Journal of Computer Engineering, Electronics and Information Technology (COELITE)

Journal homepage: https://ejournal.upi.edu/index.php/COELITE

Mapping ISO 27001:2013 and COBIT 2019 Framework to STRIDE Threat Modeling Using Qualitative Descriptive Research

Hermawan Setiawan[1], Nisrina Aliya Hana[1], Rayhan Ramdhany Hanaputra[1]*
[1]Crypto Software Engineering, Politeknik Siber dan Sandi Negara, Indonesia
Correspondence: E-mail: hermawan.setiawan@poltekssn.ac.id

ABSTRACT

One of the crucial assets in every organization is information so making its protection through robust information security processes is indispensable. COBIT and ISO/IEC 27001 are key reference frameworks for managing information security, providing organizations with tools to implement controls that are appropriate and assess security risks. Within the COBIT framework, information security management is a core element of IT, focusing on ensuring the resource's integrity, confidentiality, and availability. Given that COBIT's approach to managing information security aligns with the principles of the ISO/IEC 27001 standard, integrating ISO/IEC 27001 into a COBIT-based infrastructure is an ideal strategy for effective information security management. To facilitate their complementary use, mapping COBIT processes to ISO/IEC 27001 controls has proven highly advantageous. In this paper, we want to explore the significance of information security in COBIT and outline a method for mapping COBIT processes to ISO/IEC 27001 controls to enhance the effectiveness of information security management.

ARTICLE INFO

Article History:
Submitted/Received 05 Aug 2024
First Revised 09 Sep 2024
Accepted 01 Oct 2024
First Available online 31 Oct 2024
Publication Date 31 Oct 2024

Keyword:
COBIT,
PDCA cycle,
ISO/IEC 27001,
STRIDE,
management,
Information security

1. INTRODUCTION

In the era of globalization, information security and information technology (IT) governance have become critical factors in determining the operational success of an organization. Along with the increasing dependence on technology, the risks related to information security and IT management are also increasingly complex and diverse. Organizations are faced with the challenge of managing and protecting their information assets from various threats, both internal and external.

According to the National Cyber and Crypto Agency (BSSN) report, Indonesia experienced 88 million cases of cyber attacks from early 2020 to April 12, 2020. Of that number, 56% were identified as trojan activity attacks, 43% of which involved information gathering efforts, and 1% were attacks via web applications [1]. By the end of 2020, the number of cyber attacks had soared to 495 million, with the majority involving trojan activity and data theft [2]. This shows an increase of 205 million cases compared to 2019 which recorded 290 million incidents [3].

Organizations have to implement information security to maintain their operations. to prevent the loss of confidentiality, integrity, and availability. Information security includes protecting data throughout its lifecycle—from creation to disposal—through logical, technical, physical, and organizational measures [4]. Effective implementation of information security ensures specific protection that helps organizations achieve their goals [5]. A survey in the UK showed that 74% of organizations in the technology sector consider high-level security to be an important concern for senior management [6].

Cybersecurity, a subset of information security, focuses on protecting information assets from threats to data processed, stored, and transmitted through interconnected systems [7]. To improve information security in an organization, specific controls are needed to assess the effectiveness of cybersecurity measures. Frameworks such as COBIT and ISO 27001 are commonly used to audit and measure cybersecurity levels [8]. However, the unique needs of each organization often limit the application of these frameworks [1].An effective IT governance and information security management framework is essential to help organizations achieve their strategic objectives while making sure of the integrity and security of data. Two of the most well-known and widely used frameworks in this area are COBIT (Control Objectives for Information and Related Technologies) and ISO/IEC 27001. While both aim to improve information governance and security, their approaches and focus differ significantly.

COBIT, developed by ISACA, is a framework that provides comprehensive guidance on IT governance and management. COBIT provides a structure that enables organizations to achieve their business objectives through effective IT management. The framework covers various aspects of IT, including risk management, internal control, and regulatory compliance. COBIT is designed to help organizations ensure that IT supports and enhances their business strategy.

