JMTAS: Jurnal Teknologi Multimedia dan Perangkat Lunak Terapan
Published: 30 April 2026
E-ISSN: 3047-4760

INFORMATION SYSTEM SECURITY AUDIT OF THE ACADEMIC SYSTEM USING THE COBIT 5 (APO13) AT POLITEKNIK MARDIRA INDONESIA

Fikri Akbar Falcata Winata*, Muhammad abdul jabbar 2*
Teknologi Rekayasa Multimedia 1, Politeknik Mardira Indonesia 1, Teknologi Rekayasa Multimedia 2, Politeknik Mardira Indonesia 2

Email : fikriakbar094@gmail.com, jabbarmuammad20@gmail.com**

ABSTRACT

This study aims to conduct a security audit of the Academic Information System using the COBIT 5 framework in the APO13 (Manage Security) domain. The methods used include observation, interviews, questionnaires, and literature studies. The data obtained are then analyzed to determine the maturity level and identify gaps between current conditions and expected conditions. The results of this study indicate the capability level of the APO13 process, namely Level 0 (Incomplete Process) with status L (Largely Achieved), which means that most of the information system security management has been achieved. Level 1 (Performed Process) with a level achievement of 50% with status P (Partially Achieved), which means that information system security has been partially achieved. Furthermore, Levels 2, 3, and 5 obtained average results above 65% with status L.

Keywords: COBIT 5, APO13, Information Systems Audit, Information Systems Security.

ABSTRAK

Penelitian ini bertujuan untuk mengidentifikasi dan mengukur tingkat kematangan keamanan sistem informasi. Permasalahan yang sering dialami pada salah satu objek penelitian yaitu belum adanya evaluasi tingkat kematangan terhadap keamanan sistem informasi. Untuk menghindari permasalahan yang ada dimasa yang akan datang, maka diperlukannya audit keamanan sistem informasi. Audit ini menggunakan framework COBIT 5 dengan fokus pada proses APO13 (Manage Security) yang bertujuan untuk menjaga dampak dan kejadian insiden keamanan informasi dalam tingkat risiko yang dapat di selesaikan oleh perusahaan. Hasil dari penelitian ini diketahui tingkat kapabilitas dari proses APO13 yaitu Level 0 (*Incomplete Process*) dengan status L (*Largely Achieved*) yang artinya sudah mencapai sebagian besar pengelolaan keamanan sistem informasi. Level 1 (*Performed Process*) dengan pencapaian level sebesar 50% dengan status P (*partially achieved*) yang artinya keamanan sistem informasi sudah tercapai sebagian. Selanjutnya juga pada Level 2,3 dan 5 yang memperoleh hasil rata-rata diatas 65% dengan status L.

INTRODUCTION

In improving current business processes, companies or organizations cannot be separated from information technology. Information technology increasingly provides many conveniences to its users. These conveniences arise due to the rapid and widespread development of information technology across various aspects of life, which also brings both positive and negative impacts. To ensure its optimal use, proper and effective IT governance is required so that its existence can support the achievement of business objectives within the company or organization. A company or organization must be able to address existing problems. It should not only focus on IT governance, but also maintain and enhance the quality of its information system security. Information security includes the protection of confidentiality, availability, and integrity.

The Academic Information System is one of the important components in supporting business processes within higher education institutions. This system plays a role in managing various important data such as student data, lecturer data, class schedules, grades, and other academic information that is sensitive and crucial. Therefore, information security is a very important aspect to consider in order to maintain the confidentiality, integrity, and availability of data.

oliteknik Mardira Indonesia, as a higher education institution, has implemented an Academic Information System to improve the efficiency and effectiveness of academic services. However, along with the increasing use of information technology, the potential threats to system security are also rising, both from internal and external factors. These threats may include unauthorized access, data breaches, and disruptions to system operations that could harm the institution. n an effort to ensure that information security management is properly implemented, a structured and systematic information system security audit is required. One of the frameworks that can be used is COBIT 5, particularly in the APO13 (Manage Security) domain, which focuses on comprehensive and integrated information security management aligned with organizational objectives.

Through an audit using the COBIT 5 APO13 framework, it is expected that an evaluation of the maturity level of information

security management in the Academic Information System at Politeknik Mardira Indonesia can be conducted. The results of this audit can then be used as a basis for providing improvement recommendations to enhance system security, minimize risks, and support the optimal achievement of institutional goals.

