Journal of Applied Engineering and Technological Science
Vol 5(2) 2024: 941-954

RISK ASSESSMENT MATURITY LEVEL OF ACADEMIC INFORMATION SYSTEM USING ISO 27001 SYSTEM SECURITY ENGINEERING-CAPABILITY MATURITY MODEL

Nurbojatmiko[*1], Qurrotul Aini[2], Nabil Cahya Wasiqi[3], Muhammad Fitra Alfajri[4], Zahra Ulinnuha[5], Yuni Kurnia Purwati[6], Indah Kusuma Ayu[7], Natasya Aurora Yasmin[8]
Department of Information Systems, Universitas Islam Negeri Syarif Hidayatullah Jakarta, Indonesia[12345678]
nurbojatmiko@uinjkt.ac.id[*1], qurrotul.aini@uinjkt.ac.id[2]

Received : 08 August 2023, Revised: 03 Mei 2024, Accepted : 05 Mei 2024
**Corresponding Author*

ABSTRACT
Risk measurement from standard operating procedures implemented by an institution determines the level of maturity of a service system at that institution. The government's determination of the Tri Dharma of Higher Education consists of education and teaching, research, and community service. These activities must be implemented in the academic information system of every university in Indonesia. Appropriate and fast academic services depend on information technology and adequate and trained human resources (HR). Factors that influence information system security determine the stability of application services. The ISO/IEC 27001:2005 standard is an international benchmark for measuring the level of maturity and security risks of an application. Risk assessment in standard operating procedures in organizations can use the ISO/IEC 27001 standard. This research aims to determine the current level of Academic Information System (AIS) service by measuring maturity and security risks. Three clauses measure the maturity level of information security controls with the ISO 27001 System Security Engineering-Capability Maturity Model (SSE-CMM). These research respondents are educational work units at the Science and Technology Faculty in UIN Syarif Hidayatullah Jakarta. This research method uses quantitative research methods. This research results show the maturity level of information security in the academic information system based on three clauses as the embodiment of the stability of the academic administration activities services at the Science and Technology Faculty. The measurement results reveal that the average score of information security controls on AIS is 3.51, which means good or average standard processing has been carried out following procedures.
Keywords : *Academic Information Systems, Risk Assessment, Maturity Level, SSE-CMM, ISO/IEC 27001:2005*

1. Introduction

Information system security from all threats determines the risk assessment of the use of the system or Apps. Earlier study evaluated the maturity level of risk assessment for decision-making with the attributes of uncertainty, conservatism, knowledge, and sensitivity, and also the sub-attributes of data availability, data consistency, data reliability, experience, and value content (Bani-Mustafa et al., 2017). Fazlida & Said (2015) integrated information security into IT Governance (ITG) to guarantee the confidentiality, integrity, and availability of information The exchange of critical information between all industry entities (automotive) including world contractors affects information security vulnerabilities, and trust in research and business plans. Królikowski presented a solution that enables information security assessment using the Trusted Information Security Assessment Exchange (TISAX) by showing similarities and differences with the international standard ISO 27001 (Królikowski & Ubowska, 2021). Al-Karaki offers an independent assessment of cyber security using the Gosafe Framework for the development of Security Information Management Systems (ISMS). The Gosafe Framework uses a mathematical model for the assessment of the National Cyber Security Index (aeNCI) with parameters to determine the maturity of a cybersecurity program. Gosafe verifies system security configurations and identifies potential attack/risk vectors (Al-Karaki et al., 2022). This research evaluates the maturity level of risk assessment in information security for academic information systems.

Another systematic literature review (SLR) revealed that quantifying the return on investment in cyber security in the framework of assessing cyber security maturity in technology startup companies determines the startup's cyber maturity posture (Marican et al., 2023). The standard in SLR determines measurement parameters using an appropriate model for the information system security maturity level. The maturity levels of the COBIT model consist of Level 0 – Non-existent, Level 1 – Initial/Ad hoc, Level 2 – Repeatable but intuitive, Level 3 – Defined process, Level 4 – Managed and measurable, Level 5 – Optimized (Mohamad Stambul & Razali, 2011). Other research assessed the performance of Low Carbon City (LCC) using the Capability Maturity Model (CMM) then called LCC-CMM Key Process Area (KPA) identification (Shen et al., 2021). Also, another the study assessed maturity in the implementation of smart manufacturing to lower barriers to entry and reduce investment risks from the factory automation system transformation process (Shi et al., 2019). Meanwhile, Tan assessed the maturity of multifunctional multicapability (MFMC) systems for component development, and importance analysis during system development and maintenance (Tan et al., 2010). And, Volk & Mazanis (2017) measured the progress of defense programs in the implementation of support and sustainment strategies, referred to as Sustainment Maturity Levels (SMLs) covering logistics, but reliability, system security, configuration management, and data management.

Previous research evaluated all controls required to protect confidentiality, integrity, and availability using ISO/IEC 27001:2013 covering 114 controls across 14 different domains. The research results show the information security maturity level at level 2 (Volk & Mazanis, 2017). Increasing the effectiveness of the teaching and learning process and the quality of administration of the entire academic community through AIS at universities (Hidayah, 2020). Improving academic administration services in managing large amounts of data requires effective and simple management capabilities. Academic information system management specifications must meet information system security according to ISO 27001 standards (Volk & Mazanis, 2017). Several previous studies have carried out measurements of capability maturity levels in AIS, this research carried out SSE-CMM measurements using ISO/IEC 27001 in the asset management, human resources security, and access control clauses.

