International Journal of Advances in Data and Information Systems
Vol. 7, No. 2, August 2026, pp. 534~545
ISSN: 2721-3056, DOI: 10.25008/ijadis.v7i2.1538

Information Security Governance Model for Higher Education Based on ISO/IEC 27001:2022 and COBIT 2019

Neonatal March Parera[1], Wiwin Sulistyo[2], Johan Jimmy Carter Tambotoh[3]
[1,2,3]Faculty of Information Technology, Satya Wacana Christian University, Indonesia

Article Info
Article history:
Received Feb 10, 2026
Revised Mar 04, 2026
Accepted Mar 22, 2026

Keywords:
COBIT 2019,
Higher Education,
Information Security,
IT Governance,
ISO/IEC 27001:2022.

ABSTRACT
Higher education institutions manage large volumes of sensitive information, including personal data of students and staff, research data, financial records, and operational information. The increasing number of cyber incidents affecting universities, both globally and in Indonesia, indicated the need for a more structured approach to information security governance. This study aimed to develop an information security governance design model through the integration of ISO/IEC 27001:2022 and COBIT 2019. The research adopted a design science research methodology. The proposed model integrated ISO/IEC 27001:2022 information security controls with COBIT 2019 governance and management objectives and determined the expected capability level using COBIT design factors. The model was demonstrated through a case study at an Indonesian higher education institution, where the current capability levels were assessed using the Not, Partially, Largely, and Fully achieved rating scale. The results showed that all eight evaluated objectives were at Capability Level 2, with scores ranging from 37.40% to 62.56%, indicating that governance processes had been implemented but were not yest consistently documented and managed. The evaluation demonstrated that the proposed model can serve as a practical reference for assessing and improving information security governance in higher education institutions.

This is an open access article under the CC BY-SA license.

Corresponding Author:
Neonatal March Parera,
Faculty of Information Technology, Satya Wacana Christian University,
Dr. O. Notohamidjojo Street, Blotongan, Sidorejo, Salatiga City-50715, Central Java, Indonesia.
Email: neonatalparera@gmail.com

1. INTRODUCTION

Higher education is a sector that handles sensitive data, such as personal information of academics, research data, financial data, and other data. However, in the past two decades, American educational institutions have recorded 3,173 data breaches that compromised more than 37.6 million records [1]. This vulnerability can arise from universities storing intellectual property, high-value research data, and extensive personal databases [2]. This situation is relevant in Indonesia, given that there are 4,416 universities, which include nearly 10 million students and more than 303,000 lecturers [3]. This number indicates the large volume of sensitive data managed by each university. The various data breach incidents that have occurred at various universities in Indonesia [4], [5], [6], indicate that the higher education sector in Indonesia still faces serious challenges in information security. Sikman et al. (2023) emphasized the importance of maintaining information security in higher education institutions, given the high risk of cyber threats that impact data integrity and the continuity of academic operations [7].

Given these problems, what solutions can be offered to improve information technology security in higher education? One solution to address these issues is implementing good information security governance in higher education [8], [9], [10]. This is evidenced by several studies, Mohd Nordin et al. (2022), which showed that implementing good governance at

University X can improve risk management and operations by improving information storage, dissemination, and security [11]. Furthermore, other studies highlight the large amount of data within an educational institution, requiring information governance to protect data assets and guide data processes to achieve organizational goals [12]. These studies demonstrate the importance of implementing good governance to improve data privacy and university operations.

Various frameworks can be used to design information security governance, such as ISO/IEC, COBIT, NIST, and ITIL [13]. This study will focus on integrating the ISO/IEC 27001:2022 and COBIT 2019 frameworks. Both frameworks have been globally recognized by various countries and are flexible and can be applied to various fields, including in the context of higher education [14]. COBIT 2019 covers a broad range of IT governance and management, but lacks detailed information security control requirements like ISO/IEC 27001:2022 [15]. Recent studies have also emphasized that information security governance in higher education can be strengthened through the integration of governance frameworks and information security standards, enabling institutions to align security controls with organizational objectives and risk management practices [16]. Therefore, ISO/IEC 27001:2022 complements COBIT 2019 in implementing better information security governance.

Several studies have examined the integration of ISO/IEC 27001 with COBIT 2019. A study by Gunawan et al. (2020) showed that the integration of COBIT 2019 and ISO/IEC 27001 was more effective in enhancing information security credibility and facilitating coordination across organizational units than the integration of ITIL and ISO/IEC 27001 [17]. Sikman et al. (2023) explained in their study that the use of ISO/IEC 27001:2013 and COBIT 2019 can create a more comprehensive approach to managing information security risks in higher education institutions [7]. Another study by Aflakhah and Soewito (2023) also highlighted the importance of integrating COBIT 2019 and ISO/IEC 27001:2013 in strengthening information security governance in the public sector [18]. Similar research was conducted by Yasin et al. (2020), and the results showed that integrating these two frameworks can improve the effectiveness of information security governance and risk management processes [19].

Based on previous research, integration between ISO/IEC 27001 and COBIT 2019 has been conducted. However, there is still limited research using the integration of ISO/IEC 27001:2022 to build an information security governance model in Indonesia specifically aimed at the higher education sector, which has unique characteristics such as the complexity of the academic system, the large number of stakeholders, and the obligation to comply with educational regulations. Therefore, this study fills this gap by developing an information security governance design model based on the integration of ISO/IEC 27001:2022 and COBIT 2019, which is expected to be a reference in the implementation and evaluation of information security governance in higher education environments in Indonesia.

