and management, COBIT 2019 helps organizations ensure that IT risks are managed based on recognized industry standards and proven effectiveness. The implementation of COBIT 2019 can enhance organizational capabilities in managing risks, support the achievement of business goals, and provide significant added value

3. Advantages and Disadvantages of COBIT 2019 Framework

COBIT has been widely recognized as an effective framework in helping organizations manage IT risks, improve operational efficiency, and ensure that IT supports strategic business goals. The 2019 version of COBIT brings various updates and enhancements aimed at aligning this framework with the needs of modern business and the complexity of the continuously evolving technology landscape. However, like any other framework, COBIT 2019 has its strengths and weaknesses that organizations need to consider before adopting it. Understanding the strengths and weaknesses of COBIT 2019 is crucial so that organizations can leverage it optimally and address challenges that may arise during implementation. The following Table 1 provides an overview of the strengths and weaknesses of COBIT 2019 [7-10].

Table 2. Advantages and Disadvantages of COBIT 2019

	Advantages	Disadvantages
Comprehensive Approach	Provide a framework that covers all aspects of IT governance and management.	Can be complex and require significant time and resources to fully implement.
Focus on Business Goals	Use a goals-based approach that links strategic objectives with IT governance.	Requires a deep understanding of business goals and strategies to implement effectively.

Performance and Maturity Measurement	Introduces the concept of performance and maturity measurement for continuous evaluation and improvement.	The measurement and evaluation process may require additional time and resources.
Integration with Other Frameworks	Can be integrated with other frameworks such as ITIL AND ISO 27001, enabling a structured approach	Integration with other frameworks can be complex and requires good coordination.
Specific Guidelines	Provides specific guidance for identifying, evaluating, and managing risks.	It may be overly detailed for smaller or less complex organizations.
Security and Compliance	Provides specific guidance for information security and regulatory compliance.	Requires additional effort to ensure that all security and compliance guidelines are implemented correctly.
Principles and Best Practices	Emphasizes the use of principles and best practices in IT governance and management.	Adaptation to principles and best practices may require significant changes in organizational processes and culture.

By understanding these strengths and weaknesses, organizations can make more informed decisions regarding the adoption and implementation of COBIT 2019, ensuring that they can leverage its benefits to the fullest while addressing any challenges that may arise. The strengths and weaknesses of this method also help to assess the risk management of an organization, so knowing the strengths and weaknesses can maximize the decisions made by an organization.

4. ITIL in Managing Risk

The implementation of ITIL in risk management plays a significant role in supporting the success of information system governance in an organization. Here are some contributions of ITIL in the context of risk management:

a. Practical Guidance: ITIL provides practical guidance in managing risks related to IT services [11]. The proposed approach in ITIL helps organizations to identify, assess, and manage risks effectively to maintain operational sustainability [2].
b. Integration with Service Management: The concept of risk management in ITIL integrates well with IT service management [11]. Thus, the risk management process can be aligned with the established goals and strategies of IT services [2].
c. Application of PDCA Principles: The Plan-Do-Check-Act (PDCA) process model, which is the foundation of ITIL, can be consistently applied in risk management [2]. These steps include planning risk identification, implementing risk controls, checking the effectiveness of controls, and taking necessary corrective actions [2].
d. Minimization of Negative Impacts: One of ITIL's primary focuses is to minimize the negative impacts of incidents and risks on IT business operations [12]. Therefore, implementing ITIL practices can help organizations reduce losses and damages that may arise from uncontrolled risks [12].

DOI: https://doi.org/10.26623/fh0vee39

e. Ensuring Operational Continuity: Through integrated risk management processes, ITIL helps organizations maintain the operational continuity of information systems [13]. This is crucial in the digital transformation era, where risks related to technology and compliance with regulations can be significant concerns [13].
f. Updates and Adaptations: ITIL V4 updates the ITSM methodology by considering risks associated with digital transformation [1]. By incorporating Lean, Agile, and DevOps principles, ITIL V4 provides a more adaptive and responsive framework to changes in the business environment and emerging risks [1, 15].