AUDIT AND GOVERNANCE OF COBIT 5

IT governance audit can be defined as an activity of collecting and evaluating available evidence to determine whether IT processes within Politeknik Mardira have been managed in accordance with established standards and supported by control objectives to monitor their usage, as well as whether they effectively achieve the organization's business objectives through efficient use of resources. Information security is used to protect the confidentiality, integrity, and availability of information assets, whether in storage, processing, or transmission. This is achieved through the implementation of policies, education, training, awareness, and technology. Information security has evolved around three main concepts that serve as fundamental standards in the security industry, commonly referred to as the CIA triad: confidentiality, integrity, and availability. Information threats can harm companies or organizations that rely on such information. Several forms of information threats that may disrupt business processes include interruption, interception, modification, and fabrication.

COBIT (Control Objectives for Information and Related Technology) is a collection of documentation and guidelines used to support the implementation of IT governance. As a framework, COBIT plays an important role in assisting users, auditors, and management in bridging the gap between control requirements, business risks, and various technical issues related to information technology. COBIT 5 is a framework for managing and governing all aspects related to information technology, including meeting stakeholder needs. COBIT 5 is based on fundamental principles for IT governance and management. These five principles are expected to help organizations establish effective governance, optimize risk levels, and deliver value to the enterprise, as illustrated in the following figure :

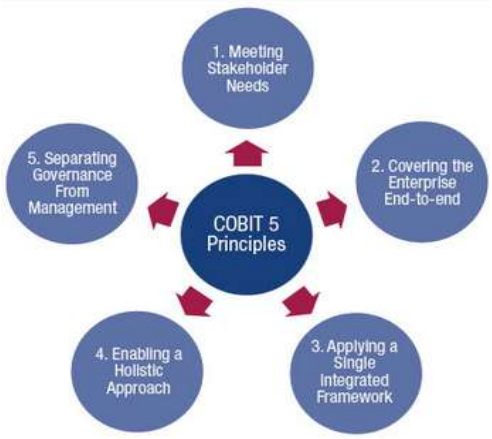

Figure 1. The Five Basic Principles of COBIT 5

The APO13 process refers to the definition, operation, and monitoring of systems implemented by an organization to manage its information security. This process aims to ensure that the occurrence and impact of information security incidents do not exceed the risk level determined by the organization.Process capability indicators represent the ability of a process to achieve a certain level of capability, which is defined by process attributes. Evidence of these capability indicators supports the assessment of the achievement of process attributes.The capability dimension in the process assessment model consists of six capability levels, as illustrated in the following figure :

Figure 2. Process Capability Model in COBIT 5

Results and Discussion

This study focuses on issues related to information security within the governance of information systems at Politeknik Mardira Indonesia. The results of this study are used to design improvement strategies that are expected to support Politeknik Mardira

Published: 30 April 2026
E-ISSN: 3047-4760

Indonesia in achieving its business objectives. A document study was conducted on security management procedures, including SOPs for internet troubleshooting, active directory (user management), web-based storage, storage server operations, and streaming servers. In addition, interviews were conducted with several informants who have roles and responsibilities in security management. Table 1 presents the results of interviews with these informants.

Table 1. Interview Results Related to Information System Security Management

Question Topics	Discussion Results
APO13.1 (Building and Maintaining an Information Security Management System)	
The Form of Existing Information System Security	Sistem *service*, akses user password and *Firewall*
The Existence of a Dedicated Division for Information System Security	There is only an IT division
SOP (standar operasional prosedur) Regarding Information System Security	SOP There is no dedicated information security unit yet
APO13.2 (Defining and Managing an Information Security Handling Plan)	
Procedures for Resolving Information System Security Issues	Monitoring is conducted onusage logs.
Plans for Improving and Enhancing Information System Security	Improvements are made when security vulnerabilities are identified; otherwise, only routine maintenance is carried out.
Information System Access Rights Management	Access rights management is regulated within each work unit
APO13.3 (Monitoring and Reviewing the Information Security Management System)	
Methods for Monitoring Information System Security	Monitoring is carried out through system logs and passwords.
Encryption in Information Systems	Only some information systems are encrypted

The questionnaire was administered to several respondents to assess the achievement levels and evaluate the processes for each attribute. Figure 3 below presents the detailed results for each level based on the process attributes, along with the breakdown of the questionnaire calculations.

