Impact of Implementation of Information Security Risk Management and Security Controls on Cyber Security Maturity (A Case Study at Data Management Applications of XYZ Institute)

Endro Joko Wibowo
Electrical Engineering Department
University of Indonesia
Indonesia
endro.joko@ui.ac.id

Kalamullah Ramli*
Electrical Engineering Department
University of Indonesia
Indonesia
kalamullah.ramli@ui.ac.id

Abstract

Information security is an important concern for governments and industry due to the increase in cyber-attacks during Covid-19. The government is obliged to maintain information security in implementing an Electronic-Based Government System following Presidential Regulation of the Republic of Indonesia Number 95 of 2018. To overcome this problem, the XYZ Institute needs an approach to implementing information security risk management and information security controls. This study aims to risk identification, risk analysis, risk evaluation, risk treatment, risk acceptance, risk control, and analysis of cyber security maturity gaps in the domain of governance, identification, protection, detection, and response. ISO/IEC 27005:2018 as guidance for conducting risk assessments. The code of practice for information security control uses the ISO/IEC 27002:2013 standard and assessing maturity using the cyber security maturity model version 1.10 developed by the National Cyber and Crypto Agency of the Republic of Indonesia. The results show that the cyber maturity value increased from 3.19 to 4.06 after implementing 12 new security controls.

Keywords: Security Risk Management, information security controls, Cyber Security Maturity, ISO/IEC 27005:2018, ISO/IEC 27002:2013

Introduction

The Interpol ASEAN Cyberthreat Assessment 2021 report shows that there were incidents of data breaches that occurred in the ASEAN region in 2021. In October 2020 Data Breach on Redmard with a total of 1.1 million accounts had been compromised. September 2020, Ransomware targeted Hospitals and Businesses in Thailand. In June 2020 some 1.5 TB of sensitive data was stolen from a subsidiary of ST Engineering Aerospace. In June 2020 Data Breach on Indonesian e-commerce, namely Tokopedia, as many as 91 million user information was leaked (INTERPOL 2021). XYZ Institute of the Republic of Indonesia has a role to create, collect, and process a large amount of information. The XYZ Institute manages more than 800 electronic systems. One service that is strategic or critical is the application of

* Corresponding author

data management from 436,639 XYZ institutional units in the region with 50,901,460 unique data (XYZ Institute 2021). To maintain effective security risk management, it is necessary to identify and implement appropriate security controls (Payette et al. 2015). Information security risk management is required to protect this information and ensure confidentiality, integrity, and availability (Kure and Islam 2019). So that Security Risk Management and control of information security in the case study organization's critical assets are important aspects in providing protection, maintaining business process continuity, and increasing security maturity level (White 2011). Cyber Maturity level aims to assess the suitability of the work process of implementing information security systems in the organization. The cyber maturity model represents the maturity of all information security processes (Plan, Do, Check, and Act) based on the clauses of ISO/IEC 27005. In the Plan Phase, the Organization establishes policies, processes and procedures related to risk management. Do phase, Organization implements and runs. Check Phase, Organizations assess and measure process performance and Act Phase, organizations take action to improve and enhance information security systems (Fauzi et al. 2018). Cyber security maturity level can help institutions measure processes against implemented standards and evaluate how government institutions develop secure information systems (Payette et al. 2015). The information security standards used in this research are ISO/IEC 27005:2018, ISO/IEC 27002:2013, and Cyber Security Maturity Tool version 1.10 which was developed by the National Cyber and Crypto Agency of the Republic of Indonesia. ISO/IEC 27005:2018 is used as a guide for conducting an information security risk assessment (ISO/IEC 27005 2018). ISO/IEC 27002:2013 is used to guide information security control practices (ISO/IEC 27002 2013). Cyber Security Maturity Model is used as an evaluation tool to help organizations to measure the improvement of information security (Karabacak et al. 2016).

Previous research (Patino et al. 2018) discusses the information security design method using the ISO/IEC 27005:2018 standard. Institutions in government entities not only apply information security risk management guidelines but also need to implement steps to conduct risk analysis and evaluation. In various cases of best practice, the evaluation format and scale are presented in detail to identify assets, vulnerabilities, threats, and controls. The impact that is a consequence and the probability of the occurrence of a threat is a risk assessment format that is assessed quantitatively. Based on ISO 27001, the organization must establish and implement an information security risk assessment process. The organization ensures that repeated information security risk assessments will provide consistent, valid and comparable results. ISO 27001 regulates the information security risk management process which includes four stages: Plan, Do, Check, and Act (ISO/IEC 27001 2013) (ISO/IEC 27005 2018).The information security risk management process is based on ISO 27001 and Plan-Do-Check-Act (PDCA) model (Sensuse et al. 2020). The following is alignment between information security risk management processes and management systems; (1) The Plan activity process is in line with the context establishment, risk assessment, develop a risk management plan, risk acceptance stages. (2) The Do activity process is in line with the application of risk assessment stages. (3) The Check process is in line with the periodic monitoring and review of risk. (4) The Act process is in line with the stages of improving and maintaining the information security risk management processes. The author concludes that the achievement of organizational performance in managing information security can have a significant impact on the reliability and availability of a system due to the lack of a security risk management planning process. On research (García-Porras et al. 2018) contains the ISO/IEC 27005 standard with Calculation and risk treatment adopting a model with a quantitative approach. The quantitative approach makes it possible to calculate residual risk. The results of the implementation of the model by the researcher that the risk level is reduced by 53% when the control recommendations are implemented. the results of risk analysis on the most important asset priorities as consideration for decisions about information security in the organization where the research is carried out. Monev (2020) evaluated the maturity level of information security using the information security management system clause in ISO/IEC 27001:2013 and utilizes the information security control guidelines in ISO/IEC 27002:2013. The author concludes is that the final result of the study is metrics and recommendations for improving information security system management. The results of this evaluation can be used by policymakers to make strategic decisions on the performance of security strategies and operations. The assessment team evaluates each requirement in the sub-clauses and controls. The results of the author's evaluation provide control recommendations for improving information security. Recommendations for improvement aim to increase the maturity level. ISO/IEC 27002 is used as the basis for identifying best practices and selecting improvements. The results of the research from the application of risk assessment and information security control can increase the maturity value of information security maturity.

The reference master data for the XYZ institution's central data management application must be unique and singular. The results of data collection through the Basic Education Data form the basis for the publication of educational statistical data that provides access to information for stakeholders. Therefore, the data management application is a strategic service XYZ Institute's Data and Information Technology Center requires guidelines for implementing information security risk management. The institution will be able to identify, manage and mitigate information security threats. As an implementing institution, an electronic-based government system can provide security protection for confidentiality, integrity, availability, authenticity, and non-repudiation (Presidential Regulation 2018).