2. RESEARCH METHOD

This research uses the Design Science Research (DSR) methodology. Design Science Research is a research methodology that focuses on the creation and evaluation of artifacts to systematically solve real-world problems [20]. In the context of information systems, the artifacts in question can be models, methods, processes, frameworks, or systems designed to provide solutions to identified problems [21]. The research flow can be seen in Figure 1:

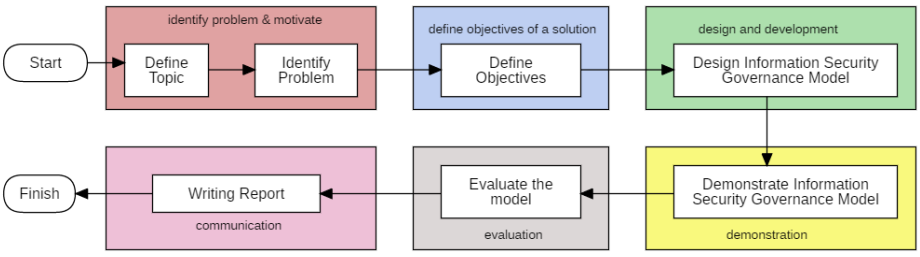


Figure 1. Research Flow

Based on Figure 1, this research begins by defining the topic and identifying issues related to information security in higher education. This stage is carried out through literature studies of scientific articles, news websites, e-books, etc. with the aim of increasing references and understanding of the concept and direction of the research. The next stage is defining the research objectives based on the problems that have been identified. Develop by the International Organization for Standardization (ISO), ISO/IEC 27001:2022 presents an Information System Management Security (ISMS) standard that has 93 information security controls. These 93 controls are divided into four main clauses: Organizational Controls (37 controls), People Controls (8 controls), Physical Controls (14 controls), and Technological Controls (34 controls) [22], [23]. Meanwhile, COBIT 2019, develop by ISACA is an IT governance and management framework that has five main domains: Evaluate, Direct, and Monitor (EDM), Align, Plan and Organize (APO), Build, Acquire and Implement (BAI), Deliver, Service, and Support (DSS), and Monitor, Evaluate, and Assess (MEA) [24]. These five domains include 40 objectives whose structure is as shown in Figure 2 below [25]:

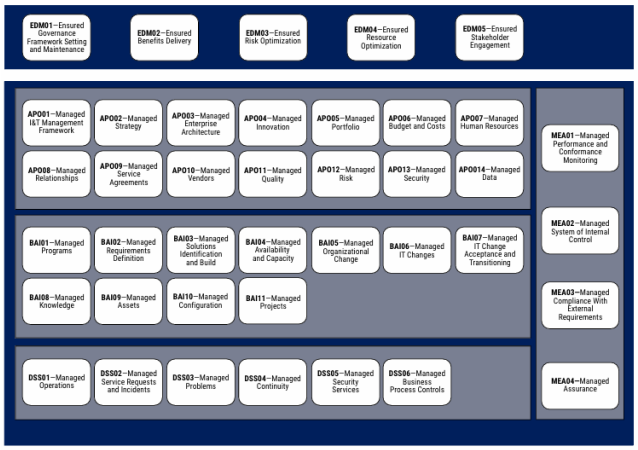


Figure 2. COBIT 2019 Structure

The next stage is to design an information security governance model by mapping the 93 ISO/IEC 27001:2022 controls to the 40 COBIT 2019 objectives. The mapping process is conducted using three alignment criteria; (1) control objective alignment, where the 93 ISO/IEC 27001:2022 controls are matched to the 40 COBIT 2019 objectives that pursue similar security or governance outcomes; (2) governance and management function alignment, ensuring that operational security controls from ISO/IEC 27001:2022 are linked to relevant strategic or management objectives from COBIT 2019; (3) risk domain consistency, where ISO/IEC 27001:2022 controls that address similar risk categories (e.g., access risks, operational risks, compliance risks) are mapped to the corresponding COBIT 2019 risk-related objectives. The goal is to ensure that every technical aspect of information security management from ISO/IEC 27001:2022 can be connected to the strategic governance aspects of COBIT 2019. The results of the mapping process are then visualized so that they function as a basis for determining the objectives for which capability measurements will be carried out. This mapping aligns with research conducted by Anoruo (2025), which asserts that ISO/IEC 27001:2022 and COBIT 2019 are not interchangeable, but rather complementary. ISO/IEC 27001:2022 serves as an information security control framework, while COBIT 2019 provides a governance and management structure to ensure these controls align with organizational objectives [26]. Therefore, the mapping in this study is positioned as a design decision aimed at building an information security governance model aligned with the higher education context.