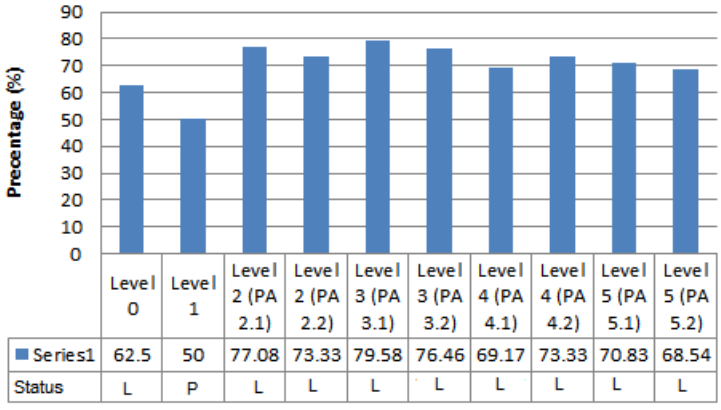

Figure 3. Rating Calculation at Each Level 3

The results of this study aim to gradually improve the management of information system security. Therefore, the next target level to be achieved is Level 2, which enables continued improvement of information system security up to the highest level, Level 5.Level 0 (Incomplete Process) has a status of L (Largely Achieved), meaning that most aspects of information system security management have been implemented. Level 1 (Performed Process) has an achievement level of 50% with a status of P (Partially Achieved), indicating that information system security has been partially implemented. Furthermore, Levels 2, 3, and 5 have achieved average results above 65% with a status of L (Largely Achieved).

Published: 30 April 2026
E-ISSN: 3047-4760

Conclution

Based on the results of the conducted community service activity, it can be concluded that the level of information system security at Politeknik Mardira Indonesia, based on the current capability level assessment, has reached Level 1 (Performed Process) at 50%, with a Managed Process status of P (Partially Achieved). This indicates that the overall management of information system security has not yet been optimally achieved, as the target to be reached is around 80%. Therefore, improvements in information system security are necessary.

Recommendations

Based on the results of this study, the following recommendations are proposed:

1. Politeknik Mardira Indonesia is advised to improve its information system security management process by developing more structured and well-documented policies and procedures.
2. Regular information system security evaluations and audits should be conducted to monitor maturity level progress and identify potential risks at an early stage.
3. It is important to enhance awareness and competence of human resources through training related to information security to ensure more effective implementation.
4. The implementation of the COBIT 5 framework, particularly in the APO13 process, should be optimized to achieve a higher capability level.
5. A continuous improvement plan should be developed to enhance the maturity level of information system security in accordance with the expected targets.

DAFTAR PUSTAKA

[1] A. L. K. W. Iik Muhamad Malik Matin, "Analisis Keamanan Informasi Data Center Menggunakan COBIT 5," Jurnal teknik informatika, vol. 10, pp. 119 -128, 2017.

[2] E. N. D. A. Dewi Ciptaningrum, "COBIT 5 Sebagai Metode Alternatif Bagi Audit Keamanan Sistem informasi (Sebuah Usulan Untuk Diterapkan di Pemerintah Kota Yogyakarta)," Seminar Nasional Teknologi Informasi dan Multimedia 2015, July 2015.

[3] E. N. D. A. Dewi Ciptaningrum, "Audit Keamanan Sistem Informasi Pada Kantor Pemerintah Kota Yogyakarta Menggunakan COBIT 5," Seminar Nasional Teknologi Informasi dan Komunikasi 2015, pp. 65 -74, 12 July 2015 [4] SimilarWeb. (2022). Most popular apps in Indonesia. https://www.similarweb.com/apps/top/google/store-rank/id/all/top-free/ [Diakses pada 24 April 2022]

[4] P. s. sukanto, "PERANCANGAN SISTEM MONITORING PERANGKAT JARINGAN BERBASIS ICMP DENGAN NOTIFIKASI TELEGRAM," ITEJ (INFORMATION TECHNOLOGY ENGINEERING JOURNALS), vol. 2, no. 2, 2017.

.[5] R. Sarno, Audit Sistem dan Teknologi Informasi, Surabaya: ITS press, 2009.

.

[6] R.T.Asmono, Proteksi Aset Informasi, Semarang, 2014.