Kurniawan's publication concentrates on ISO 27002:2013, and the SSE-CMM method for analyzing security levels of the clause access control in academic information systems. The research results show the access control services of the academic information system are still at the second layer namely the initial/ad hoc layer (Kurniawan et al., 2017). Other research compared the National Institute of Standards and Technology's (NIST) Cyber Security Framework and the ISO 27001 Information Security Standard by mapping key security control frameworks/guidelines such as NIST SP 800-53, CIS Top 20, and ISO 27002 (Roy, 2020). Previous studies investigated ISO 27005 as a reference point and did a comparison with methods of Information System Risk Assessment (ISRA) to measure the completeness of all the issues and activities (Volk & Mazanis, 2017). In the meantime, many participants in ISO 27001 have certified their businesses and presented a security policy for security requirements to the targeted organization. This standard's efficacy and efficiency benefits are extremely high, and it meets the technical requirements for worldwide security with a surprising number of certifications (Volk & Mazanis, 2017). ISO 27001 is a recommendation for the basis for designing and assessing the level of information security management capabilities of ongoing academic information systems in UIN Jakarta.

Tridharma of Higher Education, hereinafter referred to as Tridharma, is the obligation of universities to provide education, research, and community service as stated in the Regulation of The Minister of Education, Culture, Research and Technology of The Republic of Indonesia Number 53 of 2023 Concerning Guaranteing The Quality of Higher Education. Previous study had developed AIS with the implementation, and experimentation of the EU QualiChain H2020 pilot. This trial is to ensure the authenticity and integrity of the diploma for all stakeholders involved (Guerreiro et al., 2022). Ma et al. (2024) conducted a literature review and network research to examine the provision of intellectual property information services (IPIS) plays an important role in strengthening the infrastructure of academic service systems for intellectual property. All information pertaining to academic issues on campus can be found through the

Academic Information System (AIS). The Academic Information System can be utilized as a communication tool by students, lecturers, campus administrators, and anyone else in the campus environment, in addition to being the campus information resource. Therefore, the Academic Information System is a system designed to handle all academic-related issues in order to enhance the standard of instruction and learning as well as administrative standards pertaining to the university's academic community as a whole (Volk & Mazanis, 2017). The academic information system at UIN Syarif Hidayatullah is called AIS. This study aims to measure the level of maturity in the effectiveness of AIS at the Faculty of Science and Technology, UIN Syarif Hidayatullah Jakarta. The results of this research can determine the level of academic application services in asset management, human resource security, and access control. This can be a recommendation for improvements in services to information security in academic information systems.

2. Literature Review

Tanovic evaluated IPTV/VoIP services of Telecommunication operators in Bosnia and Herzegovina using ISO 20000-1 as an IT service management standard and ISO 27001 as an information security service standard (Tanovic & Marjanovic, 2019). Other researcher mapped the clauses and control targets of ISO/IEC 27001 into the domain scope and control objectives as in Table 1(Yasin et al., 2020).

Table 1- Mapping Scope to Control Objective of ISO 27001(Yasin et al., 2020)

No	Scope	Control Objectives
1	Information security policies.	Management direction for information security.
2	Organization of information security.	Internal organization. Mobile devices and teleworking.
3	Human resource security.	Prior to employment. During employment. Termination and change of employment.
4	Asset management.	Responsibility for assets. Information classification. Media handling.
5	Access control.	Business requirements of access control. User access management. User responsibilities. System and application access control.
6	Cryptography.	Cryptographic controls.
7	Physical and environmental security.	Secure areas. Equipment.
8	Operations security.	Operational procedures and responsibilities. Protection from malware. Backup. Logging and monitoring. Control of operational software. Technical vulnerability management. Information systems audit considerations.
9	Communications security.	Network security management. Information transfer.
10	System acquisition, development, and maintenance	Security requirements of information systems. Security in development and support processes. Test data.
11	Supplier relationships.	Information security in supplier relationships. Supplier service delivery management.
12	Information security incident management.	Management of information security incidents and improvements.
13	Information security aspects of business continuity management.	Information security continuity. Redundancies.
14	Compliance.	Compliance with legal and contractual requirements. Information security reviews

Almeida et al. (2018) assessed Enterprise Governance of IT (EGIT) using the COBIT framework and ISO 27001 standards to increase organizational efficiency and effectiveness. The effects of risk can differ depending on factors, including strategy, operations, reporting, and

obedience. Information technology asset risk is the potential for events affecting IT assets to negatively influence goals, plans, or IT assets (Volk & Mazanis, 2017). Evaluation of the maturity level of security controls using ISO 27001:2013 and COBIT 5 in organizations that operate an Information Security Management System (ISMS) for tactical and strategic decision-making, as well as input for organizational information security risk management (Monev, 2020). Peciña converges Physical and Logical Security management using the methodology of the ISO 31000 standard (physical security) and the ISO 27001 standard (logical security) (Peciña et al., 2011). Information system security assessment using ISO 27001 combines with various methods to complement the service management of an organization in previous research.