The next stage is a demonstration of the previously designed model to see how it works in a real-world context. This stage was conducted at a university in Indonesia, which through observations and interviews, has implemented various information systems to support its operational activities but still faces challenges in comprehensive information security management. The model demonstration stage began with an analysis of the eleven COBIT 2019 design factors

using the COBIT 2019 Design Toolkit. The COBIT 2019 design factors include eleven factors to understand organizational characteristics, risk profiles, regulatory compliance, IT roles, threat landscapes, and others as can be seen in Figure 3 below [27]:

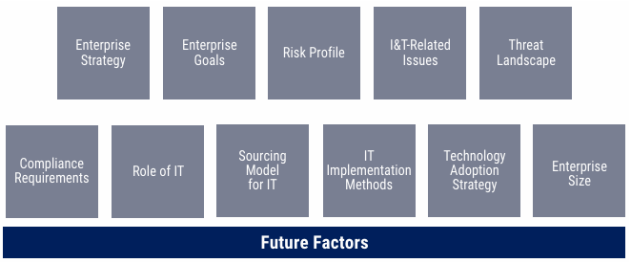


Figure 3. Design factors COBIT 2019

The results of the 11 design factors analysis were then used to determine the expected capability level. The criteria for determining the expected capability level can be seen in Table 1 [28]:

Table 1. Criteria for the Expected Capability Level

Design factors Score	Expected Capability Level Criteria
≥75%	4
≥50% to <75%	3
≥25% to <50%	2

Next, priority objectives were selected to measure the current level of capability. This study selected objectives that emerged from the mapping of ISO/IEC 27001:2022 with COBIT 2019, and were at levels 3 and 4 of expected capability. Because these objectives have a higher expected capability level value, their capabilities were considered more urgent to be measured. The measurement of the current level of capability uses the CMMI (Capability and Maturity Model Integration) COBIT 2019 model, the characteristics of each level of which can be seen in Figure 4 below [25]:

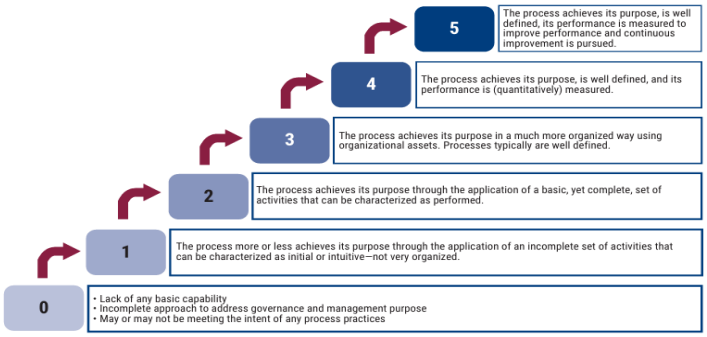


Figure 4. Capability and Maturity Model Integration

In the context of COBIT 2019, current capability measurement starts from level 2 to level 5, as there are no activities at levels 0 and 1 [29], [30].

The way to measure current capability is by assessing COBIT 2019 activities using the N-P-L-F (Not, Partially, Largely, Fully) assessment scale and has been adjusted to COBIT Performance Management (CPM) [31]. It should be noted that the N–P–L–F categories represent ordinal assessment levels, because COBIT 2019 does not specify a standard numerical value for each category (N-P-L-F) [24]. To support quantitative aggregation and percentage-based calculation, this study applied a simple linear normalization approach by assigning values within a 0 to 1 range (N = 0, P = 0.33, L = 0.66, F = 1). This conversion was used as a practical measurement simplification to facilitate internal analysis and comparison of results. The approach does not claim empirically equal distances between categories but serves as a structured

quantification mechanism. The concept of normalization in capability measurement has been carried out by Sormin (2023) [32].

The measurement results are then categorized into assessment standards which can be seen in Table 2 [33]:

Table 2. Current Capability Level Criteria

Measurement Score	Category
85% - 100%	*Fully Achieved* (F)
>50% - 85%	*Largely Achieved* (L)
>15% - 50%	*Partially Achieved* (P)
0 – 15%	*Not Achieved* (N)

The measurement process is stopped if the capability value obtained does not meet the Fully (F) assessment standard [34]. Once the current capability level is known, a GAP analysis is then carried out on the current condition and the expected condition, using equation (1) [35]:

$$GAP = Expected\ Capability - Curent\ Capability \quad (1)$$

The results of the GAP analysis can then serve as the basis for developing strategic recommendations for improving information security governance. These recommendations are based on COBIT 2019 activities that have not yet been implemented and relevant ISO/IEC 27001:2022 controls, based on the mapping of ISO/IEC 27001:2022 to COBIT 2019.

The next stage is evaluating the developed model and testing its application in a real-world context, producing accurate capability measurements, providing a clear GAP analysis, and generating relevant recommendations. The final stage is Communication, which involves delivering research results in the form of a thesis report and scientific publication. This aims to ensure that it can be utilized effectively by other parties, especially universities, as a reference in implementing information security governance.

3. RESULTS AND DISCUSSION

The design of the information security governance model in this study was conducted through a process of mapping 93 ISO/IEC 27001:2022 controls to 40 COBIT 2019 objectives. The mapping was conducted through a conceptual analysis of the alignment of objectives and control functions between each ISO/IEC 27001:2022 control and the COBIT 2019 objectives. Each ISO/IEC 27001:2022 control was analyzed based on its security objectives, such as access control, information asset management, security risk management, incident handling, service continuity, and regulatory compliance. Furthermore, the COBIT 2019 objectives were reviewed based on their objective statements, management practices, and activities that represent the IT governance and management functions within the organization.