From these existing problems, a question arises "*Can the use of security controls following ISO/IEC 27002:2013 increase the level of maturity security?*". The authors carry out an initial security maturity assessment, risk assessment, selection of information security controls and assess the maturity of information security in data management applications in the domain of governance, identification, protection, detection, and response. The gap analysis of the cyber security maturity gap score is to ensure that cyber security management is managed, organized, reviewed regularly, and continuously. and methods for identifying assets, threats, security controls that have been implemented, identifying threats, assessing risks, and evaluating comprehensive information security risks in Data Management applications managed by the XYZ Institution. The information security risk management process based on ISO/IEC 27005:2018 consists of context establishment, risk identification, risk analysis, risk evaluation, risk treatment, and risk acceptance. This research is structured as follows: Part II discusses the literature review on information security risk management, ISO/IEC 27005:2018, ISO/IEC 27002:2013, and Cyber Security Maturity. Part III presents the research methodology. Part IV presents the results. Part V on discussion obtained through the case study. Part VI contains research conclusions.

Literature Review

Information Security Risk Management

Security Risk Management is a processing technique to identify and reduce risks to the company's business continuity to the organization's important information (Bergström et al. 2019). Risk management is a combination of profiling, assessment, evaluation, mitigation, validation, and monitoring activities on assets (Wheeler 2011). Tangible or intangible entities that are needed and have value to the organization are critical need to carry out comprehensive risk management. Assets that have vulnerabilities will be exploited by Threat actors (Kure and Islam 2019). The risk management process flow according to (Wheeler 2011) there are several stages. (1) Resource profiling, namely explaining resources and level of risk sensitivity. (2) Risk Assessment to identify and assess threats, vulnerabilities, and risks. (3) Risk decides to accept, avoid, transfer, or reduce risk. (4) Document stage of information security and business owners, namely documenting risk decisions including exceptions and mitigation plans. (5) Risk Mitigation is the stage for implementing a mitigation plan with specified controls. (6) Validation, namely testing controls to ensure the actual risk exposure is by the desired risk level. (7) The flow of the last stage is Monitoring and Audit, namely continuously tracking changes to the system that can affect the risk profile and conducting routine audits.

ISO/IEC 27005:2018

Standard ISO / IEC 27005:2018 is an International standard that provides guidelines for managing information security risks within an organization, in particular those that support the requirements of an information security management system (ISMS) following the ISO/IEC 27001 standard (Wangen et al. 2018) (Fahrurozi et al. 2020). Information security risk management standards apply to types of for-profit organizations and non-profit organizations (ISO/IEC 27005 2018). The risks that have been found will affect the aspects of the information security management system in the form of asset protection Confidentiality, Integrity, and Availability (CIA) so that information managed by risk owners must be protected and guaranteed. The risk assessment obtained will affect the effectiveness of risk treatment. Risk handling involves a cyclical process starting from assessing risk treatment, determining the acceptable residual risk level if the risk level is not acceptable then a new risk treatment is needed, and assessing the effectiveness of risk treatment. The information security risk management process uses the ISO/IEC 27005:2018 standard as shown Figure 1.

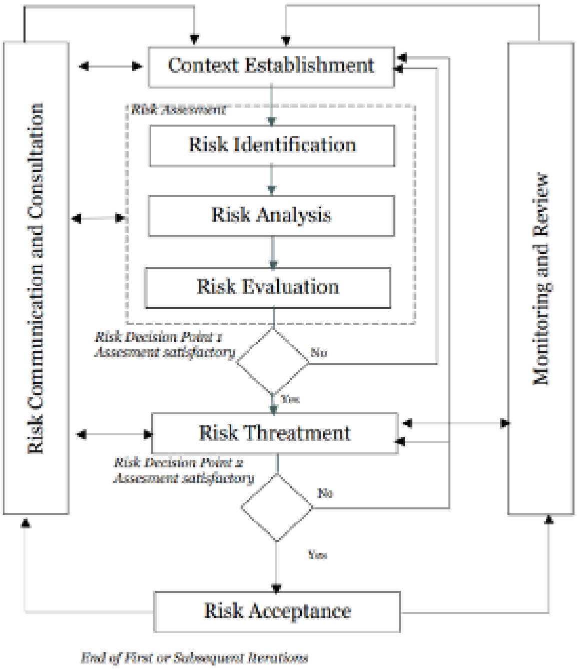
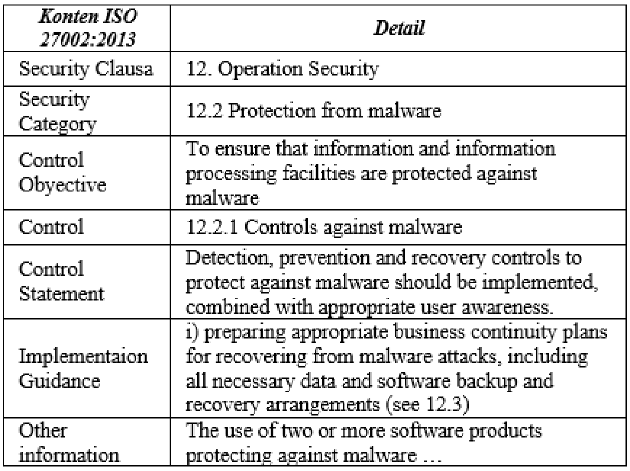


Figure 1. Information security risk management process (ISO/IEC 27005:2018)

ISO/IEC 27002:2013

International information security standard is used as an organizational guide for the selection of information security controls. Organizations can use the guidance in the ISO/IEC 27002:2013 document to reduce unacceptable risks (ISO/IEC 27002 2013). This standard is organized by 14 main security control clauses consisting of 35 major security categories and 114 controls. 114 controls are explained in detail with implementation guidelines and to achieve the fulfillment of the control objectives, suggestions for implementation are included (Gutiérrez-Martínez et al. 2015) (Fenz et al. 2016).



Konten ISO 27002:2013	*Detail*
Security Clausa	12. Operation Security
Security Category	12.2 Protection from malware
Control Obyective	To ensure that information and information processing facilities are protected against malware
Control	12.2.1 Controls against malware
Control Statement	Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.
Implementaion Guidance	i) preparing appropriate business continuity plans for recovering from malware attacks, including all necessary data and software backup and recovery arrangements (see 12.3)
Other information	The use of two or more software products protecting against malware …

Figure 2. Sample Of Steps For Implementation Of ISO/IEC 27002:2013 Controls

Figure 2 shows examples of implementation steps for ISO 27002:2013 controls (ISO/IEC 27002 2013). controls to protect against malware by ensuring that information and information processing facilities are protected from malware. Organizations implement controls by preparing appropriate business continuity plans for recovery from malware attacks, including all necessary data and software backups and recovery settings.