The development of information security processes following ISO 27001 requirements determines preventive action plans to minimize and eliminate risks (Syreyshchikovaa et al., 2019). Capability and maturity model (CMM) assessment using the ISO/IEC 15504-330xx approach contributes to alignment and improvement of organizational and business processes (Barafort et al., 2018). Risk is the possibility of something affecting a goal (Barafort et al., 2018). Due to susceptibility, risk has a negative effect as seen in Fig. 1 (Barafort et al., 2018). Assessment of the security maturity level of information resources using ISO/IEC 27001 determines the process of prioritizing security aspects according to the size and line of business of the company (Lopez-Leyva et al., 2020). The first two steps are part of risk management. First, risk analysis is the process of locating variables that have an impact on data. Second, there are four primary aspects of security risk assessment: Threats are identified, prioritized based on risk, and then control and protection measures are decided upon. Finally, a strategy is developed for the implementation of these measures (Volk & Mazanis, 2017). Selecting the appropriate index system requires doing a security risk evaluation for information systems. Only a scientific index system that is realistic and reliable can support an objective assessment activity.

An academic information system is a web-based information system that intends to create an accessible knowledge-based network through the internet (Barafort et al., 2018) —the types of information it contains. News contains the latest information published by the institution and obtained through information technology from various news sources. Education contains information relating to courses that are instituted, such as curriculum, lecturer, course materials, job training, thesis, and research. The class schedule contains class schedules, student activities, the lecturer's lecture schedule, and attendance in the following lectures. The library contains information about the book through an online catalog. Electronic mail (e-mail), the facility to send and receive mail/messages, can also be used as a means or instrument of discussion among students, faculty, and even employees in educational institutions.

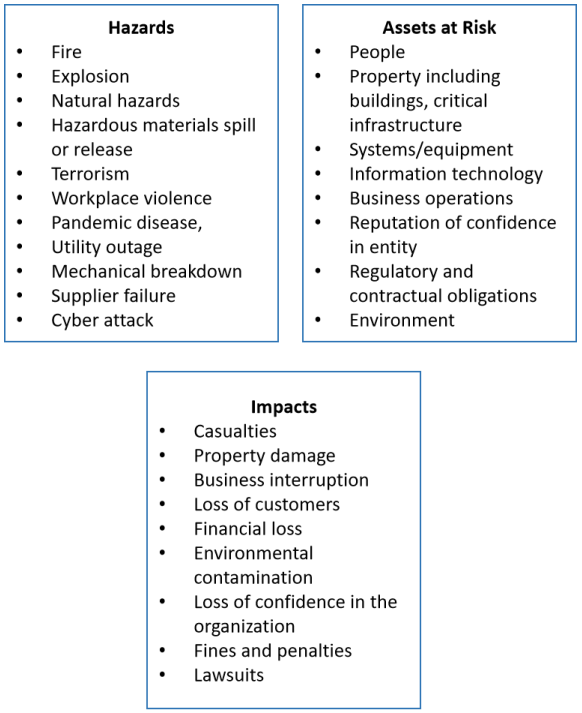

Fig. 1. Risk Assessment Process (Barafort et al., 2018).

An international standard known as ISO 27001 regulates information security management systems. The International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO) jointly released this standard. ISO/IEC 27001 provides a framework and set of principles for addressing information security risks inside an organization. The importance of ISO/IEC 27001 lies in the following: (1) it assists businesses in identifying, assessing, and managing information security risks; (2) it safeguards confidential and sensitive data as well as other information assets from threats like hacking, data theft, or damage from security incidents; (3) it complies with legal and regulatory requirements, preventing fines and penalties that could be imposed for data security violations; and (4) it can boost customer trust by demonstrating the business's strong commitment to information security, which may pique the interests of clients who are worried about the confidentiality and integrity of their data (Barafort et al., 2018). ISO 27001 provides a comprehensive framework that helps organizations develop and maintain a secure IMS. ISO 27001 is divided into 14 phases: information security policy, information security organization, risk assessment, and treatment, up risk monitoring and review (Al-Dhahri et al., 2017).

There are 11 clauses in ISO 27001, which are further divided into 133 controls. According to ISO/IEC 27001: 2005, these controls must be created, deployed, executed, monitored, analyzed, and maintained while considering the organization's business risks (Fomin et al., 2008). The organizational structure of ISO/IEC 27002: 2005 is split into two sections. If the organization uses the ISO/IEC 27001 ISMS standard, the first clause's Mandatory Process Clause (Article) must be satisfied. The Security Control Annex security oversight. It has 133 control objectives, 39 controls, and 11 security control clauses (Al-Dhahri et al., 2017).

Information security is all possible threats to ensure business continuity, minimize business risk, and maximize or accelerate return on investment and business opportunities (Al-Dhahri et al., 2017). Security Metrics are measurable measurements of some entity (system, product, or other). Specific metrics are quantitative or qualitative evidence of a particular SSE maturity level-CMM process areas are an indication of the presence or absence of mature processes, as shown in Table 2 (Ferraiolo, 2000). Barafort analyzed the organizational capabilities of risk management activities in IT settings with a centralized and integrated risk management approach based on ISO standards (Barafort et al., 2017).