Based on the explanation that has been explained in the methodology section, this mapping process is carried out using three criteria, control objective alignment, governance and management function alignment, and risk domain consistency. For example, A.5.7 (Threat Intelligence) concerns risk detection activities, making it suitable for integration with APO12 (Managed Risk), which addresses risk management through risk identification, risk analysis, risk treatment, and risk monitoring. Another example, A.6.3 (Information Security Awareness, Education, and Training), which addresses information security training for academics, is suitable for mapping to APO07 (Managed Human Resources), which also manages competencies, role structures, and IT human resource training. Another example, A.8.9 (Configuration Management), is suitable for mapping to BAI10 (Managed Configuration) because they share the same objectives related to configuration management (servers, routers, campus applications, and others). This approach allows every aspect of ISO/IEC 27001:2022 information security controls to be linked to the relevant governance and management functions in COBIT 2019.

The mapping used in this study aligns with the conceptual foundation presented by Anoruo (2025), who asserted that the integration of ISO/IEC 27001:2022 and COBIT 2019 can be achieved by linking operational information security controls with COBIT's strategic governance and management objectives [26]. Although the study does not present a detailed control mapping, the

article provides academic justification that mapping based on purpose and function alignment is a valid approach for integrating the two frameworks.

The results of the mapping process are then visualized in the form of a mapping diagram of ISO/IEC 27001:2022 controls to COBIT 2019 objectives as shown in Figure 5. This visualization illustrates the distribution of ISO/IEC 27001:2022 controls in each COBIT 2019 domain, namely EDM, APO, BAI, DSS, and MEA. The results of this mapping are then used as a basis for determining the COBIT 2019 objectives that are prioritized for measuring capability level in the next stage of this research:

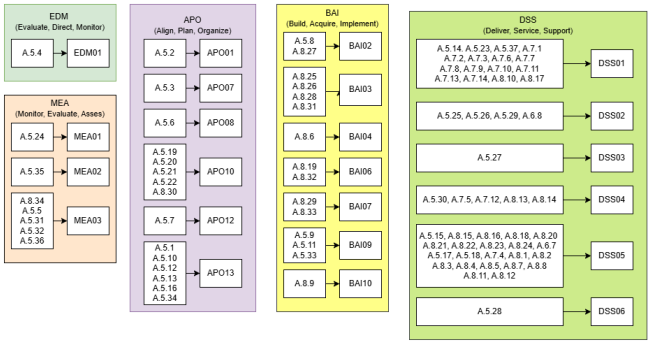


Figure 5. Mapping ISO/IEC 27001:2022 Controls to COBIT 2019 Objectives

Based on Figure 5, a model test was then carried out at one of the higher education institutions in Indonesia, which began with an analysis using 11 COBIT 2019 design factors. The design factors scoring was conducted through structured interviews and observation with the Director of Infrastructure and Digitalization (Head of IT). The scoring of the eleven COBIT 2019 design factors was performed collaboratively during interview sessions and was supported by internal institutional documents, such as strategic IT plans, organizational structure documents, security policies, operational procedures, and related governance records. Figure 6 below shows the results of the analysis of 11 COBIT 2019 design factors:

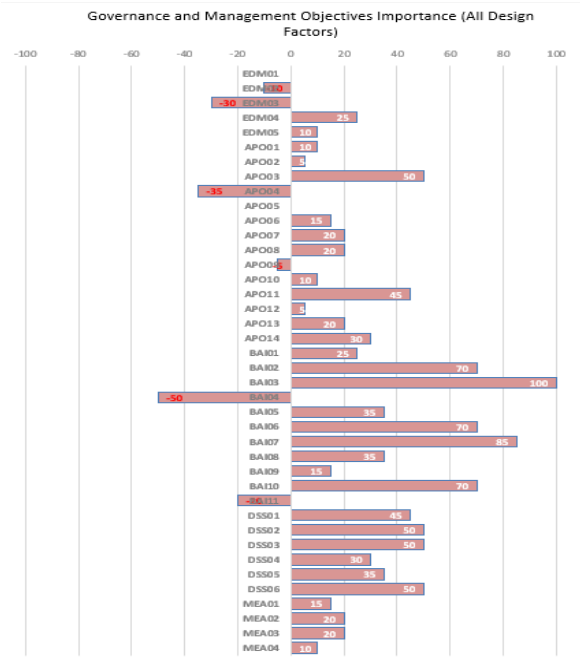


Figure 6. Design factors COBIT 2019

Based on Figure 6, this study takes objectives that have a value of ≥75% and objectives that have a value of ≥50% to 75% to calculate their capabilities. Based on Table 1, objectives that

have a value of ≥75% are at level 4 of expected capabilities, these objectives include, BAI03 and BAI07. Meanwhile, objectives that have a value of ≥50% to 75% are at level 3 of expected capabilities, these objectives include APO03, BAI02, BAI06, BAI10, DSS02, DSS03, DSS06. APO03 was excluded from the capability assessment because no ISO/IEC 27001:2022 controls were mapped to this objective in the proposed model. Therefore, capability measurement was performed only on objectives that were both prioritized by the COBIT 2019 Design Factors and associated with mapped ISO/IEC 27001:2022 controls. The selection of these objectives is the result of mapping ISO/IEC 27001:2022 to COBIT 2019. In addition, the expected capability value indicates the priority of the organization's needs, the higher the value, the more urgent the process needs to be improved so that it is worthy of being the focus of the evaluation. The selected objectives are then measured for capability in the current condition using the CMMI model and an assessment method based on the N-P-L-F model, resulting in a measurement of the current capability level which can be seen in Table 3 below:

