Integrated Methodology for Information Security Risk Management using ISO 27005:2018 and NIST SP 800-30 for Insurance Sector

Arief Prabawa Putra[1], Benfano Soewito[2]
Computer Science Department-BINUS Graduate Program-Master of Computer Science, Bina Nusantara University, Jakarta, Indonesia 11480[1, 2]

***Abstract*—The development of Information and Communication Technology (ICT) in the Industrial Revolution 4.0 era shows very fast and disruptive developments that encourage increased use of Information Technology (IT) services within organizations. However, there is a risk of creating vulnerabilities and threats to owned information systems. Plans and strategies are required to implement information security risk management to address vulnerabilities in threat events. This research is a case study of the Enterprise Resource Planning System in the Insurance Sector. The proposed methodologies for integrating information security risk management using ISO/IEC 27005:2018 as a risk management framework and NIST SP 800-30 Rev. 1 as guidance for risk assessments. The risk evaluation stage is the process of comparing the results of the risk analysis with the risk criteria to then determine whether the risk rating is acceptable or tolerable. For risk treatment and control using the ISO/IEC 27002:2022 framework.**

***Keywords*—Risk management; information security; ISO/IEC 27005; NIST SP 800-30; ISO/IEC 27002**

I. Introduction

The adoption of information and communication technology (ICT) during the fourth industrial revolution 4.0 shows very rapid and disruptive advances that support the growth of information technology services [1]. The use of ICT affects the development of a country through the development of the dissemination of knowledge, especially from developed and developing countries, and through innovations [2]. Almost all enterprises use ICT to obtain information or process data more quickly, precisely, and accurately [3].

However, along with the use of the internet, there are many sources of threats that come from inside and outside the organization. In different parts of the world, the number of cyberattacks is growing at an alarming rate and causing financial losses [4]. This can threaten the continuity of business activities in the organization, including the insurance sector.

ZZZ Insurance is part of the government of the Indonesian insurance sector, which uses an Enterprise Resource Planning (ERP) system to run its business. ERP is an integrated system used by organizations to manage day-to-day business activities, such as financial and accounting, cash management, procurement, and asset management. Their system integrates not only internal parties but also external parties, such as health social security agencies, hospitals, population and civil registration agencies, and aggregators. One aspect of ICT that needs to concern every organization is information security. Information security can be formed by implementing controls, which include policies, processes, procedures, organizational structures, and functions of software and hardware [5]. These controls need to be implemented, monitored, reviewed, and required to ensure security and achieve the goals of the business organization.

Therefore, steps are needed in detecting vulnerabilities to threats inside and outside the organization. Therefore, procedures must be made to discover vulnerabilities to both internal and external threats. In addition, the importance of implementing organizational risk management in the software lifecycle is to produce proper supervision and responsibility and increase effectiveness and efficiency [6]. Planning and strategy are needed to overcome these vulnerabilities if a risk or threat occurs.

The need for planning and strategies to overcome these vulnerabilities in the event of a risk or threat if it disrupts Business Continuity (BC) [7]. Implementing Business Continuity Planning (BCP) is critical in an organization to anticipate if a disaster occurs and ensure that the business can continue to operate, or at the very least, that the organization can continue to provide its services after the disaster [8].

Therefore, it is necessary to implement information security risk management in enterprise systems organizations. Many standards are used in the implementation of risk management, including ISO 27005, which is widely applied in profit and non-profit organizations in other countries. Based on recommendations from another study, ISO 27005 is one of the international standards that is easy to implement in providing guidelines for information security risk management [9], [10]. Other studies also use the NIST 800-30 standard, where integrating qualitative and quantitative methodologies to give accurate and reliable risk data for decision making is the optimal method for risk assessment [11].

The purpose of this research was to conduct an information security risk assessment using ISO/IEC 27005:2018 as a risk management framework and NIST SP 800-30 revision 1 as a reference matrix of qualitative and quantitative risk levels. In accordance with the ISO/IEC 27002:2022 framework, the recommended controls include risk treatment and risk acceptance. This guideline is used to determine and implement information security risk

management controls inside an information security management system (ISMS) based on ISO/IEC 27001 [12].