The application of ITIL in risk management not only provides operational benefits but also provides a solid foundation for sustainable and adaptive information system governance [14]. Thus, integrating ITIL into risk management strategies is an important step for organizations to address the complex and dynamic challenges of this digital era.

5. Advantages and Disadvantages of the ITIL Framework

The strengths of ITIL in managing risks primarily lie in providing a comprehensive framework for organizations to navigate changing business environments [11]. ITIL also offers effective IT governance, assisting organizations in extracting value from IT investments and managing associated risks [11]. Moreover, ITIL has been widely implemented across various countries and sectors, including the public sector and banking, demonstrating significant popularity and trust in this framework [11]. The implementation of ITIL has proven successful in minimizing productivity losses and maintaining service quality for organizations by emphasizing prompt responses, appropriate remedies, and ongoing risk monitoring [12]. ITIL also aids organizations in optimizing resources by enhancing services and customer satisfaction through a structured and measurable approach to incident management [12]. For instance, Sentry Insurance can utilize ITIL's structured service strategies to safeguard customer data and comply with CCPA requirements more effectively [13]. Focusing on ITIL's service operations enables Sentry Insurance to swiftly respond to changes in customer data and manage data access accurately [13]. Furthermore, through continuous service improvements facilitated by ITIL, Sentry Insurance can consistently identify areas for enhancement and measure the success of CCPA implementation [13]. Thus, ITIL provides a comprehensive and proven framework in IT risk management, enhancing operational efficiency and user satisfaction [14][15].

However, despite its numerous advantages, ITIL also has several drawbacks that need consideration. One challenge is its integration with Agile software development methodologies like Scrum, which can pose barriers to implementation [11]. Additionally, although ITIL offers a structured framework, the predominance of manual processes in incident management can lead to inaccuracies and financial losses, indicating weaknesses in ITIL practice implementation [12]. Additional difficulties emerge when implementing deep learning network models for classifying IT incidents, which might not align with ITIL's traditional manual approach. [12]. Moreover, ITIL faces constraints when dealing with extensive, unorganized, and uneven datasets typically encountered in IT incident reporting, highlighting the necessity for adaptations and improvements in ITIL methodologies to address current requirements [12]. Implementing ITIL may also require significant time and resources from organizations, especially in terms of staff training and restructuring existing business processes [13]. Moreover, cultural resistance from employees and unique complexities in specific industries can also pose obstacles to effectively adopting ITIL principles [13]. Therefore, despite its benefits, ITIL also faces challenges that need to be addressed to ensure successful implementation and effective IT risk management [11-13].

CONCLUSIONS AND RECOMMENDATIONS

In the digital era, managing information technology (IT) risks becomes crucial for organizations across various sectors. IT risks can have significant impacts on operations, data security, and organizational reputation. Therefore, a robust framework is needed to effectively identify, assess, and manage these risks. Two commonly used frameworks are COBIT and ITIL. COBIT 2019 offers a comprehensive and flexible approach to IT governance and risk management, emphasizing performance and maturity, integration with other frameworks, and performance and information security measurement. Meanwhile, ITIL V4 provides practical guidance in managing risks related to IT services, focusing on integration with service management, application of PDCA principles, and updates to accommodate digital transformation.

Through an analysis of the strengths and weaknesses of both frameworks, it can be concluded that COBIT 2019 has a more comprehensive and structured approach to managing IT risks, while ITIL V4 emphasizes adaptive operational practices and responsiveness to change. Both frameworks offer advantages and drawbacks, and the decision to choose between them should be guided by the organization's requirements and strategic goals. By understanding the theoretical and practical foundations of COBIT 2019 and ITIL V4, organizations can select and implement the most suitable approach to support business goals and effectively manage IT risks.