Table 3. Current Capability Measurement Results at Level 2

Objectives COBIT 2019	Total Activity at Level 2	Current Capability Level	Scale
BAI02	5	38.50%	*Partially Achieved*
BAI03	26	59.69%	*Largely Achieved*
BAI06	9	51.33%	*Largely Achieved*
BAI07	26	52.04%	*Largely Achieved*
BAI10	7	56.57%	*Largely Achieved*
DSS02	15	37.40%	*Partially Achieved*
DSS03	9	62.56%	*Largely Achieved*
DSS06	14	54.21%	*Largely Achieved*

Based on Table 3, no objectives reached the Fully Achieved scale. According to COBIT 2019 Performance Management guidelines, the assessment of higher capability level can only be conducted when all attributes of the previous level are Fully Achieved [30]. Therefore, because none of the evaluated objectives reached the Fully Achieved category at Capability Level 2, the assessment was not extended to the next Capability Level. This condition indicates that the current capability measurement process stops at level 2. The capability assessment results indicate that the evaluated objectives remain at Capability Level 2, suggesting that information security governance processes have been implemented but are not yet consistently documented and managed. This finding is consistent with the study by Sikman et al. (2023), which reported that higher education institutions often face challenges in formalizing information security governance despite increasing reliance on digital systems and services [7]. These results highlight the importance of establishing structured governance mechanisms to ensure that information security practices are implemented consistently across the institution. The measurement results are then compared with the expected capability level, resulting in the GAP values, which are presented in Table 4 below:

Table 4. Capability Level GAP

Objectives COBIT 2019	Expected Capability Level (EC)	Current Capability Level (CC)	GAP (EC – CC)
BAI02	3	2	1
BAI03	4	2	2
BAI06	3	2	1
BAI07	4	2	2
BAI10	3	2	1
DSS02	3	2	1
DSS03	3	2	1
DSS06	3	2	1

Table 4 shows that all selected objectives have not yet met the expected maturity level, requiring improvement through governance recommendations oriented toward information security processes. Based on the GAP results, to enhance practical implementation, the proposed recommendations are further categorized based on activities within each objective, priority level, and estimated timeline. Table 5 presents improvement recommendations categorized by priority level and estimated implementation timeline:

Table 5. Recommendations for Improvement

Objectives COBIT 2019	Problem Findings	Relevant ISO/IEC 27001:2022 Controls	Recommendations for Improvement	Priority Levels	Estimated Timeline
BAI02	There is no formal mechanism for capturing, prioritizing, and documenting information security requirements in IT projects.	A.5.8, A.8.27	Create a security requirements document template for every IT project, require security risk analysis early in the project (security-by-design), and involve the IT security unit in the requirements definition process.	High	3-6 months
BAI03	Secure development standards are not documented, and there are no consistent secure coding and security practices.	A.8.25, A.8.26, A.8.28, A.8.31	Develop Secure Development Guidelines, require code reviews and static application security testing (SAST) for each application development phase, and formally separate dev, test, and prod environments.	High	6-12 months
BAI06	Change control processes are not clearly documented, and change approvals are not standardized.	A.8.19, A.8.32	Create a Change Management Standard Operating Procedure (SOP) (urgency, approval flow, rollback plan), implement a ticketing system for all change requests, and provide regularly audited change logs.	High	3-6 months
BAI07	Testing, acceptance, and transition to production processes are not consistent.	A.8.29, A.8.33	Create a formal User Acceptance Test (UAT) for every system implementation, standardize test case documentation and test evidence, and conduct pilot testing before major implementations.	Medium	1-3 months
BAI10	IT asset configurations are not systematically documented and monitored.	A.8.9	Implement a simple Configuration Management Database (CMDB), establish security configuration baselines for servers, networks, and endpoints, and audit configurations at least semiannually.	Medium	6-12 months
DSS02	Not all incidents are recorded, and incident reporting, classification, and handling processes are not standardized.	A.5.25, A.5.26, A.5.29, A.6.8	Establish an incident handling workflow that includes reporting → classification → response → recovery. Create a single incident reporting channel. Train staff and faculty on reporting cyber incidents.	High	3-6 months
DSS03	There is no formal process for problem management and root cause analysis.	A.5.27	Create a Problem Register that includes recurring incidents. Apply the "5 Whys" or fishbone method for RCA. Ensure that each problem results in a preventative action.	Medium	1-3 months
DSS06	Business process controls are not fully documented (transaction authorization, segregation of duties, and evidence of activity).	A.5.28	Document key process controls (student registration, finance, personnel), ensure secure storage of digital transaction evidence, and implement acceptable use and security awareness training.	Medium	3-6 months

Furthermore, several fundamental cross-domain issues were identified that impact the overall effectiveness of information security governance. First, most activities across various domains are ongoing, but not yet fully supported by formally and consistently documented policies and procedures. Many activities fall into the "Partially" and "Largely Achieved" categories, indicating practices that are being implemented but lack standardized processes. Therefore, it is necessary to develop an IT Governance Handbook containing comprehensive information security SOPs, including SOPs for IT incidents, change management, asset management, cloud utilization, system development procedures, and backup, along with a mechanism for regular review and updating.