II. Literature Review

A. Risk Management

Risk management is the process of identifying risks, assessing their relative magnitudes, and taking steps to reduce them to an acceptable level [13]. Information security risk management is a practical step in managing the risk of an organization's information security and aims to provide protection for organizational information and assets [14]. Risk management has three main processes: risk identification, risk assessment, and risk control.

The implementation of risk management in non-profit organizations provides several benefits, including planning basic information technology resources, providing decision-making support systems for leaders, and improving operational performance in terms of the maturity level of the risk management process. The combination of risk management processes based on ISO 31000:2018 and ISO 9001:2015 aims to provide guidelines for risk management principles and their application processes at the organizational, strategic, and operational levels [15]. Implementation of Enterprise Resources Planning (ERP) in the organization will increase the added value of the organization and support decision-making management [16].

Several other studies regarding the application of risk management standards in government agencies include the design of information security management for data communication applications at the XYZ Institute using ISO 27005 and NIST SP-800-30 [17]. Information security risk assessment with a combination of ISO 27005 information security standards and National Institute of Standards and Technology (NIST) SP 800-30 revision 1 adapted to organizational conditions [18]. The importance of conducting a cybersecurity risk assessment of the heart of electronic devices to determine the severity of the threat, prioritize the most significant risks and ensure effective risk management using a combination of ISO/IEC 27005 and NIST SP 800-30 [19]. The implementation of information security risk management (ISRM) in government agencies at the Bali Regional Police regarding System-Based Electronic Governance (EBGS) is an attempt to protect the risk of valuable assets [20]. In the industrial era 4.0, cloud computing has become widely used in the government sector, so security is now part of risk management [21]. The proposed cloud computing security model includes data security, risk assessment, regulation, compliance, and requirements.

An organization knows the importance of implementing risk management and making it the main step in minimizing the risks that will occur. The successful implementation of risk management in government agencies is influenced by several factors, namely risk management, policy development, and policy compliance [22].

B. ISO/IEC 27005

ISO/IEC 27005 is part of the ISO 27000 series. ISO 27005:2018 is a standard used to provide guidance for information security risk management [14]. ISO 27005 supports the general concepts described in ISO 27001 and is designed to assist in the proper implementation of information security based on a risk management approach. ISO 27005 has stages, namely context establishment, risk assessment (risk identification, risk analysis, risk evaluation), risk treatment, risk acceptance, risk communication and consultation, and monitoring and review.

C. NIST SP 800-30

NIST (National Institute of Standards and Technology) Special Publication (SP) 800-30 is a guide that aims to provide risk assessment of organizational and government information systems and is a complement to NIST SP 800-39 guidelines. The latest version of NIST SP 800-30 is revision 1. The risk assessment approach for NIST SP 800-39 revision 1 is supported by security standards and other guidelines to manage information security risks. The risk assessment approach to NIST SP 800-39 revision 1 is supported by security standards and other guidelines to manage information security risks [23]. NIST SP 800-30 can be used to complement the ISO 27005 standard in conducting risk assessments.

NIST 800-30 provides a basis for the development of an effective risk management program, as well as a definition and practical guidance for assessing and mitigating a risk that exists in an IT system. This framework has nine steps of risk management activities, starting with system characterization, threat identification, vulnerability identification, control analysis, likelihood determination, impact analysis, risk determination, control recommendations, and the results document of the risk assessment report.

III. Research Design

This research uses a case study of ZZZ Insurance ERP system. As seen in Fig. 1, the proposed method uses the ISO/IEC 27005:2018 framework as the main risk management framework is integrated with the NIST SP 800-30 revision 1 risk assessment guideline. Recommendations for control using are the ISO/IEC 27002 framework.

