Journal of Information Systems and Informatics
Vol. 6, No. 1, March 2024 e-ISSN: 2656-4882 p-ISSN: 2656-5935
DOI: 10.51519/journalisi.v6i1.668 Published By DRPM-UBD

Information Security Risk Management Web-Based Final Semester Summative Assessment Application Using ISO 27001:2013

Ananda Cipta Pamungkas[1], Wegi Salman Hulu[2], Rosalin Samihardjo[3]

[1,2,3]Information Systems Study Program, Faculty of Engineering, Widyatama University, Bandung, Indonesia
Email: [1]ananda.cipta@widyatama.ac.id, [2]wegi.salman@widyatama.ac.id, [3]rosalin.samihardjo@widyatama.ac.id

Abstract

Education is often understood as more than just teaching, but as the transfer of knowledge, transformation of values, and development of character with all related aspects. Digitalization of the need for information and communication technology is increasing to facilitate access to information systems. This research was conducted at SMAN 12 Bandung with the research objective being a form of evaluation of the implementation of ISO 27001:2013 in clause 4.1. up to 10.2 and Annex A is one of the efforts and efforts to improve the PSAS Website Application ISMS. The method used in this research is to collect data in the form of school documents, identify assets, carry out risk assessments, then carry out risk assessments. The methods used are field observations, interviews, and information processing. The research results show that the Risk Opportunity on the PSAS SMAN 12 Bandung Website Application is around 45%, while the risk severity is estimated at 47%, and the Risk Rating is 49%. In processing field observation data, it was concluded that 80% of Class X, XI, and XII. Meanwhile, the percentage related to the implementation and implementation of ISO/IEC 27001:2013 variable procedures on the PSAS SMAN 12 Bandung web application is 81.43%, which has been implemented and applied well. Meanwhile, the percentage of control implemented in the PSAS web ISMS at SMAN 12 Bandung is 100%. Based on these findings, an analysis was carried out using the PDCA (Plan, Do, Check, Act) method in accordance with ISO 27001:2013 standards and procedures to overcome ISMS problems on the Final Semester Summative Assessment Website Application at SMAN 12 Bandung.

Keywords: Risk Management, ISO/IEC 27001:2013, Information Security, ISMS

1. INTRODUCTION

Government regulations regarding information security stated in Ministerial Regulation No. 82 of 2012 concerning the Implementation of Electronic Systems and Transactions refer to information security management system standards [1] [2]. This regulation requires public service agencies to establish reliable and safe information security management, and carry out responsibilities in accordance with the provisions stated in the regulation [3][4]. Information technology

governance can be interpreted as steps to ensure information technology management supports and is in line with the business strategy implemented by the agency leader [5].

In carrying out the end-of-semester summative assessment website risk assessment, SMA Negeri 12 Bandung adopted a policy regarding information technology security that was still unclear, the school did not yet have a definite understanding of the extent of its readiness to face potential threats [6][7]. The actual risks that exist have not been properly identified, and the continuation of security gaps without proper control can cause disruption from both internal and external parties [8][9].

In terms of the various problems and limitations of existing problems, there are several problem formulations prepared within the framework of this research, including: How to apply the application of information and internet security to asset identification and risk management at SMAN 12 Bandung, and How to implement the concept of implementing ISO 27001:2013 towards the introduction of asset and risk management at SMAN 12 Bandung in the process of Odd Semester Final Summative Assessment activities.

This research is expected to provide an understanding of the importance of risk analysis, especially for school management and its relationship with school operational aspects. The aim is to provide information to SMA Negeri 12 Bandung regarding risks, threats and weaknesses of information technology that can be identified [10]. In addition, this research aims to provide solutions for protecting school information assets, by presenting recommendations that can be implemented by SMA Negeri 12 Bandung.