ISO/IEC 27001, on the other hand, is an international standard that specifies requirements for an information security management system (ISMS). This standard is designed to help organizations manage and protect their information through the systematic and structured implementation of policies and procedures. ISO/IEC 27001 emphasizes the importance of risk management and ongoing information protection, ensuring that organizations can address and mitigate the impact of information security threats.

Although both frameworks share the same ultimate goal of improving information security and governance, their approaches differ. COBIT focuses more on the overall governance of IT, including how IT can support the achievement of business objectives and the management

DOI: https://doi.org/10.17509/coelite.v3i2.73228
p- ISSN 2829-4157 e- ISSN 2829-4149

of IT risks in general. Meanwhile, ISO/IEC 27001 focuses on managing information security through the implementation of an internationally recognized ISMS.

Organizations are often faced with the dilemma of choosing the most appropriate framework for their needs. Understanding the differences, advantages, and disadvantages of each framework is an important step in making the right decision. This study aims to provide a comparative analysis between COBIT and ISO/IEC 27001.

2. METHODS

In this study, a comparison and mapping of features within the cybersecurity framework are conducted using descriptive methods. The analysis utilizes various sources from existing literature, including scientific journals, books, articles in mass media, and statistical data as the primary references [9]. Specifically, this study focuses on comparing and mapping two widely recognized standards for measuring information security: COBIT and ISO 27001. Both standards offer unique advantages and disadvantages, which are analyzed qualitatively using the STRIDE threat model.

3. BASIC CONCEPT

3.1. COBIT Framework

Control Objectives for Information and Related Technology (COBIT) is a framework of best practices for IT governance developed by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) [10]. COBIT equips IT managers, auditors, and users with a set of widely accepted metrics, indicators, processes, and best practices. Its purpose is to help maximize the benefits obtained from IT while establishing appropriate governance and control mechanisms within an organization. The mission of COBIT is to support managers, auditors, and users in understanding their IT systems and determining the required levels of security and control to safeguard enterprise assets by implementing an IT governance model [10]. COBIT is highly versatile and can be applied across a variety of contexts, addressing security and other risks associated with IT usage.

From COBIT's perspective, enterprise governance (the systems used to manage and control an organization) and IT governance (the systems used to manage and control an organization's IT) are tightly interlinked. Enterprise governance cannot function effectively without proper IT governance, and vice versa. While IT can enhance and influence organizational performance, it must operate within a framework of adequate governance. Similarly, business processes rely on information from IT processes, requiring the effective management of this interdependence [11].

The aims of COBIT framework is to provide management with a robust model of IT governance that enables the control and management of information and technologies that are related. This describe how IT supplies the information business objectives needed to achieve. This is facilitated by 34 high-level control objectives, each associated with an IT process, organized into four primary domains. The framework also identifies key information criteria—effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability—as well as critical IT resources, including personnel, applications, technology, facilities, and data, which are essential for supporting business objectives. The IT Governance Institute has defined the core components of the COBIT framework as four domains, structured according to the PDCA cycle, as shown in **Figure 1** [12].

DOI: https://doi.org/10.17509/coelite.v3i2.73228
p- ISSN 2829-4157 e- ISSN 2829-4149