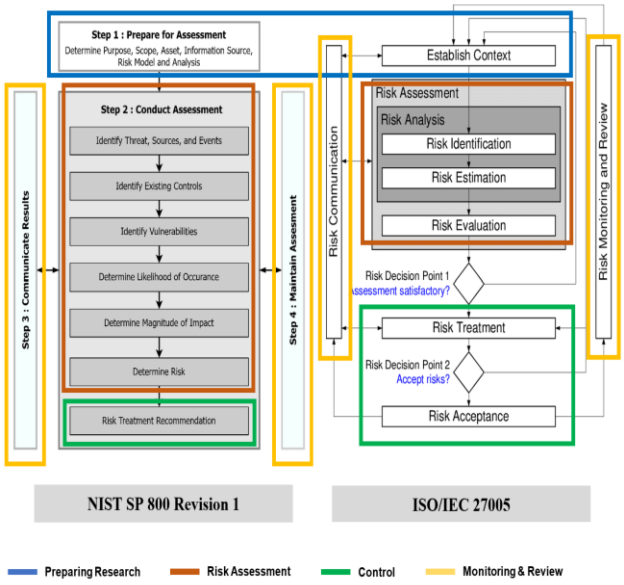

Fig. 1. Integrated methodology.

Beginning with research preparation includes identifying problems, collecting data, and context organization. In identifying problems, it is necessary to explain the problems faced by the organization, which are presented in the form of background and problem formulation, as well as solutions to the problems faced, which are presented in the form of goals and benefits.

The next stage is the collection of data obtained from document reviews, interviews, Forum Group Discussions (FGD), and observations. Document review is conducted to understand the organization in detail. During the interviews and FGD stages, it was conducted to find out the conditions and needs for information security in the organization.

Next, define the context of the organization to consider the impact that both internal and external factors have on the company's operational activities and its ability to achieve targets. The risk management process must be aligned with the corporate culture, processes, structure, and strategy. To prepare a risk assessment, it is necessary to first set the organizational context.

Risk assessment is a structured approach to identifying and analyzing uncertainties that exist in the achievement of organizational goals. Based on interviews with risk owners and IT risk officers in the organization, risk assessment aims to:

- Recognize the risks that may occur in the organization.
- Understand the risk so that the significance of the risk can be assessed, and the level of risk can be evaluated based on the organization's risk criteria.
- Identify possible risks that can be accepted or modified.
- Considering the relative impact of various risk-reduction treatment options.

At the risk treatment stage, risk scenarios that trigger risk appetite are mitigated and prioritized to receive risk treatment in the form of information security control recommendations and information security target setting based on ISO/IEC 27002:2022. The results of a series of risk management design stages are communicated to top management to confirm their suitability.

IV. Research and Discussion

A. Context Establishment

Risk criteria are used to rank risk levels as unacceptable or acceptable. Risk criteria can include several limits with a target risk scale that are adjusted to the needs of the organization. Based on the results of the interview with management, this research refers to the NIST SP 800-30 revision 1 framework standard based on the level of risk shown in Table I.

TABLE I. Risk Scale

Scala	Description	Semi Quantitative Value	
Very High	Have a negative impact	$4{,}0 < x \leq 5{,}0$	5
High	Almost certainly have a negative impact	$3{,}0 < x \leq 4{,}0$	4
Moderate	A medium probability results in a negative impact.	$2{,}0 < x \leq 3{,}0$	3
Low	A Small probability gives a negative impact	$1{,}0 < x \leq 2{,}0$	2
Very Low	A low probability has a negative impact.	$x \leq 1{,}0$	1

In determining the context, impact criteria using the level option are based on the level description in NIST SP 800-30, shown in Table II. Likelihood criteria using impact considerations that allow the threat to occur, as well as the possibility of starting or occurring, are listed in Table III.

