Implementation of APO12, APO13 and DSS05 Sub-Domains in COBIT 2019 to Improve Information System Security at LAZIS Sabilillah Malang

Mahdi Romzuz Zaki[1], Arif Tirtana[2*]

[1,2] Information Systems, Faculty of Science and Technology, Jl. Raya Tidar No.100, Karangbesuki, Kec. Sukun, Kota Malang, Jawa Timur 65146, Indonesia

Keywords
Information; Software; Application; System

***Correspondence Email:**
arif.tirtana@ubhinus.ac.id

Abstract
The rapid digital transformation requires non-profit organizations such as LAZIS Sabilillah Malang to adopt a robust information security system. A ransomware attack in 2022 exposed the vulnerabilities in their current governance practices. This research aims to enhance the organization's information security by implementing APO12 (Managed Risk), APO13 (Managed Security), and DSS05 (Managed Security Services) sub-domains from the COBIT 2019 framework. A qualitative case study method was used, supported by descriptive analysis through interviews, observations, and questionnaires using a Likert scale distributed to four key informants. The results indicate that most sub-domains have not yet reached the target capability level, with an average gap of one level below the standard. This study delivers a set of Standard Operating Procedures (SOPs) as practical references and a prioritized roadmap for improvement based on urgency and feasibility.

1. Introduction

Cybersecurity threats in Indonesia have increased significantly. In early 2024, the National Cyber and Crypto Agency (BSSN) recorded more than 74 million anomalous digital activities, with approximately 44 million of them related to malware activities (CNN Indonesia, 2024). This condition places considerable pressure on various institutions, including non-profit organizations, to strengthen their information systems and governance mechanisms in order to protect sensitive data and ensure service continuity. One of the non-profit organizations that plays an important role in managing social funds is LAZIS Sabilillah Malang (Lembaga Amil Zakat, Infaq, dan Shodaqoh). Operating under the auspices of Yayasan Sabilillah Malang, LAZIS Sabilillah is responsible for managing zakat, infaq, and sadaqah (ZIS) funds collected from the public and distributing them through social, educational, and humanitarian programs.

In carrying out this mandate, LAZIS Sabilillah relies heavily on information systems to support transparency, accountability, and public trust, particularly in managing donor personal data and institutional financial reports. However, in June 2022, LAZIS Sabilillah experienced a ransomware attack that targeted its Network Attached Storage (NAS) data storage system. This incident severely disrupted access to operational data and posed significant risks to the confidentiality and integrity of the managed information. Post-incident evaluation revealed several weaknesses in information security governance, including the absence of structured risk management, lack of access control policies, and low staff awareness of cybersecurity practices. In response to these challenges, this study proposes the adoption of the COBIT 2019 framework, which provides a comprehensive, structured, and business-aligned approach to information technology governance. Three sub-domains of COBIT 2019 are the primary focus of this research:APO12 – Managed Risk.

- APO12 – Managed Risk.
- APO13 – Managed Security.
- DSS05 – Managed

Security ServicesThese sub-domains were selected because they are directly related to the challenges faced by LAZIS Sabilillah in risk management, information security, and operational protection. Although the COBIT framework has been widely applied in both public and private sectors, its implementation in the philanthropic or non-profit sector remains relatively limited, thus creating an important research gap to be explored. By evaluating the current capability level and identifying governance gaps in LAZIS Sabilillah's IT practices, this study aims to provide implementable recommendations in the form of Standard Operating Procedure (SOP) documents and a priority roadmap that can be practically applied by the organization.

1.1 Literature Review

Cybersecurity has become a global concern, especially with the increasing number of digital threats that affect organizations across multiple sectors. In Indonesia, reports from the National Cyber and Crypto Agency (BSSN) highlight the rapid escalation of digital attacks, particularly ransomware and malware, which demand stronger security governance frameworks (CNN Indonesia, 2024). This aligns with global findings where ransomware attacks are recognized as one of the most disruptive threats to information systems, causing significant financial and operational damage (Alqahtani et al., 2022).

Non-profit organizations (NPOs) face particular challenges in cybersecurity due to their limited resources, lack of structured IT governance, and high dependence on digital platforms to manage donor data and financial records (Khan et al., 2021). As shown in previous studies, the absence of standardized security policies and low awareness among staff members often increase vulnerabilities, making NPOs attractive targets for cybercriminals (Kim & Kim, 2020). For institutions like LAZIS Sabilillah Malang, which handle sensitive data in managing Zakat, Infaq, and Sadaqah (ZIS) funds, these risks directly affect accountability, transparency, and public trust.