Table 2 – Capability Maturity Model (Ferraiolo, 2000; Barafort et al., 2018)

Maturity Level	Description
ML 1 Initial	The process is not controlled

ML 2 Managed	Implementation process
ML 3 Defined	The planning and implementation of good practices and management procedures.
ML 4 Managed	The process of integration and the interoperability of multiple applications and the exchange of information.
ML 5 Optimized	This process-oriented digital is based on a solid technology infrastructure.

The system security engineering capability maturity model (SSE-CMM) is a process reference picture that focuses on the requirements for implementing security in a set of related systems that constitute the information technology security domain. The assessment that determines the level of capability of each process area can be useful as a focus for improvement that takes into account business goals (Al-Dhahri et al., 2017). The SSE-CMM (System Security Engineering Capability Maturity Model) capability level has 5 levels in SSE-CMM, as shown in Table 3.

Table 3 - SSE-CMM Maturity Level (Proenca et. al., 2016)

Maturity Level	Level Description
Level 1,"Performed Informally"	The basic performance may not be planned and tracked closely
Level 2,"Performed Informally"	Performance in accordance with the procedures prescribed verified.
Level 3,"Performed Informally"	Basic practices are carried out in accordance with a well-defined process.
Level 4,"Performed Informally"	Detailed performance measures were collected and analyzed.
Level 5,"Performed Informally"	Quantitative performance targets for effectiveness and efficiency of the process.

The SSE-CMM assessment method has the advantage of covering security engineering activities covering the trusted product or system security life cycle, including concept definition, requirements analysis, design, development, integration, installation, operation, maintenance, and monitoring; it can be applied to secure product developers, security system developers, integrators, and organizations that provide security and security engineering services; and it is applied to all types and sizes of security engineering organizations, such as commercial, government, and academic (Al-Dhahri et al., 2017).

3. Research Method

Figure 2 shows the steps in this research method. The first stage is a literature review; a review of previous research on ISO 27001, CMM, asset management, and information system security risks. This stage also pays attention to the organization's need to obtain the three clauses in ISO 27001 SSE-CMM (Asset management, human resource security, and access control). The second stage is data collection; dissemination and collection of data uses observation, questionnaires, and interviews according to the specified clauses. The third stage is data analysis and processing; This stage analyzes gaps and determines the level of maturity based on the results of data processing. Each statement is assessed for its level of certainty according to the results of the examination using assessment criteria according to the specified clause. The results of the research are recommendations based on measuring the level of capability and maturity in the three clauses.

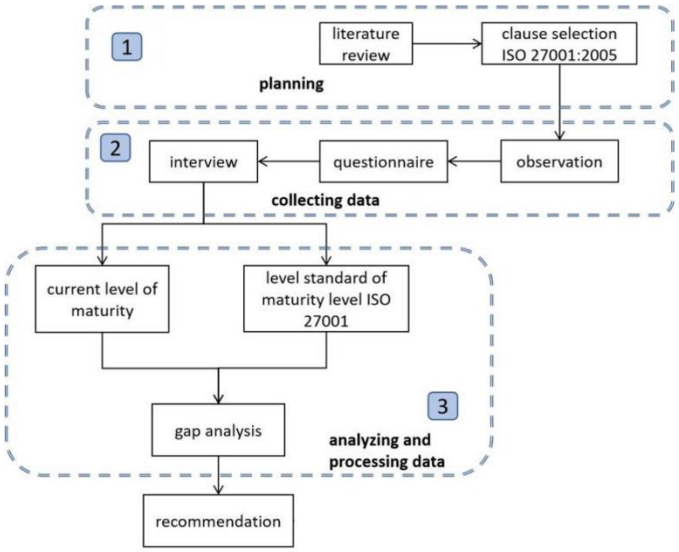

Fig. 2. Research steps.

4. Results and Discussions

A. *Determine Maturity Level*

1) Clause 7 Asset Management

The result of the calculation process, shown in Table 4 for the maturity level in clause 7 is 3.29, which is defined. This finding suggests that asset management is important for the organization's performance. Meanwhile, Figure 3 visualizes the maturity level clause 7.

Table 4 - Clause Asset Management.

Clause	Objective Control	Security Control	Ability Level	On Average Objective Control
7 Asset Management	7.1 Responsibility for assets	7.1.1 Inventory of assets	4.00	3.58
		7.1.2 Asset ownership	3.75	
		7.1.3 Use of Assets Acceptable	3.00	
	7.2 Classification of Information	7.2.1 Classification Guidelines	3.00	3.00
		7.2.2 Labeling and handling of information	3.00	
Maturity Level Clause 7				3.29

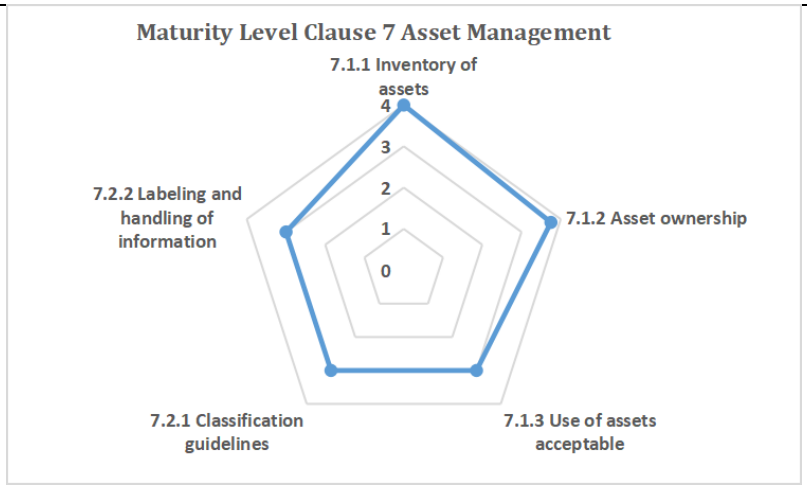

Fig. 3. Maturity Level Clause 7 Asset Management.