Cyber Security Maturity

Cyber Security Maturity is an institutional tool to measure cyber improvement so that it can improve cyber security management and monitor optimally and thoroughly. A company is judged to have achieved maturity in a particular discipline when a particular process when process is explicitly defined, managed, measured, controlled, and effective (Mayer and Fagundes 2009). The maturity model serves as an evaluation tool to assess the possibility of improving information security management. besides that it can be used as a means to assess and compare performance; a roadmap for model-driven improvement as well as a means to identify gaps and develop improvement plans (Rabii et al. 2020). There are three types of maturity models, namely progression maturity model, Capabilities Maturity Model (CMM) and Hybrid Maturity Model (Putra et al. 2020). The progression model describes a higher level of control, progress, progress, or evolution status. The capability model shows the extent to which certain practices have been established. The Hybrid Matuirty model is Combining the best features of the development model and capability maturity. This model supports the achievements in the progression model and adds to the ability to measure capabilities with the capabilities of the capability maturity model (Proença and Borbinha 2016). Model assesment analysis focuses on the application of the maturity model. To measure the maturity level of a particular reality, there must be a way to calculate the maturity level. This can be done by taking a self-assessment questionnaire or by following the full maturity assessment method. The cyber security maturity version 1.10 tool that has been developed by the National Cyber and Crypto Agency has 5 levels of information maturity categories. Level 1 is an initial implementation with an organizational description that is not measurable, inconsistent and has a high risk. Level 2 indicates that the organization is organized, inconsistent and repetitive. Level 3, the implementation carried out by the organization has been defined, namely being organized, consistent and conducting periodic reviews. Level 4 indicates that the organization has implemented information security in a managed manner, namely organized, periodic and ongoing reviews. Level 5 indicates that the organization has implemented optimally, namely automation, integration and culture of information security.

Research Methodology

This research phase consists of 6 phases, namely (1) the preparation phase, (2) the data collection phase, (3) the risk assessment phase, (4) the risk control phase, (5) the maturity level gap analysis phase. Figure 3 below describes and explains some of the phases of the research carried out.

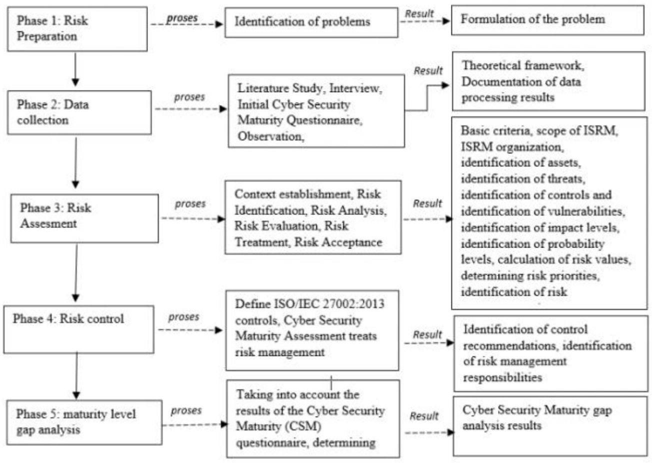

Phase 1: Risk Preparation
proses
Identification of problems
Result
Formulation of the problem
Phase 2: Data collection
proses
Literature Study, Interview, Initial Cyber Security Maturity Questionnaire, Observation,
Result
Theoretical framework, Documentation of data processing results
Phase 3: Risk Assesment
proses
Context establishment, Risk Identification, Risk Analysis, Risk Evaluation, Risk Treatment, Risk Acceptance
Result
Basic criteria, scope of ISRM, ISRM organization, identification of assets, identification of threats, identification of controls and identification of vulnerabilities, identification of impact levels, identification of probability levels, calculation of risk values, determining risk priorities, identification of risk
Phase 4: Risk control
proses
Define ISO/IEC 27002:2013 controls, Cyber Security Maturity Assessment treats risk management
Result
Identification of control recommendations, identification of risk management responsibilities
Phase 5: maturity level gap analysis
proses
Taking into account the results of the Cyber Security Maturity (CSM) questionnaire, determining
Result
Cyber Security Maturity gap analysis results

Figure. 3 Research Stages

Phase 1: Preparation Phase

The preparation of this research aims to define the problems that become priority needs in the Research Site. At this stage determine the scope and mapping of the organization as the object of research.

Phase 2: Data Collection Phase

The data collection phase was obtained by conducting online focus group discussions (FGD), online questionnaires, and analysis of existing documents. Respondents for interviews through online questionnaires were the head of the Management and Utilization of Information Technology and the Head of the Data Processing and Statistics Division. Next are two people from the management and utilization of information technolgy division and five people from the data processing and statistics division. First, by conducting a Focus Group Discussion to find out the conditions, goals, and targets that are planned to be achieved. Analysis of data processing application documents is carried out to find out detailed information and procedures in data processing applications. Questionnaires were distributed to seven interviewees from the management and utilization of information technology and the the data processing and statistics division to understand and confirm the types of risks that may occur in the the data processing system. The questionnaire is given using the cyber security maturity level assessment issued by the National Cyber Password Agency of the Republic of Indonesia. Cyber Security Maturity consists of 5 domains, 29 subdomains, and 267 questions, as shown in Table 1 below.

Table 1. Domain Cyber Security Maturity Versi 1.10

Domain	***Sub Domain***	***Number of Questions***
Governance	(a) Awareness, (b) Audit, (c) Control, (d) Compliance, (e) Policy and (f) Process	95
Identification	(a) Asset Management, (b) Inventory, (c) Management (d) Risk, (e) Priority, (f) Reporting and (g) Classification	34
Protection	(a) Network, (b) Applications, (c) Users, (d) Management and Assets, (e) Cloud and (f) Data	60
Detection	(a) Change, (b) Monitor, (c) Warning, (d) Notification, (e) Intelligence and (f) Reporting	46
Response	(a) Detention, (b) Countermeasures, (c) Recovery, (d) Post-incident Activities and (e) Reporting	32

Phase 3: Risk Assessment Phase

The Risk Assessment phase based on (ISO/IEC 27005 2018) consists of several domain processes, namely Context establishment, Risk Identification, Risk Analysis, Risk Evaluation, Risk Treatment, Risk Acceptance. Context establishment includes general considerations for determining the objectives of information security risk management as this affects the overall process and context formation in particular (ISO/IEC 27005 2018). The output of these risk management processes is risk evaluation criteria, impact criteria, risk acceptance criteria, and the scope of Information Security Risk Management and Organizational Information Security Risk Management. At this stage, the risk identification process produces several outputs, namely asset identification, threat identification, control identification, and vulnerability identification. Identified assets are assets that are the main source of business process information security (Al Fikri et al. 2019).The results at the stage of the risk analysis process are the identification of the level of impact, the identification of the level of possibility. The stages of the risk evaluation process result in the calculation of risk values and determining risk priorities. Risk treatment includes the identification of risk management plans and identification of control recommendations. Risk acceptance results in the identification of risk management satisfaction, identification of risk management responsibilities.

