Evaluation Of Information Technology Security System Using Cobit 5 Framework
(A Study At Unit Sumber Daya Informasi Udayana University)

I Made Agung Pranata[1], Dewa Made Wiharta[1], Komang Oka Saputra[1]

[1]Department of Electrical Engineering
Faculty of Engineering, Udayana University
Bali, Indonesia
agungpranata27@gmail.com

Abstract This study aims to evaluate the information technology security system at the Unit Sumber Daya Informasi (USDI) of Udayana University using the COBIT 5 framework, focusing on the APO (Align, Plan, and Organize) and DSS (Deliver, Service, and Support) domains. The use of information technology at Udayana University is crucial to support both academic and non-academic activities, making information management and security a priority. The COBIT 5 framework is used to assess IT management capabilities and identify gaps between the current and expected conditions. The research methods include questionnaires, interviews, and observations with unit leaders and staff at USDI. The evaluation results show that the APO 13 (Manage Security) and DSS 05 (Manage Security Service) subdomains have reached level 3 (established process), which means these processes have been well implemented. However, there is potential for improvement to level 4 (predictable process). This study provides recommendations to improve information security management, including establishing of an information security division, enhancing human resource competencies, preparing SOPs, and conducting regular internal monitoring and audits. With these improvements, it is expected that USDI Udayana University can optimally manage and protect the IT system, supporting institutional goals more safely and efficiently.

Keywords: Information Security, COBIT 5, IT System Evaluation, IT Governance

I. INTRODUCTION

Information technology has been applied in almost all sectors, including educational institutions. Information technology plays a crucial role in enhancing the effectiveness and efficiency of various activities within organizations and businesses. Educational institutions, whose main purpose is to offer education and academic services, leverage information technology to support and improve these functions. Thus, information technology plays an essential role in achieving optimal educational goals and academic services [1].

Udayana University has implemented Information Technology (IT) to support academic and non-academic activities. The application of IT at this university is managed by Unit Sumber Daya Informasi (USDI). Information security is an important concern for Udayana University, especially for the Information Resource Unit, which has implemented an IT system. As the number of systems used increases, the data stored, including confidential information, needs to be protected. Information security is not only carried out technically but also needs to be measured from the perspective of the information security management applied by the institution.

COBIT (Control Objectives For Information and Related Technology) is one of the tools used to measure the security of information technology systems. The COBIT Framework serves as a governance guide for IT to identify gaps between needs and the implementation of fulfilling those needs within an organization. COBIT is highly effective in IT control to improve the quality and value of an organization or institution in terms of IT implementation.

Information security is the effort to protect information from unauthorized access. There are three main aspects of information security: confidentiality, integrity, and availability. In addition, information security management is also necessary to manage security from a managerial perspective, to reduce the impact of undesirable incidents and protect information assets from threats.

This study focuses on two COBIT 5 domains, namely DSS (Deliver, Service, and Support) and APO (Align, Plan, and Organize). The DSS domain relates to service delivery, security and continuity management, as well as support for users and management of operational facilities. Meanwhile, the APO domain covers strategies, tactics, and best practices in IT to support the achievement of business goals.

This study aims to evaluate the IT security system at the Unit Sumber Daya Informasi (USDI) of Udayana University and identify necessary improvements. The COBIT 5 framework, focusing on the APO and DSS domains, is used to enhance the effectiveness of the institution's security. The main objective of this study is to develop a security strategy that involves technical processes, controls, and tools to support security across the institution, as well as provide recommendations for the Unit Sumber Daya Informasi (USDI) of Udayana University.

II. RESEARCH DESIGN

A. IT Governance

IT governance is a responsibility shared by leadership and the board of directors. It encompasses leadership, organizational structure, and processes that ensure IT aligns with and advances the organization's goals and strategies. The organization must fulfill standards for information quality, security, and reliability, while maximizing the use of available IT resources such as applications, information, infrastructure, and personnel. Additionally, management must have a clear understanding of the company's IT architecture to establish the necessary governance and controls [2].