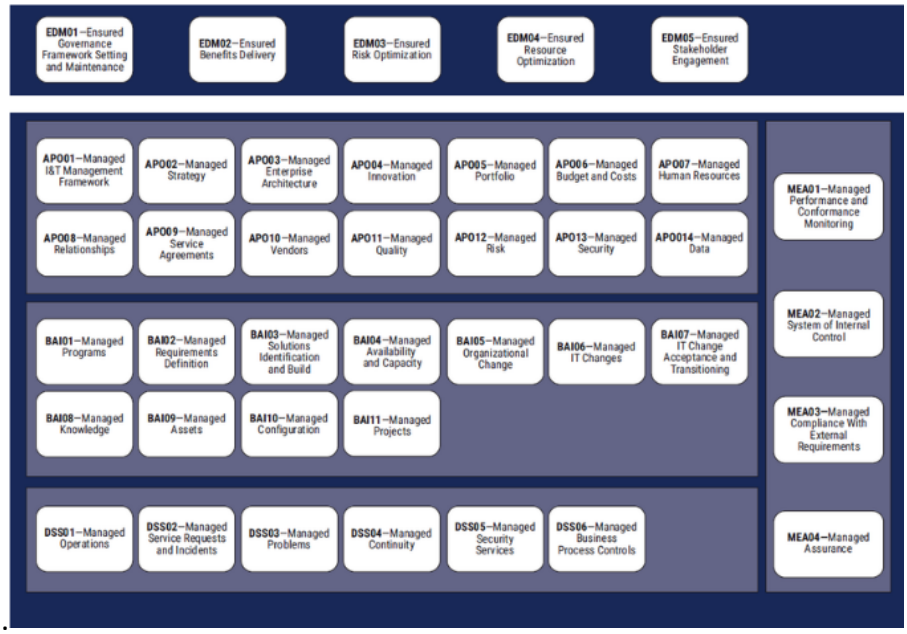

Figure 1. COBIT Domain

Information security that are effective requires a cohesive combination of management, security, and governance processes to organize, plan, and mitigate the security risks of an organization's information. COBIT offers a comprehensive management, governance, and process framework for implementing and managing information security. It outlines effective practices, processes, and control objectives for operating and managing IT systems, including the posture of their security. Organizations that adopt this framework report enhanced capabilities in delivering high-quality services to their customers, along with improved measurement and fulfillment of confidentiality, availability, and integrity requirements. COBIT emphasizes in every business function the importance of integrating security. While only one COBIT process (DS5) is specifically focused on security, security-related control objectives are distributed across processes in all domains. The baseline document of COBIT security [13] Identifies the main overarching COBIT control objectives concerning information security within the four domains of the framework.

3.2 ISO/IEC 27001 Framework

ISO/IEC 27001 originated from a code of best practices published by the UK Department of Trade and Industry in 1989, which eventually evolved into BS7799 [14]. This standard outlines the requirements for the operation, monitoring, assessment, maintenance, establishment, implementation, and continuous improvement of a documented Information Security Management System (ISMS), considering the organization's overall business risks. ISO/IEC 27001 specifies the criteria for implementing security controls tailored to the organization's needs or specific departments. The goal of the ISMS is to support the selection of suitable and proportional security controls to protect information assets and enhance trust with stakeholders.

The standard's requirements are organized into 11 clauses encompassing 39 objectives and 133 controls [15][16].

ISO/IEC 27001 outlines how organizations should address confidentiality, integrity, and availability requirements for their information assets, integrating these principles into their ISMS [17][19]. This global standard is widely adopted by commercial and governmental organizations as a foundation for managing policies and implementing information security

DOI: https://doi.org/10.17509/coelite.v3i2.73228
p- ISSN 2829-4157 e- ISSN 2829-4149

measures. It is used by organizations of various sizes—small, medium, and large—across diverse industries. Its design ensures flexibility, making it applicable to all types of organizations, and it has become the de facto "common language" for managing information security [15][16].

The standard introduces a cyclical model that aims to establish, implement, monitor, and improve the effectiveness of an organization known as the "Plan-Do-Check-Act" (PDCA) model The PDCA cycle has the following four phases as shown in **Figure 2**.

- Plan – establish the ISMS: Develop and define the policies, objectives, processes, and procedures necessary to establish an Information Security Management System (ISMS). This step involves identifying and managing risks to ensure that the outcomes align with the organization's overarching policies and objectives while aiming to enhance information security [10].
- Do – implement and operate the ISMS Execute and manage the established ISMS policies, controls, processes, and procedures to ensure their effective application in safeguarding information security [18].
- Check – monitor and review the ISMS: Evaluate and measure the performance of processes against the established ISMS policies, objectives, and practical experiences. Report the findings to management to facilitate review and ensure continuous improvement [20].
- Act – maintain and improve the ISMS: Implement corrective and preventive actions based on insights from internal ISMS audits, management reviews, or other relevant data. This ensures the ongoing enhancement and effectiveness of the ISMS [4].