TABLE II. Impact of Threat Event

Scala	Description	Value
Very High	Several severe or catastrophic negative effects on organizational operations, assets, individuals, or the nation	5
High	Severe or catastrophic adverse effect on organization operation, assets, individuals, or the nation.	4
Moderate	Serious adverse effect on an organization's operations, assets, individuals, or the nation.	3
Low	Limited effect on organization operation, assets, individuals, or the nation.	2
Very Low	Negligible adverse effect on organization operations, assets, individuals, or the nation.	1

TABLE III. LIKELIHOOD OF THREAT EVENT RESULTING IN ADVERSE IMPACTS

Scala	Description	Value
Very High	If the threat event is initiated or occurs, it is almost certain to have adverse impacts.	5
High	If the threat event is initiated or occurs, it is highly likely to have adverse impacts.	4
Moderate	If the threat event is initiated or occurs, it is somewhat likely to have adverse impacts.	3
Low	If the threat event is initiated or occurs, it is unlikely to have adverse impacts.	2
Very Low	If the threat event is initiated or occurs, it is highly unlikely to have adverse impacts.	1

B. Risk Assessment

At this stage, an assessment of the identified risks has been carried out, and an evaluation has been carried out for each risk scenario [24].

1) Risk identification: Risk identification is the process of finding, recognizing, or describing risk attributes. Risk identification includes identification of risk sources, events, and causes in the organization.

a) Asset identification: The process of asset identification begins with a weighted factor analysis of all ERP assets. Each information asset is scored for each critical factor and assigned a weight for each criterion. The weighting value is obtained from risk owner and IT risk officer in the organization.

To calculate weighted factor analysis, where each asset is scored for a critical factor and given a weight for each criterion. Criteria of weighted factor analysis consist of criterion 1 (impact to revenue – 30%), criterion 2 (impact to profitability – 40%), and criterion 3 (impact to public image – 30%). For scoring a critical factor, scores range from 0.1 to 1.0, and criteria are weighted from 1 to 100; each is weighted to indicate the importance of the criteria set for the organization [13]. The range of values obtained with reference to NIST SP 800-30 revision 1. Table IV shows that example of a weighted factor analysis worksheet.

TABLE IV. WEIGHTED FACTOR ANALYSIS WORKSHEET

Information Asset	Criterion 1 (30)	Criterion 2 (40)	Criterion 3 (30)	Weighted Score
IT Procedures and Policies	0,8	0,9	0,6	69
Network Topology	0,4	0,4	0,4	40
Server	0,8	0,9	0,7	81
ERP System	0,8	0,9	0,7	81
…				
IT Operation	0,8	0,8	0,7	77

In this discussion, we first identify two types of assets based on organization conditions, namely main assets consisting of business processes and activities, and information, and supporting assets consisting of all assets: hardware, software, network, site, personnel, and organizational structure [14].

Based on asset identification, the total number of identified primary assets is 9 assets, consisting of 3 business process and activities assets and 6 information assets. For identified supporting assets, 53 assets consist of 14 hardware assets, 18 software assets, 2 network assets, 11 site assets, and 8 personnel assets. Table IV is an example of asset identification with the following asset codes: A1-IT Procedures and Policies, A2-Network Topology, Source Code A3, Server-A4, A5-ERP System, until A62-IT Operation, as shown in Table V.

TABLE V. ASSET IDENTIFICATION

Asset Code	Asset Type	Asset Category	Risk Owner	Location
A1	Primary Asset	Business Processes and Activities	Head of ICT Division	Head Office
A2	Primary Asset	Information	Infrastructure Department	Head Office
A3	Primary Asset	Information	System Department	Head Office
A4	Supporting Asset	Hardware	Infrastructure Department	Head Office
A5	Supporting Asset	Software	System Department	Data Center
…				
A62	Supporting Asset	Personnel	Head of ICT Division	Head Office

b) Threat Identification: This research divides threat sources into two categories: adversarial and non-adversarial threat sources. Threat sources identified in this research were obtained from 12 adversarial sources and 18 non-adversarial sources.

In this discussion, the adversarial threat sources are as follows: S1: distributed denial of service, S2: injection, S3: intrusion, S4: malware, S5: social engineering, S6: sniffing, spoofing, or phishing, S7: website attack, S8: employee, S9: external stakeholder, S10: lack of employees, S11: unauthorized access, and S12: failure to maintain physical facilities.