Second, there is a lack of a structured information security risk management framework. This is reflected in objectives such as BAI06, DSS02, and BAI02, which received relatively low scores. Therefore, it is necessary to develop an ISO/IEC 27001-based IT risk management framework, including the development of a risk register and the implementation of periodic risk assessments to ensure that information security risks are effectively identified, assessed, and mitigated.

Third, the competency aspect of Human Resources (HR) is also a critical issue. Low scores on objectives such as DSS06 indicate that IT and administrative staff need to improve their understanding of information security, segregation of duties, and operational procedures. Therefore, it is necessary to implement human resource capacity development programs through mandatory information security training and encourage professional certifications such as ISO/IEC 27001, COBIT 2019 Foundation, or CompTIA Security+. These efforts are expected to ensure that information security processes are carried out by competent personnel who understand governance standards. These recommendations can be used to assist higher education institutions in achieving the desired level of capability and meeting information security governance requirements based on COBIT 2019 and ISO/IEC 27001:2022.

The improvement recommendations generated by the proposed model emphasize the importance of documented governance processes, systematic risk management practices, and information security competency development. These findings are consistent with previous studies by Gunawan et al. (2020) and Yasin et al. (2020), which highlighted that the integration of COBIT and ISO/IEC 27001 can strengthen information security governance by combining operational security controls with governance mechanisms for monitoring and continuous improvement [17], [19]. Therefore, the results of this study further support the view that integrating ISO/IEC 27001:2022 and COBIT 2019 can assist higher education institutions in addressing governance capability gaps while maintaining alignment between security controls and organizational objectives.

Model evaluation is conducted after the model is implemented and tested on a case study of a higher education institution. This evaluation is based on the results of direct model testing through mapping, factor design determination, capability measurement, and GAP analysis. In addition, the evaluation results and improvement recommendations were presented to the Directorate of Infrastructure and Digitalization, which serves as the institutional authority responsible for IT governance. The director provided confirmation that the proposed model and recommendations were aligned with the institution's governance structure and operational conditions. This confirmation served as contextual validation of the model's applicability. Model evaluation is conducted by considering various aspects, as presented in Table 6 below:

Table 6. Model Evaluation Analysis

No	Evaluation Aspects	Description
1	Compliance with ISO/IEC 27001:2022 and COBIT 2019 Integration	The developed model is able to systematically integrate ISO/IEC 27001:2022 controls into COBIT 2019 objectives. Mapping results indicate that information security controls can be linked to relevant IT governance and management processes.
2	Model's Ability to Prioritize Objectives	The results of the COBIT 2019 factor design analysis indicate that the model can identify objectives with a higher expected capability level, making them worthy of being the focus of measurement and evaluation.
3	Model's Ability to Describe Actual Conditions	Measurement of the capability level of selected objectives indicates the current state of information security governance. The measurement results show that most objectives remain at capability level 2, indicating that processes have been implemented but are inconsistent and poorly documented.
4	Model's Ability to Identify GAP (between current capability and expected capability)	A gap analysis between the expected capability level and the current capability level revealed discrepancies across all tested objectives. These gap results provide a clear picture of areas requiring improvement.
5	Feasibility of Improvement Recommendations	Recommendations were developed based on unmet COBIT 2019 activities and relevant ISO/IEC 27001:2022 controls. The resulting recommendations were submitted to the case study site and were deemed relevant, operational, and applicable to the existing conditions.

After evaluation, this study indicates that the developed information security governance model is applicable within the context of the studied institution. Based on the results of the case study implementation, the proposed model is particularly suitable for higher education institutions that have implemented information systems to support academic and administrative processes, possess an IT management function or unit, and are actively seeking to improve their information security governance. Under these conditions, the integration of ISO/IEC 27001:2022 and COBIT 2019 can provide a structured approach for identifying capability gaps and formulating improvement strategies.

However, this study was conducted in a single higher education institution, which may limit the generalizability of the findings. Universities with different organizational sizes, governance maturity levels, IT outsourcing arrangements, and structural complexity may obtain different capability outcomes when implementing the proposed model. Furthermore, the evaluation relied on practitioner confirmation within the institution and did not involve independent expert validation or inter-rater reliability testing. Future research may strengthen validation by involving multiple assessors or applying the model in different institutional contexts.

4. CONCLUSION

This research demonstrates that the integration of ISO/IEC 27001:2022 and COBIT 2019 can provide an effective approach for designing information security governance in higher education. The proposed model maps information security controls to governance and management objectives and supports capability evaluation through the COBIT 2019 process structure. Testing at a higher education institution showed that all eight priority objectives remained at Capability Level 2, indicating that governance practices have been implemented but are not yet consistently documented and supported by formal risk management mechanisms. The results suggest the need for improvements in governance documentation, information security risk management, and human resource competencies. The proposed model can serve as a practical reference for higher education institutions seeking to strengthen their information security governance capabilities.

Future research may incorporate quantitative risk analysis, involve multiple assessors across different universities, and develop automated tools to support capability assessment. In addition, the model may be extended to support AI governance and integrated with other frameworks, such as NIST CSF or ITIL 4, to provide a broader information security governance perspective.