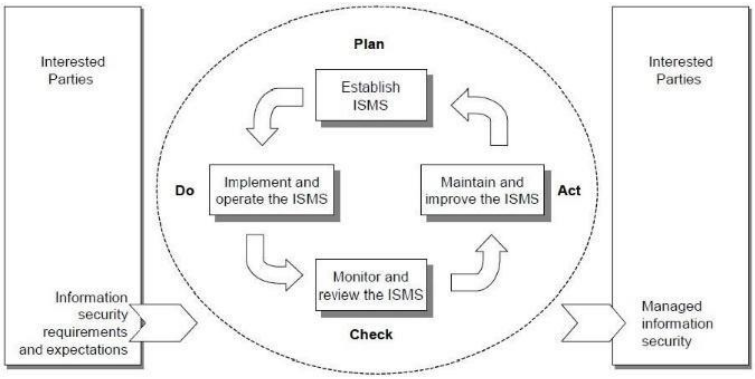

Figure 2. PDCA Model in ISMS Process

Table 1 below serves as a comprehensive overview of the key components necessary for establishing, implementing, maintaining, and continually improving an information security management system (ISMS) in alignment with ISO/IEC 27001.

Table 1. ISO/IEC 27001 Control Objectives.

Controls	Control Objectives
A.5 Security policy	A.5.1 Information security policy
A.6 Organizational information security	A.6.1
A.6.2	External parties
A.7 Asset Management	A.7.1
A.6.3	Information classification
A.8 Human resources security	A.8.1
A.8.2	During employment
A.6.4	Termination or change of employment

DOI: https://doi.org/10.17509/coelite.v3i2.73228
p- ISSN 2829-4157 e- ISSN 2829-4149

A.9 Physical and environmental security	A.9.1
A.6.5	Equipment security
A.10 Communications and operations management	A.10.1

3.3 STRIDE

STRIDE is a threat modeling method used in security analysis to identify and categorize different types of security threats. STRIDE is an acronym for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege [21]. This methodology helps in systematically analyzing potential threats across a wide range of systems, including cyber-physical systems, automotive security, distributed software-defined network applications, control systems, and computer network security [21]. The STRIDE model helps in detecting and preventing threats by guiding Spoofing (a threat to authentication where an unauthorized entity pretends to be a legitimate entity), Tampering (a threat to integrity where data or systems are altered unauthorizedly), Repudiation (a threat to accountability where an entity can deny actions that have been taken), Information Disclosure (a threat to confidentiality where information is leaked to unauthorized parties), Denial of Service (a threat to availability where a service or system becomes unavailable to authorized users), and Elevation of Privilege (a threat to authorization where an entity is granted higher access rights than it should be). The explanation can also be seen in **Figure 3**.

STRIDE-LM	Threat	Property	Definition	Controls
S	Spoofing	Authentication	Impersonating someone or something	Authentication Stores, Strong Authentication mechanisms
T	Tampering	Integrity / Access Controls	Modifying data or code	Crypto Hash, Digital watermark/ isolation and access checks
R	Repudiation	Non-repudiation	Claiming to have not performed a specific action	Logging infrastructure, full-packet-capture
I	Information Disclosure	Confidentiality	Exposing information or data to unauthorized individuals or roles	Encryption or Isolation
D	Denial of Service	Availability	Deny or degrade service	Redundancy, failover, QoS, Bandwidth throttle
E	Elevation of Privilege	Authorization / Least Privilege	Gain capabilities without proper authorization	RBAC, DACL, MAC; Sudo, UAC, Privileged account protections

Figure 3. Figure of Explanation STRIDE Threat Model

4. RESULTS AND DISCUSSION

The key distinction lies in their focus between COBIT and ISO 27001: ISO 27001 is dedicated only to information security, while COBIT addresses broader aspects of information technology controls. Consequently, COBIT has a wider scope encompassing general IT governance but lacks the requirements of detailed security provided by ISO 27001. If an organization implements all ISO 27001 security controls, it would inherently address a significant portion of COBIT, particularly the DS5 section, which focuses on system security. However, COBIT extends beyond security to include various aspects of IT governance, often forming part of a broader corporate governance framework.