Phase 4: Risk Control Phase

This risk control stage is to determine the controls contained in ISO/IEC 27002:2013 and design the treatment for risk handling. ISO/IEC 27002 (2013) Define specific control statements to meet the control objectives and then proceed to the substance responsible for the implementation of these controls. The implementation of these controls takes about eight months for the information security maturity assessment to be carried out again.

Phase 5: Analysis Gap Cyber Security Maturity Score Phase

At this stage, the organization reassesses using the same version of the cyber security maturity model. The value of the final assessment result will be compared with the value of the initial assessment result before implementing the information security control recommendations. The result of the gap analysis is obtained from the maturity value of cyber security after a risk assessment, residual risk and information security control have been carried out. This stage aims to ensure that the success factors have been achieved, namely increasing the maturity level of cybersecurity and the effectiveness of security controls based on risk assessment.

Result

The research analysis is based on the gap in the value of the Cyber Security Maturity assessment and focuses on information security risk management planning steps based on the ISO/IEC 27005:2018 standard with information security controls based on the ISO/IEC 27002:2013 standard which will be explained as follows:

Context establishment

Determining the context of information security risk by establishing basic criteria, scope, and boundaries and organizing information security risk management. Includes general considerations for determining the objectives of information security risk management as they affect the whole process and the context in particular (ISO/IEC 27005 2018)(Putra and Mutijarsa 2021).

1. Basic criteria

The basic criteria specifications consist of risk evaluation criteria, impact criteria, and risk acceptance criteria (ISO/IEC 27005 2018). Impact criteria determine the xyz institute's loss rate. The impact criteria have five levels, namely very high, high, medium, low and very low, which are shown in Table 2 below.

Table 2. Basic Criteria

Score	Impact Level	Description
5	Very High	- Main business processes are interrupted and stopped for more than 24 hours - Unauthorized access to confidential data - Organizational data is damaged, lost and there is no backup - It harms the reputation and trust of the organization
4	High	- Main business processes are interrupted and stopped for 21-24 hours - Organizational data is damaged, lost and there is no backup - It harms the reputation and trust of the organization
3	Medium	- The organization's business processes stop for 4-20 hours and the main business processes are not interrupted - Organizational data is damaged or lost - Organizations have a data backup
2	Low	- The organization's business processes stop for 1-3 hours and the main business processes are not interrupted
1	Very Low	- The organization's business processes are not disrupted

2. The likelihood level of a threat even

Threat likelihood The organization determines the threat likelihood level based on the number of attacks and incidents concerning the threats facing the organization (Ghazouani et al. 2017). The likelihood of threat event occurring more than 100 times per year is included in the very high threat category with a threat level of 5. By using the parameters in Table 3 the organization can determine the frequency level of the threat.

Table 3. Likelihood Criteria Of Threat Event

Level	Threat	Likelihood of threat event	Criteria Description
5	Very High	Very likely	Could happen more than 100 times per year
4	High	Likely	Could happen between 10 and 100 times per year
3	Moderate	Moderate	Could happen between 1 and 100 times per year
2	Low	Unlikely	Could happen within 1 year
1	Very Low	Very Unlikely	Could happen within 5 years

Idenfication of Assets

30 assets have been identified in the data management application, which consists of 7 information assets (A1-A7), 3 software assets (A8-A10), 11 hardware assets (A11-A21), 4 services assets (A22-A25), 4 human assets (A26-A29, and 1 location asset (A30). Refers to Figure 4, each asset has an asset valuation level of 4 (very high), 3 (high), 2 (moderate), 1 (low) and 0 (very low). Determination of asset value based on Confidentiality, Integrity, and Availability (Ghazouani et al. 2017).

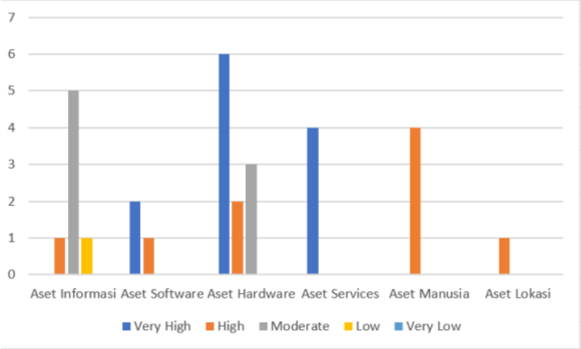


Figure 4. Types of Assets and Asset Valuation

Identification of threats

The results of interviews with informants indicate the types of potential threats to each infrastructure asset of the Student Education Basic Data Processing System and their level, vulnerability, or ease of exploitation and the level and existing controls that have been implemented that there are 87 types of threats in 30 assets, with the number of possible levels the occurrence of 45 very low, 30 low and 12 moderate threats on all assets and types of threats. Threat of 14% (T11), namely the occurrence of damage / loss of the device. One of the threats at 1% (T6) is the application has problems while running (application bug). The composition of threats on all assets can be seen in Figure 5 below. A list of threats to all assets and threat type code can be seen in appendix A.

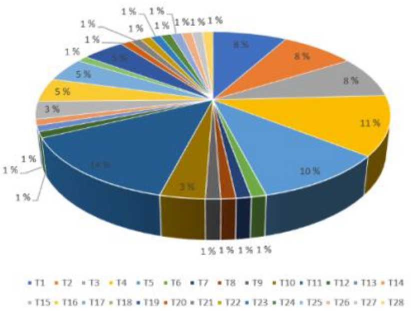


Figure 5. Frequency of each type of threat

Identification of vulnerabilities

Vulnerability is caused because the existing controls cannot reduce the threat, or the threat has no control. The process of identifying the vulnerabilities of 30 assets consists of 87 vulnerability scenarios with vulnerability levels including 78 Low levels and 9 medium levels.

Risk Evaluation

Risk Assessment is assessed quantitatively from Impact x Probability (Patino et al. 2018). The impact is a consequence of the emergence of a threat, while the level of risk shows an estimate of what will happen if the threat does come true. Very high-risk categories are 20 and 25. High risk values are 10,12,15, and 16. Medium-risk values are 5,6,8, and 9. Low-risk values are 3 and 4. Very low-risk values are 1 and 2 with the level of risk and risk mapping shown in the Table 4 and the Table 5.