IT governance is the responsibility of leadership and executive management to align and enhance the company's strategies and objectives. Management must assess the company's situation to establish the right IT governance. The primary objective of IT governance is to ensure that business processes are aligned with information technology, making certain that IT investments and implementations support the organization's business strategy[3].

B. COBIT Framework

COBIT, which stands for Control Objectives for Information and Related Technology, is an information systems audit framework and control foundation developed by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) in 1992. It includes[4].

1. Business information requirements, which consist of Information effectiveness, efficiency, confidence, integrity, availability, fulfillment, reliability.
2. Confidentiality compliance.
3. Information Technology Resources, which consist of People, applications, technology, facilities, and data.
4. High-level IT processes.

COBIT emphasizes the objectives of IT management, driven by business needs, and encompasses all IT activities. It serves as an integrator of essential IT governance practices for management, governance specialists, insurance, security, and IT auditors. Designed to align with other standards and best practices, COBIT ensures that the implementation of best practices is consistent with the organization's existing governance and controls, as well as integrated with other methods in [5].

The core principle of the COBIT framework is to provide the essential information needed to achieve the goals of higher education institutions. These institutions must manage and control IT resources by implementing the appropriate processes to deliver the necessary information. Information technology, which supports the activities of higher education institutions, is a valuable asset. Successful institutions typically recognize the benefits of IT in enhancing their performance.

IT risk management and control are now considered key elements in the good governance of higher education (IT governance). IT governance involves the structure and processes to guide the institution in achieving its goals while balancing IT risks and benefits. It also integrates best practices to ensure that IT supports the institution's business objectives. With IT governance, higher education institutions can maximize the benefits of IT to gain a competitive advantage. Therefore, a framework such as COBIT (version 4.1) is needed to support IT risk management and governance in line with the COSO Internal Control-Integrated Framework [4].

COBIT 5 has five main domains, which can be seen in Figure 1, covering various aspects of IT governance:

1. Evaluate, Direct, and Monitor (EDM): Focuses on stakeholder management and monitoring results. It consists of 5 subdomains, such as ensuring benefit delivery, risk optimization, and stakeholder transparency.
2. Align, Plan, and Organize (APO): It offers guidance for IT strategies and tactics to accomplish business objectives. The framework includes 13 subdomains, such as strategy management, enterprise architecture, and risk management.
3. Build, Acquire, and Implement (BAI): Identifies, develops, and implements IT solutions to support IT strategies. It consists of 10 subdomains, including project management, change management, and asset management.
4. Deliver, Service, and Support (DSS): It pertains to the delivery and support of IT services for end users. This area includes 6 subdomains, such as operations management, user services, and continuity and security management.
5. Monitor, Evaluate, and Assess (MEA): It oversees and assesses processes to ensure quality, compliance, and internal control. This area includes 3 subdomains, such as performance assessment, internal control, and adherence to external regulations.

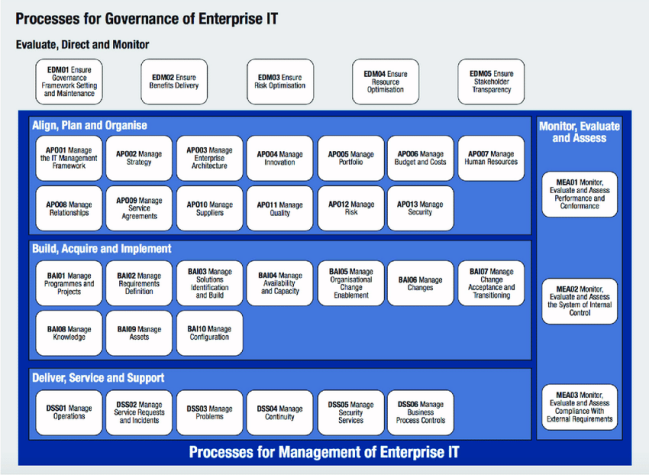

Fig. 1. Reference model process

The COBIT 5 assessment process is grounded in ISO/IEC 15504, highlighting the framework's alignment with widely recognized standards and best practices. The COBIT 5 Process Capability Model consists of six levels, as illustrated in Figure 2, which are as follows:

Level 0: Incomplete process. At this level, the process is either not defined or incapable of meeting its objectives. There are no objectives set for the process, which is why this level lacks any attributes.