Information security management is one critical area in COBIT , which ensures the integrity, confidentiality, and availability of resources. Since ISO/IEC 27001 also covers these areas and incorporates the PDCA cycle as a foundational structure, integrating ISO/IEC 27001 within the COBIT framework is an effective approach to managing information security.

To facilitate the complementary use of these frameworks, mapping COBIT processes to ISO 27001 control objectives proves highly beneficial. This mapping provides an integrated method for using both frameworks together in information security management. By aligning

DOI: https://doi.org/10.17509/coelite.v3i2.73228
p- ISSN 2829-4157 e- ISSN 2829-4149

ISO 27001 controls with COBIT processes, organizations can achieve cost efficiencies, better risk management, and reduced overall risk.

The mapping involves analyzing each COBIT process and identifying its corresponding ISO 27001 Annex A control objectives. **Table 2** illustrates the relationships between the domains of ISO/IEC 27001:2005 and COBIT processes, detailing how their subjects and control parameters align.

Table 2. Mapping of ISO/IEC 27001 and COBIT to STRIDE Threat Model.

No	ISO/IEC 27001	COBIT 2019	STRIDE Threat Model
1	Management direction for information security	EDM (Evaluate, Direct, and Monitor)	I - Information Disclosure
2	Internal organization	EDM	I - Information Disclosure
3	Mobile devices and teleworking	EDM	T - Tampering
4	Before employment	APO 07 (Manage Human Resources)	S - Spoofing
5	During employment	APO 07	S - Spoofing
6	Termination and change of employment	APO 07	S - Spoofing
7	Responsibility for assets	BAI 09 (Manage Assets)	I - Information Disclosure
8	Information classification	BAI 09	I - Information Disclosure
9	Media handling	BAI 09	T - Tampering
10	Business requirements of access control	DSS 05 (Manage Security)	T - Tampering
11	User access management	DSS 05	S - Spoofing
12	User Responsibilities	DSS 05	S - Spoofing
13	System and application access control	DSS 05	T - Tampering
14	Cryptographic controls	DSS 05	I - Information Disclosure, T - Tampering
15	Secure areas	DSS 05	T - Tampering
16	Equipment	DSS 05	T - Tampering
17	Operational procedures and responsibilities	DSS 01 (Manage Operations)	T - Tampering
18	Protection from malware	DSS 05	I - Information Disclosure, T - Tampering
19	Backup	APO 14 (Manage Availability)	T - Tampering
20	Logging and monitoring	DSS 05	S - Spoofing, T - Tampering
21	Control of operational software	DSS 05	T - Tampering
22	Technical vulnerability management	DSS 05	I - Information Disclosure, T - Tampering
23	Information systems audit considerations	MEA 04 (Monitor, Evaluate, and Assess)	S - Spoofing

DOI: https://doi.org/10.17509/coelite.v3i2.73228
p- ISSN 2829-4157 e- ISSN 2829-4149

24	Network security management	DSS 05	T - Tampering
25	Information transfer	DSS 05	I - Information Disclosure
26	Security requirements of information systems	APO 13 (Manage Security)	S - Spoofing
27	Security in development and support processes	APO 04 (Manage Development)	S - Spoofing, T - Tampering
28	Test data	APO 14	T - Tampering
29	Information security in supplier relationships	APO 10 (Manage Supplier Relationships)	S - Spoofing
30	Supplier service delivery management	APO 10	S - Spoofing
31	Management of information security incidents and improvements	DSS 05	I - Information Disclosure, T - Tampering
32	Information security continuity	DSS 04 (Manage Continuity)	T - Tampering
33	Redundancies	DSS 04	T - Tampering
34	Compliance with legal and contractual requirements	MEA 03 (Monitor, Evaluate, and Assess Compliance)	S - Spoofing
35	Information security reviews	APO 13	S - Spoofing

The following **Table 3** provides a detailed overview of these mappings, highlighting the alignment between the standards and the threat model to enhance organizational security posture.