2) Clause 8 Human Resource Security.

The calculation for maturity level in clause 8 yielded a result of 4.00, which is handled (Table 5). This outcome demonstrates that third-party users, contractors, and staff are aware of their duties. The possibility of theft, fraud, or improper use of facilities is decreased. Figure 4 visualizes the maturity level clause 8 in security human resources.

Table 5 - Clause of Human Resource Security.

Clause	Objective Control	Security Control	Ability Level	On Average Objective Control
8 Security Human Resources	8.1 Before work	8.1.1 Roles and Responsibilities	4.00	3.67
		8.1.2 Screening	4.00	
		8.1.3 Terms and Conditions of Employment.	3.00	
	8.2 During the work	8.2.1 Management responsibility	5.00	4.33
		8.2.2 Information security awareness, education, and training	4.00	
		8.2.3 Process discipline	4.00	
	8.3 Termination of employment or change of employment	8.3.1 The responsibility of termination of employment	4.00	4.00
		8.3.2 The recovery of assets	4.00	
		8.3.3 Removal of access rights	4.00	
Maturity Level Clause 8				4.00

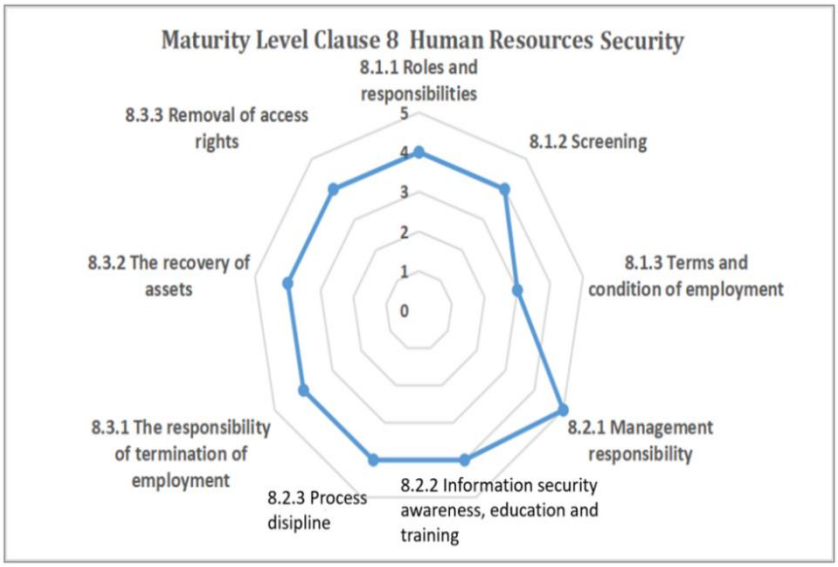

Fig. 4. Maturity level clause 8, Human Resources Security.

3) Clause 11 Access Control (Access Control)

The result of the calculation process for maturity level in clause 11 is 3.24 and it is shown in Table 6. It is evident in the documentation, quality assurance, and change management method. Software development has a specialized element that does not always depend on individual ability. The scores for the whole security control are visualized in Fig. 5.

Table 6 - Clause of human resource security.

Clause	Objective Control	Security Control	Ability Level	On Average Objective Control
11 Access Control	11.1 Business Requirements for Access Control	11.1.1 Access Control Policies	3.25	3.67
	11.2 Access Rights Management	11.2.1 User registration	3.16	3.22
		11.2.2 Management or special privileges	3.25	
		11.2.3 User password management	3.27	
		11.2.4 A review of user access rights	3.21	
	11.3 Responsibility User	11.3.1 Use of passwords	3.31	3.16
		11.3.2 User equipment unattended	3.02	
		11.3.3 Clear desk and clear policy server	3.14	

11.4 Network Access Control	11.4.1 Network service usage policy	3.24	3.03
	11.4.2 User authentication to initiate outbound connections	2.81	
	11.4.3 Identification of equipment in the network	3.04	
	11.4.4 Protection remote diagnostic and configuration port	2.97	
	11.4.5 Separation and network scanning	2.84	
	11.4.6 Control over the network connection	3.22	
	11.4.7 Control of the routing network	3.12	
11.5 Operating System Access Control	11.5.1 Procedure log-on safe	2.78	3.18
	11.5.2 Identification and User authentication	3.24	
	11.5.3 Password management system	2.73	
	11.5.4 Use of system utilities	3.42	
	11.5.5 Session time-out	3.51	
	11.5.6 Limitation of connection time	3.42	
11.6 Information and Application Access Controls	11.6.1 Restrictions on access to information	3.51	3.58
	11.6.2 Isolation-sensitive systems	3.64	
Maturity Level Clause 11			3.24

B. Academic Information System Security Check

Based on the information system security audit, the password management system has the lowest value, i.e., 2.73, in clause 11. Based on the audit results, password misuse occurs due to regulations that are less strict and less specific to the confidentiality of the password. Therefore, it results in the leakage of confidential information and other important matters. In addition, the problem is caused by the need for more authentication of users to connect, formal investigation of network scanning at regular intervals, and the lack of knowledge of employees. After calculating the maturity level in clauses 7, 8, and 11 obtained under the ISO 27001 standard, it can be seen the value of the average level of maturity or maturity level on AIS, as described in Table 7.