Level 1: Performed process. The process is established and successfully meets its objectives. At this level, the only process attribute is "Process Performance".

Level 2: Managed process. The process is carried out through a sequence of activities, including planning, monitoring, and making adjustments. The outcomes are defined, controlled, and sustained. At this level, the process attributes are "Performance Management" and "Work Product Management".

Level 3: Established process. The previous level is now executed using a defined process that ensures the achievement of the desired results. At this level, the process attributes are "Process Definition" and "Process Deployment".

Level 4: Predictable process. At this level, the process is applied within set boundaries that ensure the desired results are achieved. The process attributes at this level are "Process Management" and "Process Control".

Level 5: Optimizing process. At this level, the process is applied in a manner that supports the achievement of relevant, current, and future business goals. The process attributes at this level are "Process Innovation" and "Process Optimization".

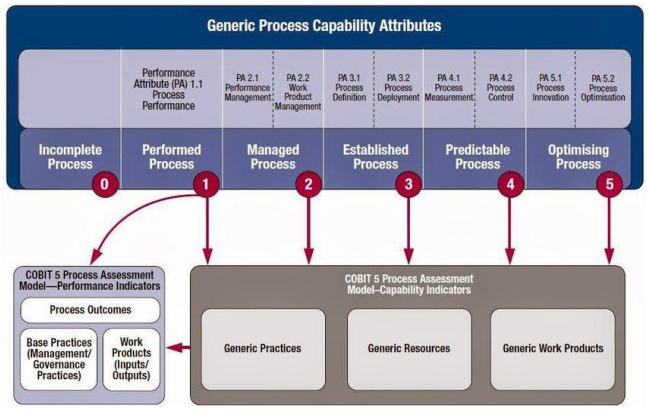

Fig. 2. COBIT 5 process capability model

II. RESEARCH METHOD

The research will be conducted at the Unit Sumber Daya Informasi (USDI) of Udayana University. The stages involved include literature study, problem definition, and data collection.

A. Data Collection

The COBIT 5 framework provides guidelines for evaluating the performance of information technology usage in an organization. The data collection method in this research uses indicators from the control objectives of relevant COBIT 5 domains, which are then developed as needed. Data collection techniques include field observations, questionnaire distribution, and interviews with the Unit Sumber Daya Informasi (USDI) of Udayana University. The primary data for the research is obtained from questionnaires, interviews, observations, and written documents.

B. Data Collection

The COBIT 5 framework provides guidelines for evaluating the performance of information technology usage in an organization. The data collection method in this research uses indicators from the control objectives of relevant COBIT 5 domains, which are then developed as needed. Data collection techniques include field observations, questionnaire distribution, and interviews with the Unit Sumber Daya Informasi (USDI) of Udayana University. The primary data for the research is obtained from questionnaires, interviews, observations, and written documents.

C. Population and Sample

The population and sample of respondents include the unit leaders and staff from the network administration division at the Unit Sumber Daya Informasi (USDI) of Udayana University. The sample selection is based on respondents who hold positions, authority, and extensive knowledge about the performance and governance of IT security systems in the unit. The sample selection was carried out by mapping respondents using the COBIT 5 RACI chart analysis.

D. Questionnaire

The questionnaire in this study is designed to assess the level of capability in implementing information technology, based on the control objectives outlined in the COBIT 5 framework. The rating scale ranges from level 0 (not implemented) to level 5 (optimal). The questionnaire is distributed to the information system development division and the network division at the Unit Sumber Daya Informasi (USDI) of Udayana University. If a level reaches the Fully Achieved (F) status, the process domain can move up one level, while if it has not reached the F value, its capability level cannot increase.