Non-adversarial threat sources are as follows: S13: error requirement and design system, S14: human error (least privilege), S15: human error (personnel IT), S16-limited budget allocation for training, S17: obsolete technology, S18: lack of monitoring and control, S19: lack of expertise, skills, and employee behavior, S20: lack of employee information security awareness, S21: insecure password, S22: the application crashes, S23: error connection database, S24: operation system crashes, S25: web server crashes, S26: failure to backup data, S27: broken communication data, S28: failure data, S29: limited storage media, S30: devices end of support, S31: short-circuit, S32: power supply failure, S33: unstable power supply, S34: interruption of service from the provider, S35: rodent, S36: overhead, S37: maintenance fiber optics; S38: fire, S39: earthquake, and S40: thunderbolt.

Then, identify all threats that interfere with information security aspects such as Confidentiality (C), Integrity (I) and

Availability (A) on assets that have been identified. The following are questions to ask when identifying threats:

- What are the threats to the asset that you know or suspect?
- What are the most dangerous threats to the organization?
- What are the most expensive threats to recover from in the event of an attack?
- What are the threats that require the greatest expenditure to prevent them?

After getting the source of the threat in the ERP System, then identify this threat. For each asset, 35 threats have been identified, with different sources of threat. Table V explained that in the ERP system, T1: errors in making policies, procedures, or other relevant documents; T2: dissemination of information by unauthorized parties; T3: cybercrime; T4: broken access control; T5: failure of hardware, a network device, or physical facility assets; and until T35: unauthorized access.

Threat events are obtained from threat sources that have been defined through event logs and interviews with IT risk officers. Relevance was obtained according to NIST SP 800-30 revision 1, shown in Table VI.

TABLE VI. THREAT IDENIFICATION

Asset Code	Threat Event	Threat Source	CIA
A1	T1	S8, S9, S18, S19	C+I
A2	T2	S8, S9, S15	C
A3	T2	S8, S9, S15	C
A4	T3	S1, S2, S3, S4, S5, S6	C+I+A
	T5	S11, S15, S27, S29, S31, S32	A
A5	T3	S2, S3, S4, S6, S7	C+I+A
	T4	S8, S9, S14, S21, S30	C+I+A
	T5	S13, S22, S23, S24, S25	I + A
…			
A62	T35	S8, S15, S18, S20	C+I+A

c) Identification of existing controls: The next step is to identify the security controls that the company has implemented to protect the organization's assets from threats. In this discussion through the observation method obtained 52 security controls on assets. For example, of the existing control in this case, namely: C1: periodically review internal IT policies, procedures, and circulars, C2: classified information (controlled restricted, unclassified information, controlled, and public), C3: non-disclosure agreement, C4-restriction of access control, C5: information security awareness, education, and training program, C6: rollback procedure, C7: periodic review of access rights, C8: using a strong password according to best practice recommendations, C9: implemented least privileges, C10: log access control failures, C11: periodic maintenance of physical assets, C12: apply periodic updates or firmware to the most recent hardware, network devices, and software versions, and until C52: monitoring and controlling.

d) Identification of vulnerabilities: Identification of vulnerabilities means the extent to which the company has implemented controls to protect assets from threats. Vulnerabilities that have no corresponding threat may not require the implementation of control, but they do need to be identified and monitored. However, implementing ineffective controls or controls that don't work properly can be a vulnerability. In obtaining our vulnerability results, we used vulnerability sources references from the OWASP top ten [25].

The results of the study found 46 vulnerabilities, and Table IV shows the vulnerabilities for each asset based on the controls that have been implemented. The following is an example of controls in this discussion: V1: ineffective implementation of information security policies, V2: unencrypted documents and files, V3: vulnerable and end of support components, V4: insecure design system, V5: cryptographic failures, V6: no backup components, V7: software or hardware misconfigurations; and until V46: lack of information security practices.

TABLE VII. IDENTIFICATION OF VULBERABILITIES

Asset code	Existing controls	Vulnerability	Severity
A1	C1	V1	Low
A2	C2, C3	V2	Low
A3	C2, C3	V2	Low
A4	C5, C7, C8, C9, C12	V4	Moderate
	C6	V3, V5	Moderate
A5	C5, C7, C8, C9, C12	V4	High
	C4, C10	V5	Moderate
	C11, C52	V3, V5, V7	Moderate
…			
A62	C4, C7, C52	V46	Moderate

2) Risk Analysis: Risk analysis is the activity of mapping assets, asset values, threats, security controls, vulnerabilities, and impacts on CIA aspects. Risk analysis is intended to obtain the results of an impact assessment and identify possible information security risks.