The COBIT 2019 framework has emerged as a comprehensive approach to aligning IT governance with organizational objectives while strengthening information security controls (ISACA, 2019). Several studies have emphasized the effectiveness of COBIT sub-domains in addressing risk management and information security issues. For example, research by Sari et al. (2021) demonstrated that APO12 (Managed Risk) provides structured mechanisms to identify, assess, and mitigate IT risks systematically. Similarly, APO13 (Managed Security) has been proven to improve information security by integrating preventive, detective, and corrective controls into organizational practices (Putra & Nugroho, 2022). Meanwhile, DSS05 (Managed Security Services) ensures operational continuity by establishing procedures for monitoring, responding to, and recovering from security incidents (Rahman et al., 2023).

Although COBIT has been extensively applied in both public and private sectors, its implementation in the non-profit sector remains underexplored. Prior research has mostly focused on enterprises and government institutions, with limited emphasis on philanthropic organizations, which often lack the resources and expertise for advanced IT governance frameworks (Mardiana & Utomo, 2020). This gap highlights the importance of applying and adapting COBIT 2019 in contexts such as LAZIS Sabilillah Malang to enhance information security governance, minimize risks, and sustain organizational trust.

2. Research Methods

This study aims to measure and evaluate information security governance at LAZIS Sabilillah Malang using the COBIT 2019 framework. Data collection methods include literature review, observation, questionnaires, and interviews with the operations manager, IT consultant, and head of the IT division. The collected data were used to determine the achieved Capability Level, conduct gap analysis, and establish target levels. The results of the analysis served as the basis for developing Standard Operating Procedures (SOPs) and policy recommendations to strengthen information security, focusing on the APO12, APO13, and DSS05 sub-domains. A final evaluation was conducted with a COBIT 2019-certified auditor to ensure the validity and feasibility of the outcomes as a reference for the organization.

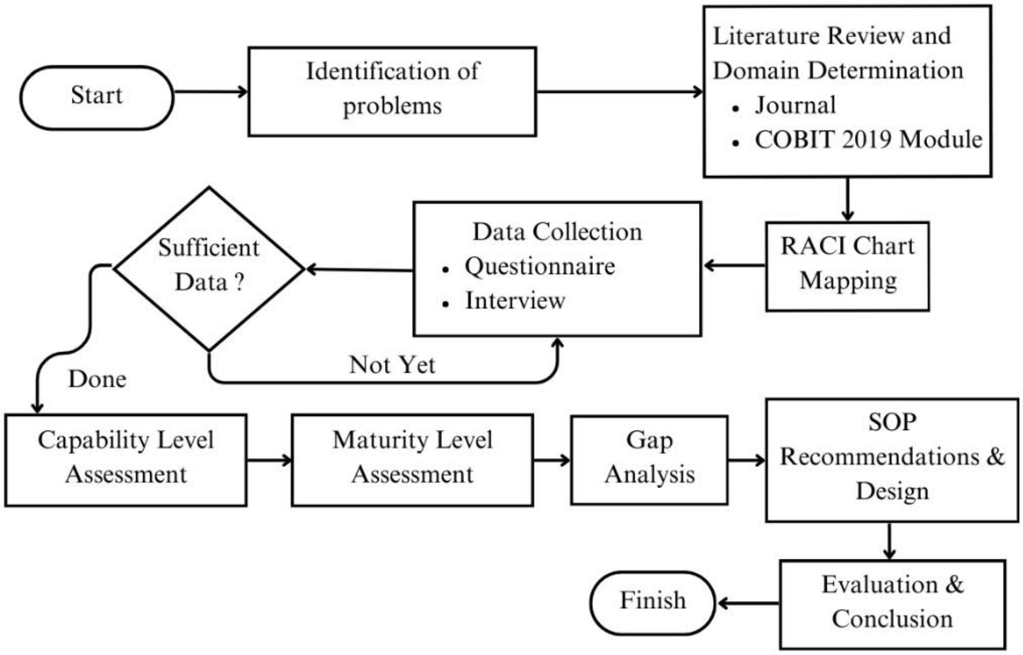

Fig. 1. Flowchart

Data Collection

Data collection in this study was carried out through several methods, namely literature review, direct observation in the working environment of LAZIS Sabilillah Malang, distribution of Likert scale–based

questionnaires, and in-depth interviews. The literature review was conducted to understand the concepts and standards of COBIT 2019, particularly the APO12, APO13, and DSS05 sub-domains. Observation aimed to identify the actual conditions of information security governance. The questionnaire was designed to measure capability levels based on COBIT 2019 indicators, while interviews were conducted with key stakeholders such as the operations manager, head of the IT division, and external consultants to gain deeper insights into the ongoing processes and to determine realistic target levels. The collected data were then analyzed to assess capability levels and formulate recommendations for enhancing information security.