REFERENCES

[1] Pratama, R. Y., & Umaroh, S. (2024). An IT Asset Governance Model Design Using COBIT 2019 And ITIL V4 Framework at BKU Itenas. E3S Web of Conferences, 484, 02006. https://doi.org/10.1051/e3sconf/202448402006

[2] Gunawan, N. K., Hadiprakoso, R. B., & Kabetta, H. (2020). Comparative study between the integration of ITIL and ISO / IEC 27001 with the integration of COBIT and ISO / IEC 27001. IOP Conference Series: Materials Science and Engineering, 852(1). https://doi.org/10.1088/1757-899X/852/1/012128

[3] Jaime, L., & Barata, J. (2023). How can FLOSS Support COBIT 2019' coverage analysis and a conceptual framework. Procedia Computer Science, 219, 680–687. https://doi.org/10.1016/j.procs.2023.01.339

[4] P., R., & V., N. (2021). Analysis of Processes Information Flows and Items as Additional Design Factor in COBIT Framework. Central European Business Review, 10(4), 63–82. https://doi.org/10.18267/j.cebr.264

[5] Atrinawati, L. H., Ramadhani, E., Fiqar, T. P., Wiranti, Y. T., Abdullah, A. I. N. F., Saputra, H. M. J., & Tandirau, D. B. (2021). Assessment of Process Capability Level in University XYZ Based on COBIT 2019. Journal of Physics: Conference Series, 1803(1). https://doi.org/10.1088/1742-6596/1803/1/012033

[6] Barraza de la Paz, J. V., Rodríguez-Picón, L. A., Morales-Rocha, V., & Torres-Argüelles, S. V. (2023). A Systematic Review of Risk Management Methodologies for Complex Organizations in Industry 4.0 and 5.0. In Systems (Vol. 11, Issue 5). MDPI. https://doi.org/10.3390/systems11050218

[7] Amali, L. N., Katili, M. R., & Suhada, S. (2023). Core model of information technology governance system design in local government. Telkomnika (Telecommunication Computing Electronics and Control), 21(4), 750–761. https://doi.org/10.12928/TELKOMNIKA.v21i4.24287

[8] Magdalena, L., & Solihah, Y. A. (2020). Design of IT Governance Evaluation Using COBIT Framework through Capability Maturity in Department of Transportation Cirebon. Journal of Physics: Conference Series, 1641(1). https://doi.org/10.1088/1742-6596/1641/1/012013

[9] Dionisius, Y. B., & Utama, D. N. (2023). Evaluation of the Implementation of Business Continuity Management Using COBIT 2019 Framework in Public Sector. Journal of System and Management Sciences, 13(2), 409–427. https://doi.org/10.33168/JSMS.2023.0228
[10] Metin, B., Duran, S., Telli, E., Mutlutürk, M., & Wynn, M. (2024). IT Risk Management: Towards a System for Enhancing Objectivity in Asset Valuation That Engenders a Security Culture. Information (Switzerland), 15(1). https://doi.org/10.3390/info15010055
[11] Ozkan, N., Tarhan, A. K., Goren, B., Filiz, I., & Ozer, E. (2020). Harmonizing IT Frameworks and Agile Methods: Challenges and Solutions for the case of COBIT and Scrum. Proceedings of the 2020 Federated Conference on Computer Science and Information Systems, FedCSIS 2020, 709–719. https://doi.org/10.15439/2020F47
[12] Ahmed, S., Singh, M., Doherty, B., Ramlan, E., Harkin, K., Bucholc, M., & Coyle, D. (2023). An Empirical Analysis of State-of-Art Classification Models in an IT Incident Severity Prediction Framework. Applied Sciences (Switzerland), 13(6). https://doi.org/10.3390/app13063843
[13] Mueller, R., & Yin, R. (2023). Sentry insurance and california consumer privacy act: a business case on IT governance, data security, and compliance. Issues in Information Systems, 24(3), 174–180. https://doi.org/10.48009/3_iis_2023_115
[14] Levstek, A., Pucihar, A., & Hovelja, T. (2022). Towards an Adaptive Strategic IT Governance Model for SMEs. Journal of Theoretical and Applied Electronic Commerce Research, 17(1), 230–252. https://doi.org/10.3390/jtaer17010012
[15] Dzemydienė, D., Turskienė, S., & Šileikienė, I. (2023). Development of ICT Infrastructure Management Services for Optimization of Administration of Educational Institution Activities by Using ITIL-v4. Baltic Journal of Modern Computing, 11(4), 558–579. https://doi.org/10.22364/bjmc.2023.11.4.03