2. METHODS

This research was conducted at SMAN 12 Bandung which is located on Jl. Sekejati No.36, Kiaracondong, Bandung city, West Java Province. The aim of this research is a form of evaluation of the implementation of ISO 27001:2013 in clause 4.1. up to 10.2 and Annex A in an effort to improve the security of the school's End of Semester Summative Assessment Website Application. The method used in this research is to collect data in the form of school documents, identify assets, carry out risk assessments, then carry out risk assessments. The methods used are field observations, interviews and data processing. The method used can be seen in Figure 1 .

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

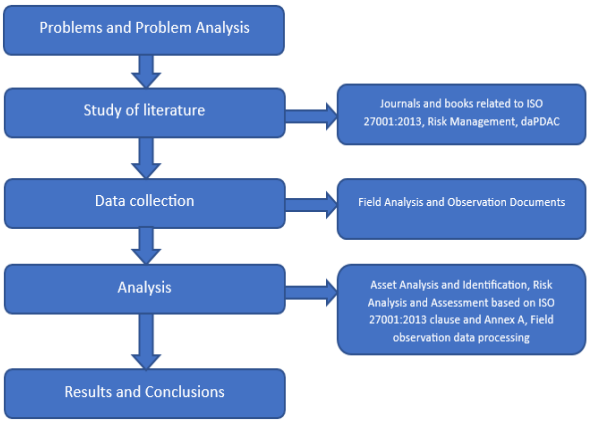

Figure 1. Research Framework

The problem recognition stage includes identifying problems that exist in the ISMS process at SMAN 12 Bandung. Next, the author conducted a literature study relating to all variables, methods and technical research carried out. After conducting a literature study, the author collected data in the form of information and physical and non-physical documents based on the ISO 27001:2013 variables that had been determined and carried out direct field observations in the process of implementing the end-of-semester summative assessment. After collecting data, the author carried out data and information analysis by carrying out asset identification, risk analysis, risk assessment and carrying out ISO/IEC 27001:2013 Statement of Applicability, and PDCA related to information and field observation data on the implementation of the ISMS on the end-of-semester summative assessment website application. SMAN 12 Bandung.

2.1 Asset Identification

In the asset identification process, there are several fields including ISMS asset category, name and description of ISMS assets, Container Type/Organizational Structure, Location and Status of ISMS assets related to planning, use and evaluation of Information Security Management System assets on the Final Summative Assessment Website Application Semester of SMAN 12 Bandung Academic Year 2023/2024. This identification is useful as an analysis of existing data and information in carrying out risk analysis and assessments related to ISO 27001:2013.

2.2 Risk Analysis and Assessment

Risk analysis in the Information Security Management System Website Application End of Semester Summative Assessment at SMAN 12 Bandung for

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

the 2023/2024 Academic Year by identifying risks that may occur, the parties analyzed who are affected by the risk, the opportunity for the risk to occur, the level of seriousness and severity of the risk if occur, ranking of risks that may occur, Mitigation or overcoming of risks if they occur, ISMS Implementation Plan, parties responsible for managing these risks, and the status of the ISMS information itself [11].

This risk analysis produces several risk assessments that can and may occur through a risk map which is prepared based on risk opportunities, risk seriousness, and ranking of risks that can and may occur. According to [12] the following are several methods for analyzing risk opportunities according to Table 1.

Table 1. Risk assessment based on Risk Probability

Risk Assesment	Risk Probability
5	High Likely
4	Likely
3	UnLikely
2	Veri UnLikely
1	Rare

Apart from risk assessment based on Risk Probability, several risk assessments via Risk Severity were also analyzed [13] according to Table 2.

Table 2. Risk assessment based on Risk Severity

Risk Assesment	Risk Severity
5	Fatality
4	Major Injuries
3	Minor Injuries
2	Veri Negligible Injuries
1	Insignificant

Apart from risk assessment based on Risk Probability and Risk Severity, several risk assessments are also analyzed through Risk Rating [14] according to Table 3.