In this research, we calculate the risk with a formula [13]: Risk is the probability of a successful attack on the organization (loss frequency = likelihood $*$ attack success probability) multiplied by the expected loss from a successful attack (loss magnitude = asset value $*$ probable loss) plus the uncertainty of estimates of all stated values.

Loss frequency is a measurement of the likelihood of an attack combined with the probability that it will succeed if it targets an organization. Loss magnitude is a combination of the asset value and the likelihood of its loss in an attack.

As shown in Table VIII, the risk analysis obtained 142 levels of risk in the ERP system, with 2 at high level, 30 at moderate level, 97 at low level, and 13 at very low level.

TABLE VIII. RISK ANALYIS

Asset Code	Threat event	Threat Source	CIA	Existing Control	Vulnerability	Risk	Level of Risk
A1	T1	S8, S9, S18, S19	C+I	C1	V1	0,20	Very Low
A2	T2	S8, S9, S15	C	C2, C3	V2	1,44	Low
A3	T2	S8, S9, S15	C	C2, C3	V2	1,64	Low
A4	T3	S1, S2, S3, S4, S5, S6	C+I+A	C4, C5, C7, C8, C9, C12	V4	2,88	Moderate
	T5	S11, S15, S27, S29, S31, S32	A	C6	V3, V5	2,23	Moderate
A5	T3	S2, S3, S4, S6, S7	C+I+A	C4, C5, C7, C8, C9, C12	V4	3,12	High
	T4	S8, S9, S14, S21, S30	C+I+A	C4, C9, C10	V5	2,11	Moderate
	T5	S13, S22, S23, S24, S25	I+A	C11, 52	V3, V5, V7	2,47	Moderate
…							
A62	T35	S8, S15, S18, S20	C+I+A	C4, C7, C52	V46	2,73	Moderate

3) Risk Evaluation: Risk evaluation in this discussion aims to compare the results of risk analysis with risk criteria and then determine whether the risk rating is acceptable or tolerable. The stages of risk evaluation include compiling risk priorities based on the amount of risk, provided that:

- The highest level of risk gets the highest priority.
- If there is more than one risk with the same risk magnitude, the risk priority is determined based on the sequence of impact areas from the highest to the lowest according to the loss magnitude.
- If there is still more than one risk that has the same magnitude and area of impact, then the risk priority is determined based on the order of the highest to the lowest risk category according to the loss frequency.
- If there is still more than one risk that has the same magnitude, loss magnitude, and loss frequency, then the risk priority is determined based on the judgment of the risk owner.

Table IX shows as risk appetite based on semi-quantitative based risk rating guidelines with NIST SP 800-30 revision 1 and two risk treatment criteria (likelihood and overall level of impact).

TABLE IX. RISK APPETITE

Overall likelihood (Threat event occurs and result in adverse impact)	Level of impact				
	Very Low (1)	Low (2)	Moderate (3)	High (4)	Very High (5)
Very High (5)	Accept	Mitigation	Mitigation	Mitigation	Mitigation
High (4)	Accept	Mitigation	Mitigation	Mitigation	Mitigation
Moderate (3)	Accept	Accept	Mitigation	Mitigation	Mitigation
Low (2)	Accept	Accept	Accept	Mitigation	Mitigation
Very Low (1)	Accept	Accept	Accept	Accept	Accept

Risk determination is the first step before risk prioritization. Priority risk matrix is classified based on NIST SP 800-30 revision 1 and is a matrix of the relationship between assets and threats, show as in Fig. 2.