ACKNOWLEDGEMENTS

The authors would like to thank all parties who contributed to this research through their support, insights, and assistance during the study.

CONFLICT OF INTEREST

The authors declare that there are no conflicts of interest regarding the publication of this paper.

DATA AVAILABILITY

The data used in this study are not publicly available due to confidentiality considerations. Data may be available from the corresponding author upon reasonable request and subject to institutional approval.

AUTHOR CONTRIBUTIONS

Neonatal March Parera: Conceptualization; Methodology; Investigation; Data Curation; Visualization; Writing – Original Draft. **Wiwin Sulistyo**: Methodology; Validation; Supervision; Writing – Review & Editing. **Johan Jimmy Carter Tambotoh**: Investigation; Resources; Validation; Supervision; Writing – Review & Editing.

REFERENCES

[1] "Higher Education Has A Lot To Learn About Data Breaches." Accessed: Dec. 01, 2025. [Online]. Available: https://www.forbes.com/sites/steveweisman/2025/08/23/higher-education-has-a-lot-to-learn-about-data-breaches/

[2] J. Li, W. Xiao, and C. Zhang, "Data security crisis in universities: identification of key factors affecting data breach incidents," *Humanit. Soc. Sci. Commun.*, vol. 10, no. 1, p. 270, Dec. 2023, doi: 10.1057/S41599-023-01757-0.

[3] "BUKU STATISTIK PENDIDIKAN TINGGI 2024 - PUSDATIN KEMDIKTISAINTEK.pdf - Google Drive." Accessed: Nov. 09, 2025. [Online]. Available: https://drive.google.com/file/d/1RcIDvDRs1VNcNAvPCOHeBxBzY3NgXizN/view

[4] D. L. Putri and I. E. Pratiwi, "Ramai soal Data Universitas Indonesia Dilaporkan Bocor, Ini Kata Kampus," Kumparan.com. Accessed: Mar. 18, 2025. [Online]. Available: https://www.kompas.com/tren/read/2024/07/19/163000865/ramai-soal-data-universitas-indonesia-dilaporkan-bocor-ini-kata-kampus

[5] D. Setya, "Data Mahasiswa UPI Diduga Bocor, Apa Langkah Pihak Kampus?," detikEdu. Accessed: Mar. 18, 2025. [Online]. Available: https://www.detik.com/edu/perguruan-tinggi/d-6247009/data-mahasiswa-upi-diduga-bocor-apa-langkah-pihak-kampus

[6] A. Evandio, "Data 125.000 Mahasiswa Undip Bocor! Begini Seharusnya," Bisnis.com. Accessed: Mar. 18, 2025. [Online]. Available: https://teknologi.bisnis.com/read/20210106/84/1339353/data-125000-mahasiswa-undip-bocor-begini-seharusnya

[7] L. Sikman, T. Latinovic, N. Sarajlic, and G. Sikanjic, "A model of sustainable information security management system in higher education institutions," *J. Phys. Conf. Ser.*, vol. 2540, no. 1, 2023, doi: 10.1088/1742-6596/2540/1/012003.

[8] P. P. Roy, "A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard," *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications, NCETSTEA 2020*, Feb. 2020, doi: 10.1109/NCETSTEA48365.2020.9119914.

[9] M. B. Pohlman, "Compliance Frameworks," *Oracle Identity Management*, pp. 55–70, Dec. 2020, doi: 10.1201/9781420072488-9/COMPLIANCE-FRAMEWORKS-MARLIN-POHLMAN.

[10] A. Alexei, "CYBER SECURITY STRATEGIES FOR HIGHER EDUCATION INSTITUTIONS ," *Journal of Engineering Science*, vol. XXVIII, no. 4, pp. 74–92, 2021, doi: 10.52326/jes.utm.2021.28(4).07.

[11] N. Mohd Nordin, A. Mat Isa, A. Z. H. Samsudin, and A. R. Ahmad, "Information Governance for Enhancing the Performance of Higher Education Institutions," *Environment-Behaviour Proceedings Journal*, vol. 7, no. SI10, pp. 135–139, Nov. 2022, doi: 10.21834/EBPJ.V7ISI10.4115.

[12] C. W. Liu, P. Huang, and H. C. Lucas, "Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions," *Journal of Management Information Systems*, vol. 37, no. 3, pp. 758–787, Jul. 2020, doi: 10.1080/07421222.2020.1790190.

[13] Doç. Dr. A. EFE, "A Comparison of Key Risk Management Frameworks: COSO-ERM, NIST RMF, ISO 31.000, COBIT," *Denetim ve Güvence Hizmetleri Dergisi*, Jan. 2023, Accessed: Mar. 18, 2025. [Online]. Available: https://www.academia.edu/105144901/A_Comparison_of_Key_Risk_Management_Frameworks_COSO_ERM_NIST_RMF_ISO_31_000_COBIT

[14] T. R. McIntosh *et al.*, "From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models," *Comput. Secur.*, vol. 144, p. 103964, Sep. 2024, doi: 10.1016/J.COSE.2024.103964.