Table 3. Risk assessment based on Risk Rating

Risk Assesment	Risk Rating
5	Extreme
4	High
3	Medium
2	Low
1	Very Low

2.3 Questionnaire Data Processing

Apart from the evaluation previously explained, this research details the results based on data obtained through questionnaires distributed widely and given to the management of the Final Semester Summative Assessment Website Application at SMAN 12 Bandung. This research adopts methods in accordance with ISO 27001 standards Clauses 4.1 to 10.2. The application of this method follows several approaches to the PDCA process, which is the approach mandated in the ISO 27001:2013 standard. The PDCA process consists of four steps, namely planning, implementing, evaluating, and taking corrective action [15].

a) Plan, this stage is an integral part of the implementation of the Information Security Management System (ISMS). This process involves planning and designing an Information Security Management System (ISMS). This implementation includes establishing commitments, policies, controls, procedures, work instructions, and other elements needed to run the ISMS in accordance with the desired objectives. In addition, a needs analysis was carried out to ensure the fulfillment of the necessary research requirements and needs.
b) Do or Do, this stage is an integral component of the process of implementing and operationalizing regulations or policies, controls, processes and procedures in the Information Security Management System (ISMS) which has been planned at the planning stage. At this stage, the focus is on preparing a questionnaire that will be submitted to the Website Application manager for summative evaluation at the end of the semester at SMAN 12 Bandung. The purpose of this survey is to collect data necessary for research. This survey aims to investigate the understanding and perception of managers of the SMAN 12 Bandung Final Semester Assessment Website Application regarding ISO 27001:2013 and how this standard is implemented in securing the SMAN 12 Bandung Website Application.
c) Check or checking. This stage involves monitoring the implementation of the Information Security Management System (ISMS), which includes evaluation and audit of the Information Security Management System (ISMS). In this phase, researchers manage the data obtained from the questionnaire in accordance with the provisions of the ISO 27001:2013 standard. The purpose of this evaluation and audit is to evaluate the performance of the ISMS, make improvements if necessary, and ensure that the implementation of the ISMS is running in accordance with established standards.
d) Act or Action. This stage involves a series of activities with the aim of improving or continuing to improve the Information Security Management System (ISMS). This action is carried out to ensure that the ISMS continues to develop and can adapt to technological developments and environmental changes. Apart from that, this stage also functions as a platform to provide suggestions and recommendations to perfect and

develop the ISMS to make it more effective in the future. Therefore, continuous improvement activities in the ISMS life cycle become a necessity.

3. RESULTS AND DISCUSSION

ISO 27001:2013 is a regulation that regulates the information security management system (ISMS) implemented in organizations. In the context of this research, these standards are used to assess the level of security of the Final Semester Summative Assessment Website Application at SMAN 12 Bandung, with a focus on clauses 4.1 to 10. Research respondents consisted of Class X, XI, and Manager of the Final Semester Summative Assessment Website Application at SMAN 12 Bandung. The research results show that the Risk Opportunity on the Final Semester Summative Assessment Website Application at SMAN 12 Bandung is around 45%, while the risk severity is estimated at 47%, and the Risk Rating is 49%. In processing field observation data, it was concluded that 80% of Class X, XI, and 2013. Based on these findings, an analysis was carried out using the PDCA method and approach stages in accordance with ISO 27001:2013 standards and procedures to overcome ISMS problems on the Final Semester Summative Assessment Website Application at SMAN 12 Bandung.

At the stage before implementing the assets identification, researchers collected data in the form of school documents in the form of reports on preparation, implementation, reflection and evaluation of activities related to the end-of-semester summative assessment objectives and the security of the PSAS information system at SMAN 12 Bandung.

3.1 Asset Identification

In the fourth stage related to this research, the researcher identified assets consisting of the asset category, description of the asset, type of user using it, location of the asset used, and asset status which was analyzed based on direct field observations, information on these assets can be seen in Table 4.