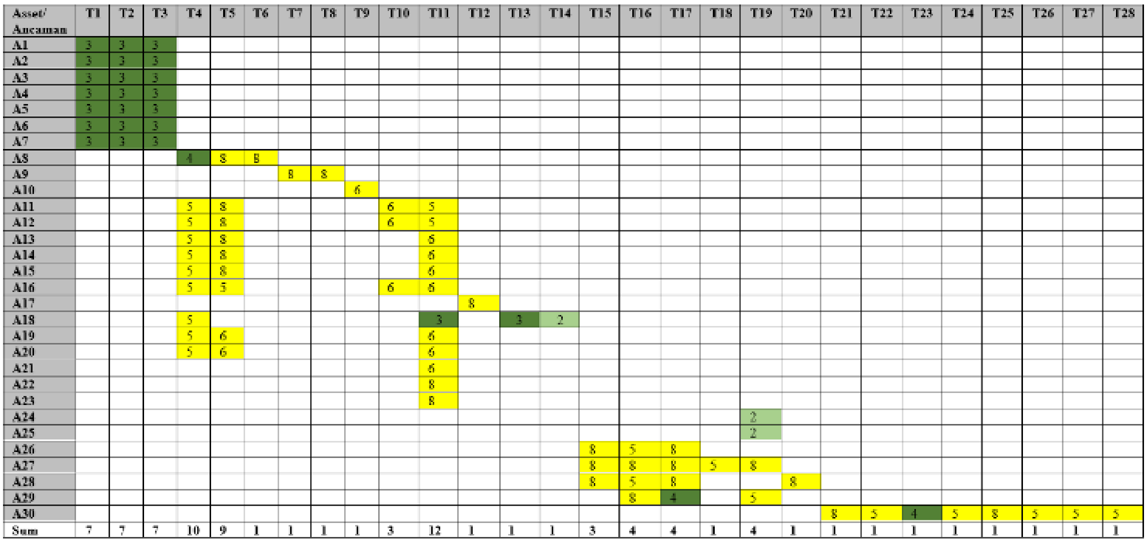
Table 4. Risk Level (Patino et al. 2018)

Risk Level	Impact x Probability
Very High	20-25
High	10-12-15-16
Medium	5-6-8-9
Low	3-4
Very Low	1-2

Table 5. Risk Matrix (Patino et al. 2018)

Risk Matrix/Map		Likelihood Level				
		1- Very unlikely	2- Unlikely	3-Moderate	4-Likely	5-Very likely
Impact Level	*1-Very Low*	1	2	3	4	5
	2-Low	2	4	6	8	10
	3-Medium	3	6	8	10	12
	4-High	4	8	12	16	20
	5-Very High	5	10	15	20	25

Table 5 above shows that the results of the assessment or determination of the risk level will be mapped into a risk mapping table according to the category. This mapping will help to see the overall level of risk in data management assets. If the impact level is high and the likelihood is level 3 or moderate, a risk value of 12 will be obtained with a high-risk value category refers to Figure 6.



Asset/ Ancaman	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	T16	T17	T18	T19	T20	T21	T22	T23	T24	T25	T26	T27	T28
A1	3	3	3																									
A2	3	3	3																									
A3	3	3	3																									
A4	3	3	3																									
A5	3	3	3																									
A6	3	3	3																									
A7	3	3	3																									
A8				4	8	8																						
A9							8	8																				
A10									6																			
A11				5	8					6	5																	
A12				5	8					6	5																	
A13				5	8						6																	
A14				5	8						6																	
A15				5	8						6																	
A16				5	5					6	6																	
A17												8																
A18				5							3		3	2														
A19				5	6						6																	
A20				5	6						6																	
A21											6																	
A22											8																	
A23											8																	
A24																			2									
A25																			2									
A26															8	5	8											
A27															8	8	8	5	8									
A28															8	5	8			8								
A29																8	4		5									
A30																					8	5	4	5	8	5	5	5
Sum	7	7	7	10	9	1	1	1	1	3	12	1	1	1	3	4	4	1	4	1	1	1	1	1	1	1	1	1

Figure 6. Risk value mapping

Risk Priority

The results of determining the level of risk found a total of 87 risk scenarios consisting of 23 risk scenarios medium with a risk score of 8. 13 risk scenarios medium with a risk score of 6, 22 risk scenarios medium with a risk score of 5. 3 risk scenarios medium with a risk score of 5. 3 risk scenarios low with a risk score of 4. 23 risk scenarios low with a risk score of 2 and 3 risk scenarios very low with a risk score of 2. The top fifty-eight risk scenarios in Table 6 need to be mitigated to reduce the risk value.

Table 6. Risk Priority

No	***Risk Code***	***Asset Code***	***Threat Code***	**Risk Value**	**Status**
1	R23	A8	T5	8	Mitigate
2	R24	A8	T6	8	Mitigate
3	R25	A9	T7	8	Mitigate
4	R26	A9	T8	8	Mitigate
5	R29	A11	T10	8	Mitigate
6	R37	A13	T5	8	Mitigate
7	R40	A14	T5	8	Mitigate
8	R43	A15	T5	8	Mitigate
9	R49	A17	T12	8	Mitigate
10	R61	A22	T11	8	Mitigate
11	R62	A23	T11	8	Mitigate
12	R65	A26	T15	8	Mitigate
13	R67	A26	T17	8	Mitigate
14	R68	A27	T15	8	Mitigate
15	R69	A27	T18	8	Mitigate
16	R70	A27	T19	8	Mitigate
17	R72	A27	T17	8	Mitigate
18	R73	A28	T15	8	Mitigate
19	R75	A28	T20	8	Mitigate
20	R76	A28	T17	8	Mitigate
21	R77	A29	T17	8	Mitigate
22	R80	A30	T21	8	Mitigate
23	R84	A30	T25	8	Mitigate
24	R27	A10	T9	6	Mitigate
25	R30	A11	T5	6	Mitigate
26	R34	A12	T5	6	Mitigate
27	R38	A13	T11	6	Mitigate
28	R41	A14	T11	6	Mitigate
29	R44	A15	T11	6	Mitigate
30	R47	A16	T5	6	Mitigate
31	R48	A16	T11	6	Mitigate
32	R55	A19	T5	6	Mitigate
33	R56	A19	T11	6	Mitigate
34	R58	A20	T5	6	Mitigate
35	R59	A20	T11	6	Mitigate
36	R60	A21	T11	6	Mitigate
37	R28	A11	T4	5	Mitigate
38	R31	A11	T11	5	Mitigate
39	R32	A12	T4	5	Mitigate
40	R33	A12	T10	5	Mitigate
41	R35	A12	T11	5	Mitigate
42	R36	A13	T4	5	Mitigate
43	R39	A14	T4	5	Mitigate
44	R42	A15	T4	5	Mitigate
45	R45	A16	T4	5	Mitigate
46	R46	A16	T10	5	Mitigate
47	R50	A18	T4	5	Mitigate
48	R54	A19	T4	5	Mitigate
49	R57	A20	T4	5	Mitigate
50	R66	A26	T16	5	Mitigate
51	R71	A27	T16	5	Mitigate
52	R74	A28	T16	5	Mitigate
53	R79	A29	T16	5	Mitigate
54	R81	A30	T22	5	Mitigate
55	R83	A30	T24	5	Mitigate
56	R85	A30	T26	5	Mitigate
57	R86	A30	T27	5	Mitigate
58	R87	A30	T28	5	Mitigate
59	R22	A8	T4	4	Accept
60	R78	A29	T19	4	Accept
61	R82	A30	T23	4	Accept
62	R1	A1	T1	3	Accept
63	R2	A1	T2	3	Accept
64	R3	A1	T3	3	Accept
65	R4	A2	T1	3	Accept
66	R5	A2	T2	3	Accept
67	R6	A2	T3	3	Accept
68	R7	A3	T1	3	Accept
69	R8	A3	T2	3	Accept
70	R9	A3	T3	3	Accept
71	R10	A4	T1	3	Accept
72	R11	A4	T2	3	Accept
73	R12	A4	T3	3	Accept
74	R13	A5	T1	3	Accept
75	R14	A5	T2	3	Accept
76	R15	A5	T3	3	Accept
77	R16	A6	T1	3	Accept
78	R17	A6	T2	3	Accept
79	R18	A6	T3	3	Accept
80	R19	A7	T1	3	Accept
81	R20	A7	T2	3	Accept
82	R21	A7	T3	3	Accept
83	R51	A18	T13	3	Accept
84	R52	A18	T14	3	Accept
85	R53	A18	T11	2	Accept
86	R63	A24	T19	2	Accept
87	R64	A25	T19	2	Accept