D. Interview

The interview guidelines in this research are based on the control objectives and capability levels within the COBIT 5 framework.

E. Observation

The observation is conducted by directly monitoring the activities and documents related to IT planning and development within the organization. The researcher also reviews supporting documents to ensure alignment between the questionnaire responses and the actual conditions. The aim is to validate the data and examine the implementation of IT and system security governance at Unit Sumber Daya Informasi (USDI) of Udayana University by the COBIT 5 framework.

III. Result and Discussion

A. RACI Chart Analysis

The determination of respondents is carried out using the RACI calculation, which stands for Responsible, Accountable, Consulted, and Informed. With the RACI chart, the researcher can identify the appropriate respondents to complete the questionnaire based on their respective roles.

TABLE I
LIST OF RESPONDENTS

Number of Respondents	Position	Amount
1	Head of Technology Infrastructure	1 person
2	Information Technology Infrastructure Staff	9 person
3	Programmer staff	11 person
	TOTAL	21 person

Head of Technology Infrastructure, Information Technology Infrastructure Staff, and Programmer staff Unit Sumber Daya Informasi are competent to be respondents in filling out the questionnaire for the APO 13 and DSS 05 process domains. This has been adjusted according to the individual roles within the Unit Sumber Daya Informasi and has received approval from the Unit Sumber Daya Informasi.

B. Capability Level Analysis

From the overall responses of the respondents to each process attribute, the majority of the capability level achievements for the APO 13 (Manage Security) subdomain are at level 3, and for the DSS 05 (Manage Security Service) subdomain, they are also at level 3.

TABLE II
CAPABILITY LEVEL ACHIEVEMENT RESULT

Process	Respondents	*Capability Level*
APO 13	Head of Technology Infrastructure	3
	Information Technology Infrastructure Staff	3
	Programmer staff	3
DSS 05	Head of Technology Infrastructure	3
	Information Technology Infrastructure Staff	3
	Programmer staff	3

The assessment results of the capability level process, based on data gathered from 21 respondents through questionnaires and interviews, indicate that for the APO 13 subdomain, level 3 (established process) has been reached, meaning the implemented processes have met their objectives. Similarly, for the DSS 05 subdomain, level 3 (established process) has also been attained, suggesting that the processes are now well-managed (planned, monitored, and organized), with results being effectively applied, controlled, and maintained.

The capability level results for the APO 13 process are at level 3, which means that the processes and activities have been implemented using defined processes and can achieve the desired process results. The target level that the Unit Sumber Daya Informasi aims to achieve for the APO 13 domain process is level 4, which is a predictable process.

The capability level assessment for the DSS 05 process is at level 3 (established process), indicating that the processes and activities have been implemented using defined procedures and are capable of achieving the intended outcomes. The target level that Unit Sumber Daya Informasi aims to achieve for the DSS 05 process is level 4 (managed process).

TABLE III
CAPABILITY GAP

Domain Process	Existing Capability Level	Target Capability Level	Gap
APO13 Manage Security	3	4	1
DSS05 Manage Security Services	3	4	1

C. Recommendations

Recommendations Based on APO 13:

1. Establishment of an Information Security Division: Create a management or special division to manage information security with a structured, monitored, and organized approach, ensuring that the results are applied effectively and controlled.
2. Human Resource Development: The staff in the Information Resource Unit should receive regular, up-to-date training to improve their competencies, enabling them to perform continuous system maintenance and anticipate emerging cyber threats.
3. Development and Socialization of SOPs: Written Standard Operating Procedures (SOPs) should be developed and socialized to ensure smooth operations, consistency, and quality, and serve as tools for control, documentation, and organizational performance improvement. The existence of clear SOPs will enhance efficiency and reduce risks.
4. Internal Monitoring and Audits**:** Regular internal monitoring and audits should be conducted to detect potential data breaches or violations, whether committed by employees or other internal parties.