Table 4. Identification of ISMS Assets for Final Semester Summative Assessment Website Application

No	Category	Asset	Container Type/Organizational Structure	Location	Status
1	Hardware	Primary Laptop	Physical	ICT Room	Develop the system
2		Server	Physical	ICT Room	Organize the system
3		Tab	Physical	Ruang IT	Do the exam

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

No	Category	Asset	Container Type/Organizational Structure	Location	Status
4		Handphone Siswa (Android)	Physical	Siswa	Do the exam
5		Boot disk	Physical	Server	
6		CPU	Physical	Server	
7		Memory	Physical	Server	
8	Software	PSAS (Assessment Management System) application	Digital	pve Virtual Env	
9		Smart Elmu (Exam)	Digital	Drive storage	
10		Proxmox Virtual Environtment	Digital	pve Virtual Env	
11		Datacenter	Digital	pve Virtual Env	
12		Backup Data	Digital	pve Virtual Env	
13		PSAS Question Bank	Digital	PSAS (Assessment Management System) application	
14		PSAS Activity Attendance List	Physical	Committee Room	
15		PSAS Activity Minutes	Physical	Committee Room	
16		Late cards follow PSAS	Physical	Committee Room	
17	Information	Participant PSAS Card	Physical	Siswa	
18		Certificate of non-implementation of PSAS	Physical	Committee Room	
19		PSAS activity information letter	Physical	Ruang Wakil Kepala Sekolah	
20		Activity flyer	Digital	Sosial Media Sekolah	
21		Activity documentation	Digital	Aarchive School photos	
22		Snack Vouchers	Physical	Committee Room	
23	Infrastructure	Electricity	Physical	IT Center	

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

No	Category	Asset	Container Type/Organizational Structure	Location	Status
24		LAN	Physical	IT Center	
25		Network	Digital	Network Enterprise	
26		Network Enterprise	Digital	Network Server	
27		Aruba Network Management	Physical	IT Center	
28		Ruang Kelas	Physical	School Center	
29		Committee Room	Physical	School Center	
30	HUMAN RESOURCES	Person responsible	Headmaster	School Center	
31		Chief Executive	Deputy Principal for Curriculum	School Center	
32		Activity Auditor	TIM TPMPS	School Center	
33		Supervisor	Teacher	School Center	
34		Input edit Bank Soal	IT TEAM	School Center	
35		User	Student	School Center	
36		Technician	IT TEAM	IT Center	
37	STAKEHOLDER	Network Center	Internet Service Provider Company	Service Center	
38		SYSTEM DEVELOP	Internet Service Provider Company	Service Center	
39		Activity and Financial Reporting	Kantor Cabang Dinas	Service Center	
40		Documentation Reporting	PSMA Dinas Pendidikan	Service Center	
41		Finance report	Dinas Pendidikan	Service Center	
42		Training and Workshops	BBGP	Service Center	
43		Activity Supervision	Assistant Supervisor of the Education Department	Service Center	

According to Table 4, it can be concluded that 44.18% of assets are physical container type assets and 23.25% of assets are digital container type assets and 32.55% of the data above are other container type assets. This is proven, that ISMS is really needed in the planning, implementation, management and implementation of the web-based Final Semester Summative Assessment at SMAN 12 Bandung for the 2023/2024 Academic Year.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

3.2 Risk Analysis and Assessment

In Table 5, it can be concluded that the chance of risk occurring or Risk Probability on the ISMS Website Application Final Semester Summative Assessment of SMAN 12 Bandung for the 2023/2024 Academic Year is 45% based on existing information, data and observations. Meanwhile, regarding Risk Violence or Risk Severity, it was 47%, and the Risk Rating on the ISMS Website Application for the Final Semester Summative Assessment of SMAN 12 Bandung for the 2023/2024 Academic Year was 49%.

Table 5. Risk Analysis and Assessment Table

Risk probability	Qty	Total	Risk severity	Qty	Total	Risk rating	Qty	Total
Highly Likely	0	0	Fatality	0	0	Extreme	0	0
Likely	0	0	Major Injuries	1	4	High	2	8
Unlikely	7	21	Minor Injuries	7	21	Medium	7	21
Very Unlikely	12	24	Negligible Injuries	11	22	Low	10	20
Rare	0	0	Insignificant	0	0	Very Low	0	0
TOTAL	**19**	**45%**	**TOTAL**	**19**	**47%**	**TOTAL**	**19**	**49%**