Risk Acceptance

Risk mitigation is carried out on 58 risk scenarios that have a medium value. The medium-risk value is reduced through the selection of security controls so that the residual risk can be assessed as an acceptable risk as shown in the Table 7. The information security control used is based on ISO/IEC

27002:2013 and the implementation details are adjusted to the control statement on the Cyber Security Maturity Tool used. Controls can provide several types of protection in aspects of awareness, policy, asset identification management, network protection, application protection, cyber-attack detection, post-incident response, and recovery.

Table 7. Risk Acceptance Analysis

Asset-Threat	*Control Security*	*Maturity Model organizational indicators*	*Responsible Area*
A8-T5	14.1.5 Business continuity management	- Implementing the Business Continuity Plan (BCP) - Determine the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) in the Business Continuity Plan (BCP) document	Data Processing and Statistics Division
A8-T6	18.2.3 Technical compliance review	- The Institutions form Red Teams and Blue Teams and conduct periodic testing at least once a year	Data Processing and Statistics Division
A9-T7	16.1.3 Reporting information security weaknesses	- Mitigation of minor incidents as soon as possible in coordination with related parties for the anticipation of larger follow-up incidents - Records of incidents and violations in the Institutions are kept and reported based on 6 months trend.	Data Processing and Statistics Division
A13-T5, A14-T5, A15-T5, A17-T12, A22-T11, A23-T11, A11-T5, A12-T5, A16-T5, A19-T5, A20-T5, A21-T11, T12-T11	17.2.1 Availability of information processing facilities	- The institution provides sufficient redundancy to recover from device failure and must be tested to ensure failover from one component to another is functioning as intended.	- Data Processing and Statistics Division - Management and Utilization of Information Technology Division
A25-T15,A27-T15, A27-T18, A27-T19, A26-T16, A28-T15	7.2.1 Management responsibilities (Human resource security)	- The institution cultivates awareness of information security - The institution makes a gap analysis to understand the skills and behaviors that employees do not have and uses this information to create a roadmap related to education baselines and training related to information security - The institution makes an information security awareness understanding program on an ongoing basis at least once a year to ensure an understanding of information security in the institution - The Institution provides awareness of personnel needs regarding terms and conditions of work that must be fulfilled by their responsibilities	- Data Processing and Statistics Division - Management and Utilization of Information Technology Division
A26-T17, A27-T17, A28-17, A29-17, A28-T20, A27-T16, A29-T16	7.2.2 Information security awareness,	- The Institution provides training on how to identify various forms of social engineering attacks - The Institution conducts phishing simulation at least annually	- Data Processing and Statistics Division

Asset-Threat	*Control Security*	*Maturity Model organizational indicators*	*Responsible Area*
	education and training	- The Institution provides training in making good secure code in software/application development - The Institution provides training on how to protect sensitive data, use restrictions, and document the processes that employees must follow - The Institution provides training for employees on how to properly identify and store, transmit, archive, and destroy sensitive information.	- Management and Utilization of Information Technology Division
A30-T21, A30-T25, A30-T22, A30-T24, A30-T26, A30-T27, A30-T28	11.1.4 Protecting against external and environmental threats	- Physical protection against natural disasters, dangerous attacks, or accidents should be designed and implemented. - The Institution has BCP and DRP documents.	- Data Processing and Statistics Division - Management and Utilization of Information Technology Division
A10-T9, A9-T8, A11-T10, A12-T10	12.2.1 Controls against malware (Protection from malware)	- The Institution has an incident handling policy and is in line with the policy of managing organizational continuity or business continuity planning - The Institution can detect information from cyber attacks in the form of tools/malware used - The Institution has systems in place to perform malicious code detection to detect, remove, and protect against malicious code - All endpoints including servers using antivirus	- Data Processing and Statistics Division - Management and Utilization of Information Technology Division
A13-T11, A14-T11, A15-T11, A16-T11, A19-T11, A20-T11, A11-T11	8.1.1 Inventory of assets	- The Institution conducts and maintains identification and inventory of Assets related to information and information processing facilities - The Institution compiles the identification of all assets based on the classification of criticality and has assigned a person responsible for each asset	-Data Processing and Statistics Division
A11-T4, A12-T4, A13-T4, A16-T4	10.1.1 Policy on the use of cryptographic controls 18.1.3 Protection of records	- The Institution establishes a policy on the use of cryptographic controls for the protection of information. - The Institution melindungi Data dengan persyaratan legislatif, peraturan, kontrak dan bisnis. - Backup data is encrypted and stored in a secure location both physically and non-physically	-Data Processing and Statistics Division
A14-T4, A15-T4, A16-T10, A18-T4, A19-T4, A20-T4	9.1.1 Access control policy	- The Institution ensures the use of complex passwords for all logins even manually access - The Institution ensures that passwords are changed regularly even if manually	-Data Processing and Statistics Division

Asset-Threat	*Control Security*	*Maturity Model organizational indicators*	*Responsible Area*
		- Information security policies and procedures are developed following the ISO 27001 framework and standards	

Maturity Gap Level Analysis

The maturity value obtained from strengthening information security in the areas of governance, identification, protection, detection, and response is 4.06. Level 4 indicates that the organization implements information security in an organized manner, implementing self-information security on a regular and ongoing basis. The result of the maturity value applied following the initial questionnaire before the information security risk assessment and information security control compliance with the risk value is 3.19. A comparison of the maturity values of each of the 5 domains and 29 subdomains before and after the implementation of control recommendations for information security risk mitigation is as in Table 8 below.