COBIT 2019

COBIT 2019, an acronym for Control Objectives for Information and Related Technology, is a framework developed to govern and manage information and technology. COBIT defines the essential elements required to build and maintain an effective management system, including processes, organizational structures, policies and procedures, information flows, culture and behavior, skills, as well as supporting infrastructure (Saleh et al., 2021).

LAZIS Sabilillah

LAZIS Sabilillah is a zakat, infaq, and sadaqah management institution based in Malang, Indonesia, focusing on the collection and distribution of social funds for educational, social, and economic empowerment programs. As a philanthropic organization, LAZIS Sabilillah upholds transparency and accountability by utilizing digital technologies such as an Android-based zakat application and the Sistem Informasi Mustahik (SIM) in its operations. The use of these information systems requires the application of information security principles—confidentiality, integrity, and availability—to ensure both efficiency and security in managing data and distributing aid to beneficiaries.

Process Assessment Model

Information Technology (IT) objectives must be aligned with the vision and mission of the organization to ensure effective and efficient management by balancing benefits, risks, and resources. In this study, the author employed the COBIT 2019 framework and conducted preliminary observations to understand the business objectives and IT processes at LAZIS Sabilillah Malang. Based on these observations, three sub-domains relevant to information security were identified: APO12 (Managed Risk), APO13 (Managed Security), and DSS05 (Managed Security Services).

The APO12 sub-domain focuses on IT risk management through six processes, ranging from data collection to risk response. The APO13 sub-domain consists of three processes that emphasize the establishment and monitoring of an Information Security Management System (ISMS). Meanwhile, DSS05 serves to maintain IT security risks in accordance with applicable policies and encompasses seven processes, including protection against malware, network security management, endpoint security, user identity management, physical access control, sensitive document handling, and infrastructure monitoring. These three sub-domains form the foundation for the assessment and design of information security governance within the organization.

Analisis Capability Level

Process capability level analysis serves as an indicator of how well a process is being carried out. The higher the capability level, the more optimally the process is implemented. Capability level progression is cumulative, meaning that each level builds the foundation for the subsequent one (Sukamto et al., 2021). COBIT 2019 adopts a process capability scheme based on the Capability Maturity Model Integration (CMMI) to assess whether governance and control objectives are performed at varying functional levels, ranging from 0 to 5 (ISACA, 2019).

Analisis Kesenjangan

Gap analysis is used to compare an organization's current condition with the desired ideal state. In other words, the purpose of this analysis is to identify the differences between what currently exists and what should be in place. By conducting this comparison, it becomes possible to determine which areas need improvement or updates. The results of the gap analysis can then serve as the basis for developing a more focused and efficient action plan. Simply put, gap analysis helps us understand where we are now and what must be done to achieve the intended objectives (Yulianto, 2024).

3. Result and Discussion

Role Identification

The identification of role classification and responsibilities of employees or related parties in LAZIS Sabilillah's activities, particularly within the IT Media division, is presented using a RACI Chart. The distribution of roles and responsibilities is explained in the table below:

Table 1. RACI Matrix

Activities	IT Staff	IT Manager	Operational Manager	IT Consultant
APO12: Managed Risk				
1. Identify IT security risks	R	A	C	C
2. Assess impact and probability of risk	R	A	I	C
3. Prepare risk mitigation	R	A	C	R
4. Monitor effectiveness of risk mitigation	R	A	I	I
APO13: Managed Security				
1. Identify regulations	R	A	C	C
2. Implement compliance controls	R	A	I	C

3. Conduct internal/external compliance audit	R	A	I	C
4. Report audit results to management	R	A	I	C
DSS05: Managed Security Services				
1. Arrange physical access to server room	R	A	C	C
2. Implement CCTV system	R	A	I	C
3. Maintain protection systems	R	A	I	C
4. Conduct incident response simulation	R	A	C	C

The classification of roles and responsibilities in the RACI Chart was developed based on the COBIT 2019 framework and adapted to the context of LAZIS Sabilillah as a non-profit organization. The IT staff act as Responsible, as their duties involve carrying out operational tasks such as the installation of surveillance cameras (CCTV). The IT manager is designated as Responsible for all IT activities due to their position as the decision-maker for technical policies. The operations manager serves as Consulted for activities related to operational workflows, such as the integration of compliance with organizational SOPs. Meanwhile, the IT consultant plays both Consulted and Responsible roles in activities requiring specialized expertise, such as the development of risk mitigation plans.