3.3 Statement of Applicability Summary

Table 6. Statement of Applicability Summary

Area	ISO/IEC 27001 Controls	No of Applicable Controls	% Controls applicable	No of Applicable Controls Implemented	% Applicable Controls Implemented
A.5 Information security policy	2	2	100%	2	100%
A.6 Information security organization	7	7	100%	7	100%
A.7 Human resource security	6	6	100%	6	100%
A.8 Asset management	10	10	100%	10	100%
A.9 Access control	14	14	100%	14	100%
A.10 Cryptography	2	2	100%	2	100%
A.11 Physical and environmental security	15	15	100%	15	100%
A.12 Operational security	14	14	100%	14	100%
A.13 Communications security	7	7	100%	7	100%
A.14 Acquisition, development and maintenance of systems	13	13	100%	13	100%
A.15 Supplier relationships	5	5	100%	5	100%
A.16 Information security incident management	7	7	100%	7	100%
A.17 Information security aspects in business continuity management	4	4	100%	4	100%
A.18 Compliance	8	8	100%	8	100%
TOTAL	**81.43%**		**100%**	**81.43%**	**100%**

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

According to table 6, it can be interpreted that the percentage related to the Implementation and Execution of Procedures for the ISO/IEC 27001:2013 variable on the Final Semester Summative Assessment web application at SMAN 12 Bandung is 81.43%, which has been implemented and applied well. Meanwhile, the percentage of control applied in the web ISMS Summative Final Semester Assessment of SMAN 12 Bandung for the 2023/2024 Academic Year is 100%.

3.4 Field observation

3.4.1 Plan

This stage discusses needs analysis which includes two main aspects, namely data analysis and process analysis. In needs analysis, there are two main focuses, namely Data Analysis by collecting the necessary data related to evaluating the needs for the final semester summative assessment Website Application at SMAN 12 Bandung. The data obtained and collected includes information related to the latest technological development targets. The results of this data analysis are used to determine Website Application specifications that meet the needs of the target audience and enable them to compete effectively with competitors. Apart from that, Process Analysis involves identifying and analyzing business processes used in a company or organization. The main objective of this analysis is to identify how to implement business processes on a Website Application and how the Website Application can increase the efficiency and effectiveness of ongoing business processes. The results of this process analysis will be used to detail the specifications of the Website Application so that it meets the company's business process needs. By integrating data analysis and process analysis, this stage aims to ensure that Website Application requirements not only meet the expectations of the target audience and market competition, but also support and improve the effectiveness of the organization's business processes.

3.4.2. Do

This phase explains how to create a survey according to the ISO 27001: 2013 standard. This survey consists of two parts, one for class X, in Bandung. The stage of preparing a questionnaire in accordance with ISO 27001:2013 includes several things:

1) Identification of related needs. The first step in developing a survey is identifying and analyzing information needs. In this case, the researcher conducted a questionnaire to collect information regarding the security level of the Bandung Semester 12 Final Summative Assessment Website Application from class X, XI, and XII students as users and school principals represented by the Website Application manager.

2) Preparing several questions. After analyzing and identifying the needs needed to gather information, these questions must be prepared well and aimed at themes in accordance with the ISO 27001:2013 standard,
3) Questionnaire trial, the researcher conducts a questionnaire trial first to determine the validity and reliability of the questions to be submitted.
4) Dissemination of research questionnaires. After the questionnaire has gone through several stages of preparation, the questionnaire is distributed to Class X,
5) Data analysis, conduct data analysis to determine the security level of the Final Semester Summative Assessment Website Application at SMAN 12 Bandung in accordance with ISO 27001:2013 standards.