Table 3. Scenario Example of Threat

No	Scenario	Threat	ISO/IEC 27001	COBIT 2019	STRIDE
1	Data Theft through Unauthorized Access	Spoofing (S)	11. User Access Management	DSS 05 (Manage Security)	S – Spoofing
2	Malware Attack on the System	Tampering (T)	18. Protection from Malware	DSS 05 (Manage Security)	I - Information Disclosure, T – Tampering
3	Non-compliance with regulations	Spoofing (S)	34. Compliance with Legal and Contractual Requirements	MEA 03 (Monitor, Evaluate, and Assess Compliance)	S – Spoofing

In scenario 1, attackers gain unauthorized access to a system due to inadequate access controls. This poses a significant risk of data theft. By mapping the ISO/IEC 27001 standard, specifically the user access management controls, and the COBIT 2019 framework, particularly the DSS 05 domain focused on security management, organizations can implement stricter access controls and user management protocols. This ensures that only authorized individuals have access to sensitive information and reduces the risk of data theft through unauthorized access.

Scenario 2 involves malware infiltrating the system, causing damage, or accessing sensitive information. Such an attack can lead to data tampering and information disclosure.

DOI: https://doi.org/10.17509/coelite.v3i2.73228
p- ISSN 2829-4157 e- ISSN 2829-4149

By implementing the controls outlined in ISO/IEC 27001 for malware protection and leveraging the security management practices from COBIT 2019, organizations can prevent their malware attacks and enhance their ability to detect them. These measures include robust malware protection strategies and continuous security monitoring, which help safeguard systems from malicious software.

In scenario 3, an organization fails to meet applicable regulatory requirements, which can result in fines or reputational damage. By clearly mapping the requirements of ISO/IEC 27001 and COBIT 2019, organizations can ensure better compliance with legal and contractual obligations. The ISO/IEC 27001 standard emphasizes compliance with regulatory requirements, while COBIT 2019's MEA 03 domain focuses on monitoring, evaluating, and assessing compliance. Together, these frameworks provide an approach that is comprehensive to maintain compliance and mitigate the risks associated with regulatory non-compliance.

5. CONCLUSION

Information security is essential for safeguarding organizational assets. Given that no single approach can guarantee complete security, implementing benchmarks or standards is crucial to ensure sufficient security levels, optimize resource usage, and adopt best practices. Frameworks like COBIT and ISO/IEC 27001 can serve as a combined foundation for establishing a robust information security process. To leverage the complementary nature of these frameworks, COBIT processes can be aligned with the control objectives of ISO/IEC 27001. This paper provides a comparison between the two frameworks, illustrating how their alignment can assist organizations in reducing costs while ensuring adequate security levels, managing risks efficiently, and lowering overall risk exposure. Furthermore, this mapping helps mitigate misunderstandings and inconsistencies between IT and Audit. Future efforts will focus on creating a comprehensive, cost-efficient framework to balance the implementation of ISO/IEC 27001 and COBIT processes in organizations.

6. AUTHORS' NOTE

The authors affirm that there are no conflicts of interest related to the publication of this article. They also confirm that the paper is free from plagiarism.

7. REFERENCES

[1] E. Handoyo. "Analisis Tingkat Keamanan Informasi: Studi Komparasi Framework Cobit 5 Subdomain Manage Security Services (DSS05) dan NIST Sp 800 – 55," *J. CoSciTech Computer Sci. Inf. Technol.*, vol. 1, no. 2, pp. 76–83, Oct. 2020. doi: 10.37859/coscitech.v1i2.2199.

[2] "Rekap Serangan Siber (Januari - April 2020)," *BSSN*, Online. Available: https://www.bssn.go.id.

[3] "BSSN: Malware Trojan Dominasi Serangan Siber di 2020," *Tempo.co*, Online. Available: https://www.tempo.co/.

[4] "Laporan Tahunan 2019 PUSOPSKAMSINAS," *BSSN*, Online. Available: https://www.bssn.go.id.

[5] A. Ključnikov, L. Mura, and D. Sklenár, "Information Security Management in SMEs: Factors of Success," *Entrep. Sustain*. Issues, vol. 6, no. 4, pp. 2081–2094, Jun. 2019. doi: 10.9770/jesi.2019.6.4(37).