Recommendations Based on DSS 05:

1. Sensitive Data Classification Policy: Create a policy for classifying sensitive data, allowing the Information Resource Unit to build appropriate protection systems.
2. Limitation of VLAN Usage: Create rules to limit VLAN usage for accessing key IT asset devices.
3. Scheduling Monitoring and Evaluation Meetings: Regular meetings should be scheduled to monitor and evaluate the achievement of goals, identify strengths and weaknesses, and provide a basis for improving future decisions.
4. Diversification of Service Providers: Diversify service providers to reduce the risk of dependency on a single provider by using different vendors for various services (e.g., one provider for cloud services and another for network security). This reduces the impact if one provider experiences issues or an attack.

V. CONCLUSION

A. Conclusion

This study explores the implementation of Information Technology (IT) at the Unit Sumber Daya Informasi (USDI) of Udayana University, with a focus on information security management using the COBIT 5 framework, particularly within the APO (Align, Plan, and Organize) and DSS (Deliver, Service, and Support) domains. Information technology is vital in improving the effectiveness and efficiency of educational institutions, and Udayana University uses IT to support its educational activities and academic services.

The research findings indicate that, based on data collected from 21 respondents, the APO 13 and DSS 05 subdomains reached level 3 (established process), meaning that these processes have been well-implemented and can achieve the desired results. Although level 3 has been achieved, the target is to reach level 4, which signifies a more controlled and well-managed IT governance process.

This study provides a foundation for the Unit Sumber Daya Informasi (USDI) of Udayana University to improve IT governance and security to support the achievement of optimal and secure institutional goals.

REFERENCES

[1] Farhatika, N. M., Suprapto, Kussyanti, A., "Evaluasi Tata Kelola Sistem Keamanan Informasi Pada Universitas Muhammadiyah Malang Menggunakan Kerangka Kerja COBIT 5," Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK). x-x, 2016.

[2] ISACA 2013, "A Business *Framework* for the Governance and Management of Enterprise IT," Available at: https://www.isaca.org/COBIT/Documents/COBIT-5-Enabling-Processes-Introduction.pdf.

[3] Ko, D. and Fink, D., "Information technology governance: an evaluation of the theory-practice *gap*. Corporate Governance," The international journal of business in society, 10(5), pp. 662–674. doi: 10.1108/14720701011085616, 2010.

[4] Setiawan, A., "Evaluasi penerapan teknologi informasi di perguruan tinggi swasta Yogyakarta dengan menggunakan model Cobit *Framework*," Seminar Nasional Aplikasi Teknologi Informasi (SNATI), 2008(Snati), p. A-15. doi: 1979- 2328, 2009.

[5] Khther, R. A. and Othman, M., "Cobit *Framework* as a Guideline of Effective *IT governance* in Higher Education," A Review. International Journal of Information Technology Convergence and Services, 3(1), pp. 21–29. doi: 10.5121/ijitcs.2013.3102, 2013.

[6] Mufti, R. G., Suprapto, Mursityo, Y. T., "Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan *Framework* COBIT 5 Fokus Proses APO13 dan DSS05 (Studi Pada PT Martina Berto Tbk)," Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer. 1622-1631, 2017

[7] Saridewi, A. I., Wiharta, D., M., Sastra, N., P., "Evaluation of Integrated University Management Information System Using COBIT 5 Domain DSS," IEEE journal, 2018.

[8] Imany, Y. D., Putra, W. H. N., Herlambang, A. D., "Evaluasi Tata Kelola Keamanan Informasi menggunakan COBIT 5 pada Domain APO13 dan DSS05 (Studi pada PT Gagas Energi Indonesia)," Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer. 5926-5935, 2019.

[9] Effendi, M. F. A., Perdanakusuma, A. R., Hanggara, B. T., "Evaluasi Kapabilitas Keamanan Teknologi Informasi pada Proses APO13 dan DSS05 berdasarkan *Framework* Cobit 5 (Studi pada Dinas Komunikasi dan Informatika Kota Malang)," Jurnal

Pengembangan Teknologi Informasi dan Ilmu Komputer. 698-708, 2020.