Table 8. Gap Analysis

Domain	*Sub Domain*	*Pre*	*Post*	*Gap*
Governance	Awareness	1.82	4.47	2.65
	Audit	2.92	3.83	0.91
	Control	3.48	3.91	0.43
	Compliance	2.26	3.79	1.53
	Policy	2.10	4.00	1.19
	Process	3.64	4.14	0.50
Identification	Asset Management	3.75	3.75	0.00
	Inventory	3.20	4.20	1.00
	Risk management	2.08	4.15	2.07
	Priority	4.20	4.20	0.00
	Reporting	3.33	4.00	0.67
	Classification	2.29	4.25	1.96
Protection	Network	3.86	4.00	0.14
	Application	2.80	4.00	1.20
	User	1.89	3.89	2.00
	Identity and Asset Management	3.00	3.85	0.85
	Cloud	4.00	4.29	0.29
	Data	2.71	4.29	1.58
Detection	Change	4.33	4.33	0.00
	Monitor	4.21	4.43	0.22
	Warning	3.38	4.13	0.75
	Notification	2.60	3.80	1.20
	Intelligence	3.45	3.82	0.37
	Reporting	3.80	3.80	0.00
Response	Detention	2.08	3.92	1.84
	Countermeasures	3.60	4.00	0.40
	Recovery	4.25	4.25	0.00
	Post-incident Activities	3.75	4.00	0.25
	Reporting	3.43	4.14	0.71
Maturity Level		**3.19**	**4.06**	**0.87**

Discussion

Results Based on the literature study that has been carried out and previous studies related to information security risk management ISO 27005:2018, code of practice for information security controls ISO 27002:2013, and cyber security maturity version 1.10 developed by the National Cyber and Crypto Agency that the implementation of information security controls ISO/IEC 27902 can increase the maturity level of cybersecurity. ISO/IEC 27002:2013 provides guidance for an organization's information security standards and information security management practices including the selection, implementation and management of controls taking into account the organization's information security risk environment (ISO/IEC 27005 2018) (ISO/IEC 27002 2013).

We conclude that with the research results found from 30 assets, 28 types of threats such as in Appendix A with 87 risk scenarios and the implementation of 12 new security controls for 58 medium-level risk scenarios, there is an increase in cybersecurity maturity of 0.87. The top three maturity subdomains with large gaps are Awareness 2.65, Risk Management 2.07, and User 2.00.

Our research can help XYZ Institute as a risk unit owner to improve the conditions for developing information security management by implementing a risk assessment process based on the ISO/IEC 27005:2018 standard as well as risk management and mitigation using the ISO/IEC 27002:2013 standard. we recommend that organizations increase the maturity level to be optimal. In subdomian compliance, organizations can sandbox all email attachments to prevent and analyze more security against malicious behavior. In the Intelligence subdomain, it is necessary to configure automatic threat intelligence feeds for preventive controls, such as IPS signature fixes, rule updates and other configurations. Organizations can run vulnerability scanning tolls automatically to detect cyber vulnerabilities. In the user subdomain, the organization must perform all encryption on all external storage media, the organization applies access settings (read/write) to USB devices/external storage media, and all endpoint devices used by users including servers must use antivirus.

Conclusion

This research focuses on the application of the information security risk management standard ISO/IEC 27005:2018, the code of practice for information security control ISO/IEC 27002:2013, and the cyber security maturity assessment version 1.10 developed by National Cyber and Crypto Agency of the Republic of Indonesia. Limitation of research on one of the strategic applications of government at the XYZ Institute of the Republic of Indonesia with the stages of identification, risk analysis, risk evaluation, risk treatment, risk acceptance, risk control, and gap analysis of Cyber security maturity. From this research, it can be concluded that risk control with a code of practice for information security control ISO 27002:2013 can increase the cyber maturity value of an organization from a maturity value of 3.19 to 4.06. At maturity level 4 the organization ensures that cyber security management is managed, organized, reviewed regularly and continuously.

This research resulted in 87 scenarios of medium risk, low risk, and very low risk. 29 risk scenarios are still in the category of institutional risk acceptance. 58 of the 87 risk scenarios obtained from the assessment have a medium risk level with a risk value of 5, 6, and 8. The institution mitigates risk at a medium level by implementing 12 new controls consisting of 30 implementation instructions.

References

Al Fikri, M., Putra, F. A., Suryanto, Y., and Ramli, K. 2019. “Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency,” in *Procedia Computer Science* (Vol. 161), Elsevier B.V., pp. 1206–1215. (https://doi.org/10.1016/j.procs.2019.11.234).

Bergström, E., Lundgren, M., and Ericson, Å. 2019. “Revisiting Information Security Risk Management Challenges: A Practice Perspective,” *Information and Computer Security* (27:3), Emerald Group Holdings Ltd., pp. 358–372.

Fahrurozi, M., Tarigan, S. A., Tanjung, M. A., and Mutijarsa, K. 2020. “The Use of ISO/IEC 27005: 2018 for Strengthening Information Security Management,” in *Proceedings of the 12th*

International Conference on Information Technology and Electrical Engineering, Institute of Electrical and Electronics Engineers Inc., October 6, pp. 86–91.

Fauzi, R., Supangkat, S. H., and Lubis, M. 2018. "The Pdca Cycle of ISO/IEC 27005:2008 Maturity Assessment Framework," in *Communications in Computer and Information Science* (Vol. 886), Springer Verlag, pp. 336–348.

Fenz, S., Plieschnegger, S., and Hobel, H. 2016. "Mapping Information Security Standard ISO 27002 to an Ontological Structure," *Information and Computer Security* (24:5), Emerald Group Publishing Ltd., pp. 452–473.

García-Porras, C., Huamani-Pastor, S., and Armas-Aguirre, J. 2018. "Information Security Risk Management Model for Peruvian SMEs," in *Proceedings of the 2018 IEEE Sciences and Humanities International Research Conference (SHIRCON): Lima, Peru, 20-22 November 2018*. (https://doi.org/10.1109/SHIRCON.2018.8592994).

Ghazouani, M., Medromi, H., and Moussaid, L. 2017. "Design and Implementation of a Comprehensive Information Security Risk Management Tool Based on Multi-Agents Systems," *International Journal of Applied Information Systems* (12:7), Foundation of Computer Science, pp. 1–8. (https://doi.org/10.5120/ijais2017451711).