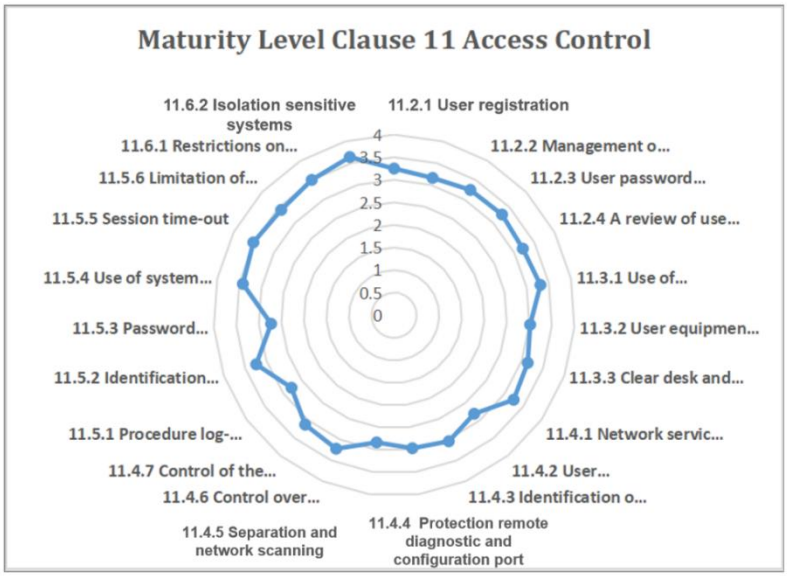

Fig. 5. Maturity level clause 11, Access Control.

Table 7 - Result of maturity level calculation.

Security Control	Description	Index	Level
7	Asset Management	3.29	3
8	Control Access	4.00	4
11	Human Resource Security	3.24	3
Maturity Level Average		3.51	3

The average of information security controls on AIS is 3.51. From this score, it can be concluded that the security information at the level of four is defined by good or average standards executed following the procedure.

C. Gap Analysis

Based on the calculation of the current academic information system's information security maturity level, 3.51 (managed) is included in level 4, and the expected maturity level is 5 (optimized).

Table 8 - Result of gap measurement.

Clause	Information	Maturity Level		GAP
		Present Condition	Expected Condition	
7	Asset Management	3.29	5.00	1.71
8	Human Resource Security	4.00	5.00	1.00
11	Control Access	3.24	5.00	1.76
		Average		1.49

The average output, as seen in Table 8, is a 1.49 mean value of the gap between current conditions and conditions expected to have a gap. As a result, it is necessary to adjust each control in terms of the ratio of the current maturity level's value to the expected maturity level.

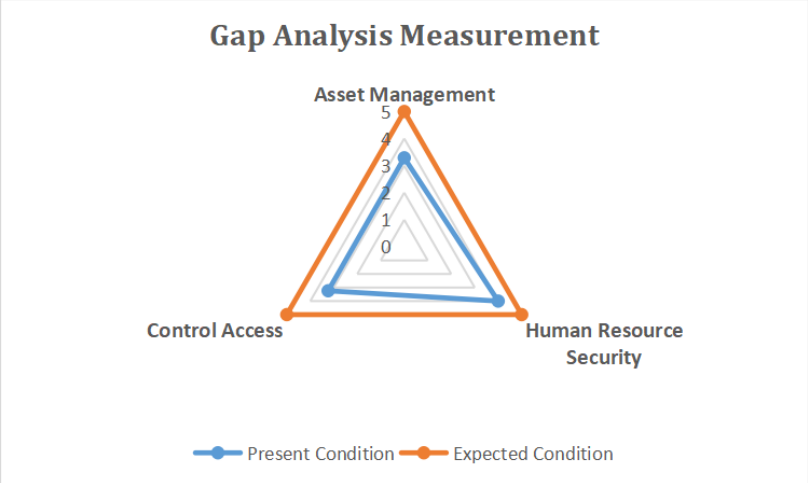

Fig. 6 Gap analysis measurement.

Figure 6 shows that the maturity level on the condition that is expected to increase continuously indicates the default has been perfect and focuses on adapting to change. The target selection level is based on the analysis results, where the value of the security controls is spread between grades 1 and 3. The current security level of the highest value gap analysis is 1.76, whereas Clause 11 with the maturity level of information security at the level of 3,24 condition this time. Whereas in clause 8, the value of the level of maturity reached 4.00, so it has the lowest gap value is 1.00.