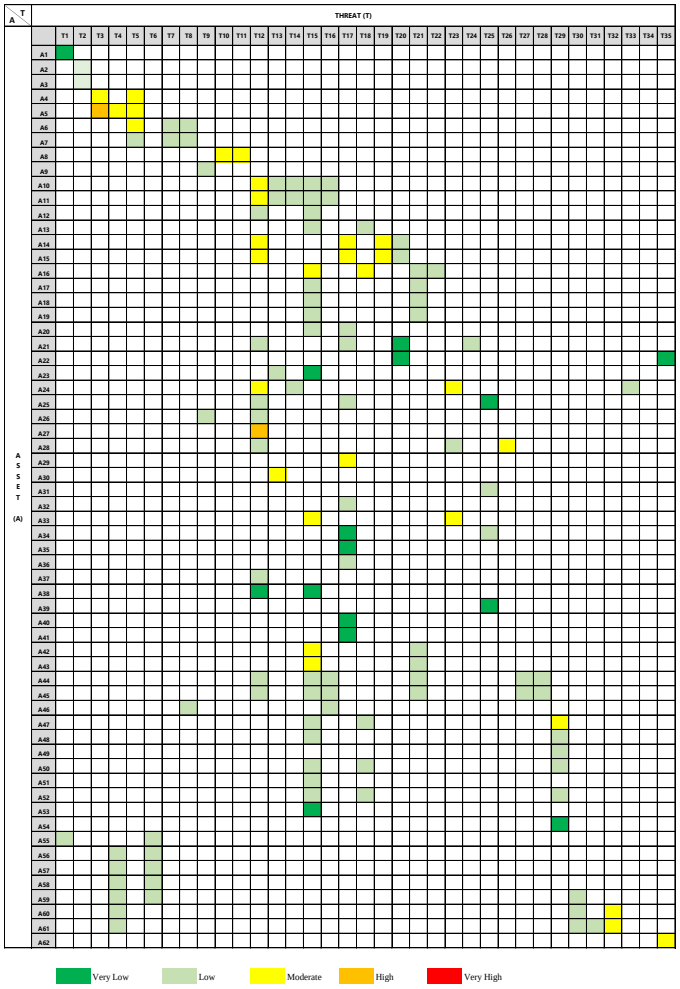

Fig. 2. Risk matrix.

C. Risk Treatment and Risk Acceptance Strategy

1) Risk treatment strategy: Risk treatment aims to control dangerous risks by developing relevant treatments to control the causes of risk, measuring the effectiveness of the treatment, and if the estimated risk value remains at an intolerable level, preparing alternative treatments.

According to ISO/IEC 27005:2018, there are four options available for risk treatment, namely risk modification, risk avoidance, risk sharing, and risk retention. In this discussion, we found 142 risks with unacceptable decisions for 32 modification risks. Total risk acceptance is 110, of which there are 90 risk retention, 2 risk avoidance, and 18 risk sharing.

In selecting the risk treatment that has been sorted based on risk priority from the highest to the lowest risk level. The following is an example of a risk priority in Table X.

TABLE X. RISK TREATMENT

Priority	Risk Scenario	Level of Risk	Decision	Risk Appetite
1	A5, T3	High	Mitigation	Risk Modification
2	A4, T3	Moderate	Mitigation	Risk Modification
3	A62, T35	Moderate	Mitigation	Risk Modification
…				
142	A1, T1	Very Low	Accept	Risk Retention

2) Risk Acceptance Strategy: This activity is carried out to describe more clearly some of the security controls that have been selected for risk treatment. In this discussion, we propose that an information security team be created to define the roles and responsibilities, or Person in Charge (PIC), of information security activities in every organization.

In establishing information security controls, PIC is required to be responsible for risk acceptance, as shown in Table XI.

TABLE XI. RISK ACCEPTANCE

Priority	Risk Scenario	Control with ISO/IEC 27002:2022	PIC
1	A5, T3	**Organizational controls:** 5.1 Policies for information security 5.37 Documented operating procedures. **People controls:** 6.3 Information security awareness, education, and training **Technology controls:** 8.7 Protection against malware 8.20 Networks security 8.23 Web filtering	Head of Department Information Technology System
2	A4, T3	**Organizational controls:** 5.1 Policies for information security 5.37 Documented operating procedures. **People controls:** 6.3 Information security awareness, education, and training **Technology controls:** 8.7 Protection against malware 8.20 Networks security 8.32 Change management	Head of Department Information Technology Infrastructure and Service
3	A62, T35	**Organizational controls:** 5.1 Policies for information security 5.17 Authentication information **People controls:** 6.2 Terms and conditions of employment 6.3 Information security awareness, education, and training **Physical controls:** 7.7 Clear desk and clear screen **Technology controls:** 8.2 Privileged access rights	Head of Department Information Technology Infrastructure and Service
…			