Questionnaire and Interview Results

This section presents the results of the questionnaire responses and in-depth interviews involving four respondents who have direct responsibility for managing the information system at LAZIS Sabilillah Malang. The recap of the questionnaire responses from the four respondents, along with the calculated average scores, is presented as follows:

Table 2. Capability Level Evaluation

Sub-Domain	**Sub-Domain Average Score**	**Target CMMI to-be (ISACA Standard)**	**Achievement (%)**	**Capability Level (as-is)**	**CMMI Level (as-is)**	**Gap**
APO12 – Managed Risk	1.325	3	44%	2	2 (Managed)	-1
APO13 – Managed Security	1.5	4	38%	2	2 (Managed)	-2
DSS05 – Managed Security Services	2.25	3	75%	4	4 (Predictable)	+1

The calculation results indicate that APO12 – Managed Risk is still below the minimum standard level, with the current score at level 2 compared to the minimum standard of level 3. APO13 – Managed Security is also below the standard, with a current score of level 2 against the standard level of 4. Meanwhile, DSS05 – Managed Security Services has reached level 4, which exceeds the predetermined minimum standard of level 3.

Furthermore, the table above also presents the results in relation to the Capability Maturity Model Integration (CMMI), as explained in Figure 2.5 Capability Levels for Process and further detailed in Table 2.2 Description of Process Capability Levels. The results show that APO12 and APO13 both reached level 2, which indicates that the processes achieve their objectives through the implementation of a complete set of basic activities, categorized as "operating." In contrast, DSS05 achieved level 4, meaning that the process consistently achieves its objectives, is well-defined, and its performance can be measured quantitatively.

These findings demonstrate that DSS05 possesses a higher level of maturity compared to APO12 and APO13. Nevertheless, all three sub-domains still indicate the need for significant improvement, particularly in terms of process documentation, monitoring, and quantitative performance measurement.

4. Conclusions

This study aims to evaluate and implement the APO12 (Managed Risk), APO13 (Managed Security), and DSS05 (Managed Security Services) domains of COBIT 2019 in order to enhance information system security at LAZIS Sabilillah Malang. Based on the results of questionnaires and interviews with four key respondents, it was found that most processes related to risk management and information security were still at relatively low levels of capability and maturity. From the capability level analysis, only the DSS05 sub-domain had reached level 4, while APO12 and APO13 remained at level 2. In terms of maturity level, DSS05 was assessed at level 3 (Defined), APO12 at level 2 (Managed), and APO13 at level 1 (Initial). These results indicate that information security governance at LAZIS Sabilillah is not yet optimal and requires gradual and continuous improvement.

As an outcome of this research, the author formulated a set of Standard Operating Procedures (SOPs) designed to support the improvement and strengthening of information system security. The SOPs were developed based on the identification of process activities that are both urgent and feasible to be implemented immediately. The implementation of these SOPs is expected to help the organization reduce the gap between the current and ideal conditions in accordance with COBIT 2019 standards.

5. References

Agustinus, M., & Zuraidah, E. (2023). Kajian ilmiah informatika dan komputer audit sistem informasi absensi fingerprint menggunakan COBIT 5. KLIK: Kajian Ilmiah Informatika dan Komputer, 4(2), 854–863. https://doi.org/10.30865/klik.v4i2.1082

Akbar, H., & Saputra, R. (2023). Evaluasi kinerja tata kelola teknologi informasi terhadap tools internal framework COBIT 2019. Sebatik, 27(2), 27. https://doi.org/10.46984/sebatik.v26i2.2336

Alfiana, A., Lubis, R. F., Suharyadi, M. R., Utami, E. Y., & Sipayung, B. (2023). Manajemen risiko dalam ketidakpastian global: Strategi dan praktik terbaik. Jurnal Bisnis dan Manajemen West Science, 2(3).

Algiffary, M. A., Herdiansyah, M. I., & Kunang, Y. N. (2023). Audit keamanan sistem informasi manajemen rumah sakit dengan framework COBIT 2019 pada RSUD Palembang BARI. Journal of Applied Computer Science and Technology (JACOST), 4(1), 2723–1453. https://doi.org/10.52158/jacost.505

CNN Indonesia. (2024, May 16). BSSN deteksi 44 juta aktivitas malware hingga Mei 2024. CNN Indonesia. https://www.cnnindonesia.com/teknologi/20240516184354-185-1098626/bssn-deteksi-44-juta-aktivitas-malware-hingga-mei-2024

ISACA. (2019). COBIT 2019 framework: Governance and management objectives.

Saleh, M., Nawawi, H., & Barat, K. (2021). Penerapan framework COBIT 2019 pada audit teknologi informasi di Politeknik Sambas. Jurnal Edukasi dan Penelitian Informatika, 7(2).

Sukamto, A. S., Novriando, H., Reynaldi, A., & Nawawi, H. (2021). Tata kelola teknologi informasi menggunakan framework COBIT 2019 (Studi kasus: UPT TIK Universitas Tanjungpura Pontianak).

Yulianto, A. (2024). Gap analysis penerapan sistem manajemen keselamatan ketenagalistrikan bidang instalasi pemanfaatan tenaga listrik di Lembaga Diklat XYZ. SoSAINS. http://sosains.greenvest.co.id