D. Recommendation

Recommendations for evaluating the implementation of this information system security audit appear after the previous comparison. The findings give recommendations that can be used to improve the information system process in the future.

Table 9 - Finding and recommendation clause 7 asset management.

Clause	Objective Control	Security Control
7. Asset Management	7.1 Responsibility for assets	7.1.3 Use of Assets Acceptable
	Finding: - Assets owned compliance but keep their regular maintenance of each asset - The addition of the assets needed to support the performance **Recommendation:** - Maintain assets routinely held each month e.g. maintenance to protect and safeguard these assets are free of viruses or anything detrimental to their use. - The addition of assets as necessary to support the performance felt able to improve services organization	
	7.2 Classification of Information	7.2.1 Classification Guidelines
	Finding: - Information can be sorted by criteria **Recommendation:** - The information obtained has been grouped based on the criteria of each subsequent process based on rules for later follow-up.	
		7.2.2 Labeling and handling of information
	Finding: - Information constraints created a plan for handling information **Recommendation:** - Planning and handling information to solve a problem needs to be a lesson. Therefore, we need a database of the same problem recurred, it would be easy to re-adjusted based on the experience.	

Table 10 - Finding and recommendation clause 8, security human resource.

Clause	Objective Control	Security Control
8. Security Human Resources	8.1 Before work	8.1.3 Terms and conditions of employment
	Finding: - Update operational standard organization working - Selecting human resources following the criteria and needs of the organization. **Recommendation:** - The need to upgrade in making operational standards and regulatory requirements of work includes prospective members of the organizations before work. - The need for an interview and some tests to determine the capabilities and criteria of the organization.	

Table 11 - Finding and recommendation clause 11, access control.

Clause	Objective Control	Security Control
11. Access Control	11.5 Operating System Access Control	11.5.3 Password Management System
	Finding: - There are conditions to change a user's password but no service password changes regularly. - Application stores passwords in encrypted form using a one-way encryption algorithm. **Recommendation:** - Forcing the user to change their password after a certain period of time and refusing to enter a password when the same user with previously used when changing the password. - Store passwords secure (encrypted) - Disconnecting or user access if there is no response for a certain period.	

5. Discussions

Almeida and Monev combine the COBIT 5 framework and ISO 27001 for information system security risk assessment and effective and efficient governance (Almeida et al., 2018), while Monev emphasizes tactical and DSS for risk security management (Monev, 2020). Tanovic combines ISO 20000 and ISO 27001 for assessing service management standards and information system security risks (Tanovic & Marjanovic, 2019), while Peciña combines ISO 31000 and ISO 27001 for physical and logical security management assessments (Peciña et al., 2011). This research used ISO 27001 and SSE-CMM, which can be empirically adopted to measure the information security of academic information systems and is proven (Kurniawan & Riadi, 2018). Another difference is the determination of clauses according to organizational needs. This research determines clauses on asset management, human resource security, and access control. AIS assessment using ISO 27001 in this research can determine information system security risks and the effectiveness and efficiency of academic systems in 3 clauses. The Academic Capability System shows asset management at level 3, human resource security at level 4, and access control at level 3, so that it can recommend improvements.

6. Conclusion

The results of information system security analysis in academic information systems use ISO-27001 clauses that meet maturity level standards, namely clauses on the acquisition, development, and maintenance of academic information systems. The level of information security maturity for academic information systems is still at the second layer of access control clauses (initial/ad hoc). The next research is to measure the quality of application performance with its maturity level.

References

Al-Dhahri, S., Al-Sarti, M., & Abdul, A. (2017). Information Security Management System. *International Journal of Computer Applications*, *158*(7), 29–33. https://doi.org/10.5120/ijca2017912851

Al-Karaki, J. N., Gawanmeh, A., & El-Yassami, S. (2022). GoSafe: On the practical characterization of the overall security posture of an organization's information system using smart auditing and ranking. *Journal of King Saud University - Computer and Information Sciences*, *34*(6), 3079–3095. https://doi.org/10.1016/j.jksuci.2020.09.011

Almeida, R., Lourinho, R., Da Silva, M. M., & Pereira, R. (2018). A model for assessing COBIT 5 and ISO 27001 simultaneously. *Proceeding - 2018 20th IEEE International Conference on Business Informatics, CBI 2018*, *1*(20), 60–69. https://doi.org/10.1109/CBI.2018.00016

Bani-Mustafa, T., Zeng, Z., Zio, E., & Vasseur, D. (2017). A framework for multi-hazards risk aggregation considering risk model maturity levels. *2017 2nd International Conference on System Reliability and Safety, ICSRS 2017, 2018-Janua*(2), 429–433. https://doi.org/10.1109/ICSRS.2017.8272859

Barafort, B., Mesquida, A. L., & Mas, A. (2017). Integrating risk management in IT settings from ISO standards and management systems perspectives. *Computer Standards and Interfaces*, *54*, 176–185. https://doi.org/10.1016/j.csi.2016.11.010

Barafort, B., Mesquida, A. L., & Mas, A. (2018). Integrated risk management process assessment model for IT organizations based on ISO 31000 in an ISO multi-standards context. *Computer Standards and Interfaces*, *60*, 57–66. https://doi.org/10.1016/j.csi.2018.04.010

Fazlida, M. R., & Said, J. (2015). Information Security: Risk, Governance and Implementation Setback. *Procedia Economics and Finance*, *28*(April), 243–248. https://doi.org/10.1016/s2212-5671(15)01106-5

Ferraiolo, K. (2000). The Systems Security Engineering Capability Maturity Model. *International Systems Security Engineering Association*, 64. https://csrc.nist.gov/csrc/media/publications/conference-paper/2000/10/19/proceedings-of-the-23rd-nissc-2000/documents/papers/916slide.pdf

Fomin, V. V., Vries, H. J. de, & Barlette, Y. (2008). ISO/IEC 27001 Information System Management Standard: Exploring The Reasons for Low Adoption. *Proceedings of The Third European Conference on Management of Technology (EUROMOT), September*.