[10] ISACA, 2012a, "COBIT 5: A Business *Framework* for The Governance and Management of Enterprise IT Rolling Meadows," ISACA.

[11] Adikara, F., "Implementasi Tata Kelola Teknologi Informasi Perguruan Tinggi Berdasarkan Cobit 5 Pada Laboratorium Rekayasa Perangkat Lunak," *Jurnal Teknik Informatika Universitas Esa Unggul*, pp. 1–6, 2013.

[12] Alhan, M., "Perancangan *IT governance* di Politama Menggunakan COBIT Versi 4.1," X(2), pp. 11–22, 2011.

[13] Amid, A. and Moradi, S, "A Hybrid Evaluation *Framework* of CMM and COBIT for Improving the Software Development Quality," *Journal of Software Engineering and Applications*, 2013(May), pp. 280–288. doi: 10.4236/jsea.2013.65035, 2013.

[14] Andry, J. F., "Audit of *IT governance* Based on COBIT 5 Assessments: A Case Study," Jurnal Teknologi dan Sistem Informasi, 2(2), pp. 27–34, 2016.

[15] Azizah, N., "Audit Sistem Informasi Menggunakan *Framework* COBIT 4.1 Pada E-Learning UNISNU Jepara," Jurnal SIMETRIS, 8(1), pp. 377–382, 2017.

[16] Ekowansyah, E., "Audit Sistem Informasi Akademik Menggunakan COBIT 5 di Universitas Jenderal Achmad Yani," Seminar Nasional Komputer dan Informatika (Senaski), 2017, pp. 201–206, 2017.

[17] De Haes, S., Van Grembergen, W. and Debreceny, R. S., "COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities. Journal of Information Systems, 27(1), pp. 307–324. doi: 10.2308/isys-50422, 2013.

[18] Mangalaraj, G., Singh, A. and Taneja, A., "*IT governance Framework*s and COBIT-A Literature Review," Twentieth Americas Conference on Information Systems, pp. 1–10. doi: 10.2308/jis.2009.23.1.79, 2014.

[19] Mayang Sari, I., Noor Ali, A. H. and Kurnia, I., "Pembuatan Metode Evaluasi Kematangan Pelaksanaan Proyek dengan Menggabungkan COBIT 5 Domain VAI 1.11 dan MEA 1.04 dengan Best Practice PMBOK 4th. Studi Kasus : Direktorat Pengelolaan Sistem Informasi (DPSI) Bank Indonesia," Teknik POMITS, 1(1), pp. 1–8, 2013.

[20] Nugroho, H., "Conceptual model of *IT governance* for higher education based on COBIT 5 *Framework*," Journal of Theoretical and Applied Information Technology, 60(2), pp. 216–221. doi: ISSN: 1992-8645, 2014.

[21] Pasquini, A. and Galiè, E., "COBIT 5 and the Process Capability Model. Improvements Provided for *IT governance* Process," Proceedings of FIKUSZ '13 Symposium for Young Researchers, pp. 67–76, 2013.

[22] Prasetyo, A. and Mariana, N., "Analisis Tata Kelola Teknologi Informasi (*IT governance*) pada Bidang Akademik dengan Cobit Frame Work Studi Kasus pada Universitas Stikubank Semarang," Jurnal Teknologi Informasi DINAMIK, 16(2), pp. 139–149, 2011.

[23] Purnomo, L. H. D. and Tjahyanto, A., "Perancangan Model Tata Kelola Ketersediaan Layanan Ti Menggunakan *Framework* Cobit Pada Bpk-Ri," Seminar Nasional Informatika, 2010(semnasIF), pp. 113–119, 2010.

[25] Radha, V. and Reddy, D. H., "A Survey on Single Sign-On Techniques," Procedia Technology. Elsevier B.V., 4, pp. 134–139. doi: 10.1016/j.protcy.2012.05.019, 2012.

[26] Rozas, I. S. and Galulien, D., "Kuesioner berbasis control objective cobit 4.1 untuk melakukan audit teknologi informasi," 18(1), pp. 29–34, 2013.