3.4.3. Check

This stage takes the form of a discussion by the SMAN 12 Bandung team regarding file evaluation and proof of survey completeness. Management or administrator of SMAN 12 Bandung proof of file evaluation stage and survey completion:

1) Carrying out the verification stage to ensure the authenticity of the data aims to check the validity of the data obtained from filling out the research questionnaire. This step aims to ensure that the data received from each respondent has been validated and has not been manipulated.
2) After data validation has been carried out, researchers need to carry out an analysis to determine the extent to which the security level of the Final Semester Summative Assessment Website Application at SMAN 12 Bandung has met the ISO 27001:2013 standard.
3) Identification of the problem formulation is carried out based on the results of the completed data analysis. Information regarding security problems on the Final Semester Summative Assessment Website Application at SMAN 12 Bandung can be identified.
4) After the problem has been identified, the next step is to create a report containing the results of data analysis, problem identification, and recommendations for improving information security on the Final Semester Summative Assessment Website Application at SMAN 12 Bandung.
5) Implementation of mitigation measures is carried out after preparing the report. Corrective actions must be implemented to address identified problems.
6) Monitoring and evaluation is carried out after corrective actions are implemented. Website performance is monitored to ensure that problems have been resolved and that the Information Security Management System (ISMS) on the website complies with the ISO 27001:2013 standard, as well as evaluating the results of the actions taken.

This questionnaire was used as an example with the participation of 50 students in classes X, XI and XII who answered 15 questions. Of the total 15 questions asked to respondents, 12 questions were answered with "yes" and 3 questions were answered with "no". Based on calculations, the percentage of "yes" responses obtained by calculation is (12/15) x 100 = 80%, while the percentage of "no" responses obtained by calculation is (3/15) x 100 = 20%.

This questionnaire was used as an example with the participation of 10 School Operators and Admins who answered 17 questions. Of the total 17 questions asked to respondents, 15 questions answered "yes" and 2 questions were answered "no". Based on calculations, the percentage of "yes" responses obtained by calculation is (15/17) x 100 = 88.2%, while the percentage of "no" responses obtained by calculation is (2/17) x 100 = 11.8%.

3.4.4. Act

This stage involves discussing improvements and deficiencies contained in the Final Semester Summative Assessment (PSAS) Website Application at SMAN 12 Bandung. This includes an evaluation of deficiencies, such as the absence of procedures related to Website Application management, such as guidelines for changing passwords, hierarchy of levels in the network, and other aspects. The existence of these procedures has important significance to ensure the management of the PSAS SMAN 12 Bandung Website Application in accordance with ISO 27001 standards. Therefore, it is recommended to first develop procedures related to Website Application management to create a more orderly structure that can be understood by all related parties. Based on the evaluation of the management of the Website Application for the Final Semester Summative Assessment of SMAN 12 Bandung which reached a level above 80%, it can be concluded that the management of the Website Application can be categorized as quite safe to safe in accordance with the ISO 27001:2013 standard.

4. CONCLUSION

This research shows that the risk on the Final Semester Summative Assessment (PSAS) Website Application at SMAN 12 Bandung reaches around 45%, with an estimated risk severity level of 47%, and a Risk Rating of 49%. Based on data processing from field observations, it can be concluded that 80% of Class X, XI and ISO 27001:2013 standard. The percentage related to the implementation and execution of procedures based on the ISO/IEC 27001:2013 variable on the PSAS SMAN 12 Bandung web application reached 81.43% which has been successfully implemented and implemented well. Meanwhile, the percentage of controls implemented in the PSAS SMAN 12 Bandung web Information Security Management System (SMKI) reached 100%. Thus, it can be concluded that security management on the Final Semester Summative Assessment Website

Application at SMAN 12 Bandung for the 2023/2024 Academic Year refers to the ISO 27001:2013 standard clause 4.1. up to 10.2 can be considered "SAFE".

REFERENCES

[1] R. Samihardjo, E. Amalia, and A. C. Pamungkas, "Analysis of Web-Based E-Learning Management System Business Proccess to Increase Learning Effectiveness at SMA ABC Bandung," *Brilliance: Research of Artificial Intelligence,* vol. 3, no. 2, pp. 329–337, 2023.

[2] E. Pratama, "Analisis Korelasi Eta Dalam Menentukan Hubungan Antara Tempat Wisata Dan Jumlah Wisatawan Mancanegara Di Kota Surakarta," *Mabha J.*, vol. 4, pp. 2746–8941, 2023.