Guerreiro, S., Ferreira, J. F., Fonseca, T., & Correia, M. (2022). Integrating an academic management system with blockchain: A case study. *Blockchain: Research and Applications*, *3*(4), 1–10. https://doi.org/10.1016/j.bcra.2022.100099

Królikowski, T., & Ubowska, A. (2021). TISAX - Optimization of IT risk management in the automotive industry. *Procedia Computer Science*, *192*(25), 4259–4268. https://doi.org/10.1016/j.procs.2021.09.202

Kurniawan, E., & Riadi, I. (2018). Security level analysis of academic information systems based on standard ISO 27002: 2003 using SSE-CMM. *ArXiv*, *abs/1802.03613*.

Lopez-Leyva, J. A., Kanter-Ramirez, C. A., & Morales-Martinez, J. P. (2020). Customized diagnostic tool for the security maturity level of the enterprise information based on ISO/IEC 27001. *Proceedings - 2020 8th Edition of the International Conference in Software Engineering Research and Innovation, CONISOFT 2020*, 147–153. https://doi.org/10.1109/CONISOFT50191.2020.00030

Ma, L., Liu, Y., & Ran, C. (2024). Framework for intellectual property information services in academic libraries: Example from the United States and China. *Journal of Academic Librarianship*, *50*(1), 102830. https://doi.org/10.1016/j.acalib.2023.102830

Marican, M. N. Y., Razak, S. A., Selamat, A., & Othman, S. H. (2023). Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review. *IEEE Access*, *11*(November 2022), 5442–5452. https://doi.org/10.1109/ACCESS.2022.3229766

Mohamad Stambul, M. A., & Razali, R. (2011). An assessment model of information security implementation levels. *Proceedings of the 2011 International Conference on Electrical Engineering and Informatics, ICEEI 2011*, *July*. https://doi.org/10.1109/ICEEI.2011.6021561

Monev, V. (2020). Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002. *2020 34th International Conference on Information Technologies, InfoTech 2020 - Proceedings*, *September*, 17–18. https://doi.org/10.1109/InfoTech49733.2020.9211066

Peciña, K., Estremera, R., Bilbao, A., & Bilbao, E. (2011). Physical and Logical Security management organization model based on ISO 31000 and ISO 27001. *Proceedings - International Carnahan Conference on Security Technology*, 1–5. https://doi.org/10.1109/CCST.2011.6095894

Roy, P. P. (2020). 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*, *53*(June), 27001–27003. https://doi.org/10.1109/NCETSTEA48365.2020.9119914

Shen, L., Du, X., Cheng, G., & Wei, X. (2021). Capability Maturity Model (CMM) method for assessing the performance of low-carbon city practice. *Environmental Impact Assessment Review*, *87*(January), 106549. https://doi.org/10.1016/j.eiar.2020.106549

Shi, X., Baba, T., Osagawa, D., Fujishima, M., & Ito, T. (2019). Maturity Assessment: A Case Study Toward Sustainable Smart Manufacturing Implementation. *Proceedings - 2019 IEEE International Conference on Smart Manufacturing, Industrial and Logistics Engineering, SMILE 2019*, *June*, 155–158. https://doi.org/10.1109/SMILE45626.2019.8965284

Syreyshchikovaa, N. V., Pimenova, D. Y., Mikolajczykb, T., & Moldovan, L. (2019). *2019_Information Safety Process Development According to ISO 27001.pdf* (pp. 278–285).

Tan, W., Sauser, B., & Ramirez-Marquez, J. (2010). Analyzing Component Importance in System Maturity Assessment. *IEEE Transaction on Engineering Management*, *58*(2), 275–294.

Tanovic, A., & Marjanovic, I. S. (2019). Development of a new improved model of ISO 20000 standard based on recommendations from ISO 27001 standard. *2019 42nd International Convention on Information and Communication Technology, Electronics and*

Microelectronics, MIPRO 2019 - Proceedings, *May 20*(42), 1503–1508. https://doi.org/10.23919/MIPRO.2019.8756843

Volk, D. R., & Mazanis, J. C. (2017). Sustainment maturity levels and health assessment metrics to drive supportability. *Proceedings - Annual Reliability and Maintainability Symposium*, *17*. https://doi.org/10.1109/RAM.2017.7889738

Yasin, M., Akhmad Arman, A., Edward, I. J. M., & Shalannanda, W. (2020). 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*, *2013*(95), 3–7. https://doi.org/10.1109/TSSA51342.2020.9310875.