[6] Department for Digital Culture Media and Sport, "Reino Unido Cyber Security 2018," *Cyber Security. Breaches Surv.*, no. 1, pp. 1–58, 2018.

DOI: https://doi.org/10.17509/coelite.v3i2.73228
p- ISSN 2829-4157 e- ISSN 2829-4149

[7] M. G. Cains, L. Flora, D. Taber, Z. King, and D. S. Henshel, "Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation," *Risk Anal*, Vol. 42, No.8, pp. 1643-1649. Feb. 2021. doi: https://doi.org/10.1111/risa.13687.

[8] D. Sulistyowati, F. Handayani, and Y. Suryanto, "Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology using nist csf, cobit, iso/iec 27002 and pci dss" *Int. J. Informatics Vis.*, vol. 4, no. 4, pp. 225–230, Jul. 2020. DOI: 10.30630/joiv.4.4.482.

[9] D. Prasanti, D. R. Fitriani, "Penelitian Kepustakaan (Library Research) dalam Penelitian Pendidikan IPA," Pembentukan Anak Usia Dini Keluarga, Sekolah, Dan Komunitas, vol. 2, no. 1, p. 15, jun. 2018. DOI: 10.31004/obsesi.v2i1.2

[10] Etzler, J. (2008). IT Governance According to COBIT (Master's Thesis). Royal Institute of Technology, Stockholm, Sweden. OAI: https://api.core.ac.uk/oai/oai:CiteSeerX.psu:10.1.1.66.2955

[11] IT Governance Institute (ITGI). (2000). *COBIT Mapping: Mapping of ISO/IEC 17799:2000 with COBIT*, 2nd Edition, Printed in the United States of America, United States of America.

[12] R. Witjaksono. "Audit Sistem Informasi Akademik Universitas Telkom Menggunakan Framework COBIT 5 Domain DSS Untuk Optimasi Proses Service Delivery," *Jurnal Rekayasa Sistem & Industri (JRSI)*, 6(01), 16-23. Jun. 2019. doi: 10.25124/jrsi.v6i1.341

[13] IT Governance Institute (ITGI), "COBIT Security Baseline. An Information Security Survival Kit", Rolling Meadows: Author. Retrieved (2008) Jun. 30, from http://www.isaca.org.

[14] A. A. Alrehili and O. H. Alhazmi, "ISO/IEC 27001 standard: Analytical and Comparative Overview," in *Proc. Int. Conf. Adv. Data-driven Comput. Intell. Syst.*, Sep. 2023, pp. 143–156. doi: 10.1007/978-981-99-9524-0_12.

[15] M. Stamp, *Information Security: Principles and Practice*. Hoboken, NJ, USA: Wiley, 2011.

[16] T. R. Peltier, *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*. Boca Raton, FL, USA: CRC Press, Apr. 2016.

[17] K. L. Thomson and R. V. Solms, "Information Security Obedience: a Definition", J Computers & Security, Vol. 24, pp. 69-75, Feb 2005. doi: 10.1016/j.cose.2004.10.005.

[18] T. Humphreys. *Guide to the Implementation and Auditing of ISMS Controls Based on ISO/IEC 27001*, BSI British Standards Institution, 2005.

[19] Ganji D, Kalloniatis C, Mouratidis H, Gheytassi SM. Approaches to Develop and Implement iso/iec 27001 Standard-Information Security Management Systems: A Systematic Literature Review. Vol.12, No.3, pp. 228-238, *Int. J. Adv. Softw*. 2019.

[20] Haufe, Knut, et al. "A Process Framework for Information Security Management." *International Journal of Information Systems and Project Management*, Vol. 4, No.4, pp. 27-47. Aug. 2016. doi: 10.12821/ijispm040402

[21] H. Kayan, M. Nunes, O. Rana, P. Burnap, C. Perera. "Cybersecurity of Industrial Cyber-Physical Systems: A review". *ACM Computing Surveys (CSUR)*. Vol.54, No.11, pp. 1-35 Sep. 2022. doi: https://doi.org/10.1145/3510410