[3] I. Epriatna, R. Wiguna Permana, I. Bukhori, and A. Hidayat, "Pemanfaatan Google Form sebagai alternatif efisiensi Pembiayaan Penilaian Sumatif Akhir Semester di SMP IT Nurul Wasilah," *Tadbir Muwahhid*, vol. 7, no. 1, pp. 1–12, 2023, doi: 10.30997/jtm.v7i1.6240.

[4] A. C. Pamungkas and E. Nurjanah, "Kolajar 12 (Komunitas Guru Pembelajar 12) Sebagai Sarana Meningkatkan Kompetensi Guru Di SMAN 12," *Jurnal Pendidikan Dan Keguruan,* vol. 2, no. 2, pp. 239–249, 2024.

[5] ATSDR, *Peraturan Pemerintah Republik Indonesia Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik*, vol. 66. 2012.

[6] ISO, "International Standard ISO / IEC Information technology — Security techniques — Information security management systems — Overview and," *ACM Work. Form. Methods Secur. Eng. DC, USA*, vol. 34, no. 19, pp. 45–55, 2018.

[7] A. Hartomo, "Menggunakan Ward & Peppard Pada Perusahaan Transshipment," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 10, no. 1, pp. 141–152, 2023, doi: 10.25126/jtiik.2023105604.

[8] E. Riana, M. Eka, S. Sulistyawati, and O. P. Putra, "Analisis Tingkat Kematangan (Maturity Level) Dan PDCA (Plan-Do- Check-Act) Dalam Penerapan Audit Sistem Manajemen Keamanan Informasi Pada PT Indonesia Game Menggunakan Metode ISO 27001 : 2013," *Journal of Information System Research (JOSH),* vol. 4, no. 2, pp. 632–640, 2023, doi: 10.47065/josh.v4i2.2552.

[9] A. Penting, "Standard Internasional ISO 27001 dan Manfaat Keamanan Informasi," pp. 7264126.

[10] J. Benyamin, M. Mualim, and E. P. Duarte, "Information Security Risk Management In Minimizing Cyber Threats At The Data Center And Communication Information Technology Of The National Cyber And Crypto Agency To Improve Cyber Defense And Security," *J. Manaj. Pertahanan*, vol. 9, no. 1, pp. 40–54, 2023.

[11] J. Primaranti, A. F. Setyowardhani, I. Nurlela, V. Ghrandiaz, and Y. Yulhendri, "Analisis Resiko Keamanan Informasi Website Repository

Digital Library Menggunakan Framework ISO/IEC 27001 & 27002: Studi Kasus Perguruan tinggi X," *J. Ris. Multidisiplin dan Inov. Teknol.*, vol. 2, no. 01, pp. 327–373, 2023, doi: 10.59653/jimat.v2i01.500.

[12] E. Tarakçı, A. M. Gönül, U. H. A. Ş, and U. H. A. Ş, "Risk Analysis and Assessment Framework for Cyber Security in Management Systems," *OHS ACADEMY*, vol. 6, no. 3, pp.165-172, 2023.

[13] S. Clarissa and G. Wang, "Assessing Information Security Management Using ISO 27001:2013," *Jurnal Indonesia Sosial Teknologi*, vol. 4, no. 9, pp. 1361–1371, 2023, doi: 10.59141/jist.v4i9.739.

[14] D. Widiyasti, I. Rusi, and F. Febriyanto, "Manajemen Risiko Keamanan Teknologi Informasi Menggunakan Metode Octave Allegro Dan Kontrol ISO / IEC 27001 : 2013 (Studi Kasus : PLN UP2D Kalimantan Barat)," *Coding Jurnal Komputer dan Aplikasi,* vol. 11, no. 02, 2023.

[15] A. Faza, "Evaluation the Information Security Management System : A Path Towards ISO 27001 Certification," *Journal of Information Systems and Informatics,* vol. 5, no. 4, pp. 1240–1256, 2023, doi: 10.51519/journalisi.v5i4.572.