[15] H. Setiawan, N. A. Hana, and R. R. Hanaputra, "Mapping ISO 27001:2013 and COBIT 2019 Framework to STRIDE Threat Modeling Using Qualitative Descriptive Research," *Journal of Computer Engineering, Electronics and Information Technology*, vol. 3, no. 2, pp. 101–110, Nov. 2024, doi: 10.17509/COELITE.V3I2.73228.

[16] S. U. Adamu, M. A. Ahmad, and M. Ibrahim, "A systematic literature review on the adoption and effectiveness of cybersecurity frameworks in higher education institutions," *Information and Computer Security*, pp. 1–16, 2025, doi: 10.1108/ICS-10-2025-0403/1339707.

[17] N. K. Gunawan, R. B. Hadiprakoso, and H. Kabetta, "Comparative study between the integration of ITIL and ISO / IEC 27001 with the integration of COBIT and ISO / IEC 27001," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 852, no. 1, Jul. 2020, doi: 10.1088/1757-899X/852/1/012128.

[18] E. Aflakhah and B. Soewito, "Assessing Information Security using COBIT 2019 and ISO 27001:2013 for Developing a Mitigation Plan," *International Journal of Engineering Trends and Technology*, vol. 71, no. 10, pp. 223–237, 2023, doi: 10.14445/22315381/IJETT-V71I10P221.

[19] M. Yasin, A. Akhmad Arman, I. J. M. Edward, and W. Shalannanda, "Designing information security governance recommendations and roadmap using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimsus Polda XYZ)," *Proceeding of 14th International Conference on Telecommunication Systems, Services, and Applications, TSSA 2020*, Nov. 2020, doi: 10.1109/TSSA51342.2020.9310875.

[20] M. Gandhi, A. Gaur, A. Kumar Kar, and Y. K. Dwivedi, "Crafting user experiences in the metaverse: A design science study," 2024, doi: 10.1016/j.techfore.2024.123759.

[21] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, Dec. 2007, doi: 10.2753/MIS0742-1222240302.

[22] S. Nasional Indonesia, "SNI ISO/IEC 27001:2022 (Ditetapkan oleh BSN tahun 2023)," 2023. [Online]. Available: www.bsn.go.id

[23] P. Nurmi, "Enhancing ISO 27001:2022 Implementation Through Project Management," 2024.

[24] N. Andriani, R. Mulyana, and Rd. R. Saedudin, "Ambidextrous Cloud Governance Approach to Enhance TelCo's Digital Transformation Using COBIT 2019 Traditional and DevOps," *International Journal of Advances in Data and Information Systems*, vol. 6, no. 2, pp. 357~375-357~375, Jul. 2025, doi: 10.59395/ijadis.v6i2.1398.

[25] ISACA, *COBIT 2019 Framework Governance and Management Objectives*.

[26] C. C. Anoruo, "The Governance Game of Chess: Mapping ISO/IEC 27001:2022 to COBIT ®," *ISACA Journal*, vol. 2, Apr. 2025, [Online]. Available: www.isaca.org

[27] S. De Haes, W. Van Grembergen, A. Joshi, and T. Huygh, "Enterprise Governance of Information Technology," in *Management for Professionals (MANAGPROF)*, in Management for Professionals. , Cham: Springer International Publishing, 2020. doi: 10.1007/978-3-030-25918-1.

[28] N. M. Parera and J. J. C. Tambotoh, "Measuring IT Governance Capability at DISKOMINFO Salatiga using COBIT 2019," *Sistemasi: Jurnal Sistem Informasi*, vol. 13, no. 1, pp. 324–334, Jan. 2024, doi: 10.32520/stmsi.v13i1.3669.

[29] L. Gorgona, "Building a Maturity Model for COBIT 2019 Based on CMMI," 2021. [Online]. Available: https://www.isaca.org/resources/cobit

[30] P. Widharto, Z. Suhatman, and R. F. Aji, "Measurement of information technology governance capability level: a case study of PT Bank BBS," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 20, no. 2, pp. 296–306, 2022, doi: 10.12928/TELKOMNIKA.v20i2.21668.

[31] ISACA, *COBIT® 2019 Framework : introduction and methodology*.

[32] F. N. Sormin, "Analisis Tingkat Kemampuan (Capability Level) Teknologi Informasi Pada Pt.Pos (Persero) Indonesia Cabang Perdagangan Menggunakan Framework Cobit 5 Domain Apo (Align, Plan, And Organise)," *SISFO : Jurnal Ilmiah Sistem Informasi*, vol. 7, no. 1, 2023.

[33] ISACA, *COBIT 2019 Design guide designing an information and technology governance solution*.

[34] A. Safitri, I. Syafii, and K. Adi, "Identifikasi Level Pengelolaan Tata Kelola SIPERUMKIM Kota Salatiga berdasarkan COBIT 2019," *Jurnal RESTI*, vol. 5, no. 3, pp. 429–438, Jun. 2021, doi: 10.29207/RESTI.V5I3.3060.

[35] Rahmat Rian Hidayat and D. Jatikusumo, "IMPLEMENTATION OF COBIT 2019 TO MEASURE IT MATURITY LEVELS IN DIGITAL BANKS," *Jurnal Teknik Informatika (Jutif)*, vol. 5, no. 4, pp. 497–504, Aug. 2024, doi: 10.52436/1.jutif.2024.5.4.2135.