Gutiérrez-Martínez, J., Núñez-Gaona, M. A., and Aguirre-Meneses, H. 2015. "Business Model for the Security of a Large-Scale PACS, Compliance with ISO/27002:2013 Standard," *Journal of Digital Imaging* (28:4), Springer New York LLC, pp. 481–491.

INTERPOL. 2021. "ASEAN Cyberthreat Assessment 2021 Key Cyberthreat Trends Outlook From The Asean Cybercrime Operations Desk." (https://www.interpol.int/).

ISO/IEC 27001. 2013. "Informaiton Security Management System, ISO/IEC 27001:2013(E)."

ISO/IEC 27002. 2013. "Code of Practice for Information Security Controls, ISO/IEC 27002:2013(E)."

ISO/IEC 27005. 2018. "Information Security Risk Management, ISO/IEC 27005:2018(E)."

Karabacak, B., Yildirim, S. O., and Baykal, N. 2016. "A Vulnerability-Driven Cyber Security Maturity Model for Measuring National Critical Infrastructure Protection Preparedness," *International Journal of Critical Infrastructure Protection* (15), Elsevier B.V., pp. 47–59. (https://doi.org/10.1016/j.ijcip.2016.10.001).

Kure, H. I., and Islam, S. 2019. "Assets Focus Risk Management Framework for Critical Infrastructure Cybersecurity Risk Management," *IET Cyber-Physical Systems: Theory and Applications* (4:4), Institution of Engineering and Technology, pp. 332–340.

Mayer, J., and Fagundes, L. L. 2009. "A Model to Assess the Maturity Level of the Risk Management Process in Information Security," in *2009 IFIP/IEEE International Symposium on Integrated Network Management-Workshops, IM 2009*, pp. 61–70.

Monev, V. 2020. "Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002," in *International Conference on Information Technologies (InfoTech-2020) : Proceedings of the 34th Edition of the InfoTech Conference : 17th-18th September 2020, St. St. Constantine and Elena Resort, Varna, Bulgaria*. (https://doi.org/10.1109/InfoTech49733.2020.9211066)

Patino, S., Solis, E. F., Yoo, S. G., and Arroyo, R. 2018. "ICT Risk Management Methodology Proposal for Governmental Entities Based on ISO/IEC 27005," in *2018 5th International Conference on EDemocracy and EGovernment, ICEDEG 2018*, Institute of Electrical and Electronics Engineers Inc., June 4, pp. 75–82. (https://doi.org/10.1109/ICEDEG.2018.8372361).

Payette, J., Anegbe, E., Caceres, E., and Muegge, S. 2015. "Secure by Design: Cybersecurity Extensions to Project Management Maturity Models for Critical Infrastructure Projects," *Technology Innovation Management Review* (Vol. 5).

Presidential Regulation. 2018. "Regulation Of The President Of The Republic Of Indonesia Number 95 Of 2018 Concerning Electronic-Based Government Systems." (https://peraturan.bpk.go.id/Home/Details/96913/perpres-no-95-tahun-2018).

Proença, D., and Borbinha, J. 2016. "Maturity Models for Information Systems - A State of the Art," in *Procedia Computer Science* (Vol. 100), Elsevier B.V., pp. 1042–1049.

Putra, A. P. G., Humani, F., Zakiy, F. W., Shihab, M. R., and Ranti, B. 2020. "Maturity Assessment of Cyber Security in the Workforce Management Domain: A Case Study in Bank Indonesia," in *2020 International Conference on Information Technology Systems and Innovation, ICITSI 2020*

- *Proceedings*, Institute of Electrical and Electronics Engineers Inc., October 19, pp. 89–94. (https://doi.org/10.1109/ICITSI50517.2020.9264982).

Putra, I. M. M., and Mutijarsa, K. 2021. "Designing Information Security Risk Management on Bali Regional Police Command Center Based on ISO 27005," in *3rd 2021 East Indonesia Conference on Computer and Information Technology*, *EIConCIT 2021*, Institute of Electrical and Electronics Engineers Inc., April 9, pp. 14–19. (https://doi.org/10.1109/EIConCIT50028.2021.9431865).

Rabii, A., Assoul, S., Ouazzani Touhami, K., and Roudies, O. 2020. "Information and Cyber Security Maturity Models: A Systematic Literature Review," *Information and Computer Security*, Emerald Group Holdings Ltd., pp. 627–644.

Sensuse, D. I., Syahrizal, A., Aditya, F., and Nazri, M. 2020. "Information Security Risk Management Planning of Digital Certificate Management Case Study: Balai Sertifikasi Elektronik," in *2020 5th International Conference on Informatics and Computing*, *ICIC 2020*, Institute of Electrical and Electronics Engineers Inc., November 3. (https://doi.org/10.1109/ICIC50835.2020.9288593).

Wangen, G., Hallstensen, C., and Snekkenes, E. 2018. "A Framework for Estimating Information Security Risk Assessment Method Completeness: Core Unified Risk Framework, CURF," International Journal of Information Security (17:6), Springer Verlag, pp. 681–6.

Wheeler, E. 2011. *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up*, (1st ed.).

White, G. B. 2011. "The Community Cyber Security Maturity Model," in *2011 IEEE International Conference on Technologies for Homeland Security*, *HST 2011*, pp. 173–178.

XYZ Institute. 2021. "The Application of Data Management." (https://sub.xyzinstitute, accessed September 5, 2021).

Appendix A – Threat Types

Threat Type Code	Statement
T1	Abuse of Rights (Modify stored files, retrieve files without permission, access by unauthorized parties)
T2	Damage/loss of data (Physical document)
T3	Stored data (physical document) is read by unauthorized parties
T4	Abuse of Rights (Modifying apps, infiltrating malware, stealing account passwords, attacks to get passwords)
T5	Application cannot be used (app error, application cannot be accessed, application is dead, network connection is lost)
T6	Application problems when running (application bug)
T7	Unusable Operating System (OS Crash)
T8	Operaing System not running normally caused by malware
T9	Antivirus function is not running / Out of Date
T10	The occurrence of damage / loss of data
T11	Device damage/loss occurs
T12	UPS does not work when the power goes out
T13	Infected with malware
T14	Laptop can't be used/error
T15	vailability of personnel
T16	Abuse of authority
T17	Data leaks (eg caused by Social engineering)
T18	Team assignment
T19	Trouble using/operating the application system
T20	Imperfect system development
T21	Flood
T22	Earthquake
T23	Thunderstorm
T24	Fire
T25	Pandemic
T26	Terrorism
T27	Theft
T28	Labor Dispute

How to cite:
Wibowo, E. J., Ramli, K., 2022. “ Impact of Implementation of Information Security Risk Management and Security Controls on Cyber Security Maturity (A Case Study at Data Management Applications of XYZ Institute),” *Jurnal Sistem Informasi (Journal of Information System)* (18:2), pp. 1-17.