32	A5, T4	**Organizational controls:** 5.1 Policies for information security 5.15 Access control **People controls:** 6.3 Information security awareness, education, and training **Physical controls:** 7.7 Clear desk and clear screen **Technology controls:** 8.2 Privileged access rights 8.32 Secure coding	Head of Department Information Technology Infrastructure and Service

According to research findings, there are 10 controls on 14 types of threats for organizational control (clause 5), 5 controls on 7 types of threats for people control (clause 6), 3 controls on 4 types of threats for physical control (clause 7) and 14 controls on 11 types of threats for technology control (clause 8), as shown in Fig. 3.

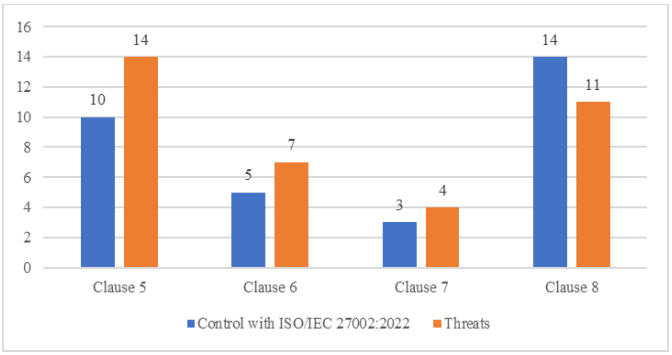

Fig. 3. Determination controls on risk categories.

For documentation and monitoring risks, we are using a risk register. The risk register provides holistic information about risks and enables stakeholders to make decisions regarding those risks and their management. The risk owner or PIC uses the risk register to document and manage risks to asset organizations.

V. Conclusion

Risk management principles are something to consider when preparing the framework and forming the foundation for risk management practices. The risk management process must also be aligned with the corporate culture, processes, structure, and strategy. We use an integrated ISO/IEC 27005:2018 and NIST SP 800-30 revision 1 framework, to make it easier to implement in organizations.

Context establishment is the process of determining the basic parameters in risk management by providing an understanding of the internal and external environments in management implementation. The risk assessment has three stages, namely risk identification, risk analysis, and risk evaluation. Risk identification includes risk sources, events, and causes, and impacts on each asset. Risk identification is sourced from historical data, theoretical analysis, expert opinion, and stakeholder needs.

Risk analysis is a systematic process to determine how often an event occurs, the risk of the impact that might occur, and the size of the consequences that arise from the event. The results of risk analysis obtained: 142 levels of risk with a high level (high) of 2 risks, a moderate level (moderate) of 30 risks, a low level (low) of 97 risks, and 13 levels of very low (very low).

Risk evaluation is the process of comparing the results of risk analysis with risk criteria to then determine whether the risk rating is acceptable or tolerable. There are 142 identified risk priorities, of which 110 are acceptable and 32 are unacceptable. We have developed this research up to the risk treatment stage by providing control recommendations using ISO 27002:2022 guidelines. The risk management strategy in this case aims to eliminate the threat of risk so that it does not become an obstacle in efforts to achieve organizational goals.

Risk treatment option depends on the risk appetite and risk tolerance. In this case, we use several options to deal with these risks, such as risk modification to reduce risk through selecting controls so that the risk is acceptable, avoiding risks by avoiding activities or conditions that may pose risks, sharing risks by working with third parties who are able to deal with risks, and accepting risks without taking further action.

References

[1] J. Tupa, J. Simota, and F. Steiner, “Aspects of Risk Management Implementation for Industry 4.0,” Procedia Manuf, vol. 11, pp. 1223–1230, 2017, doi: 10.1016/j.promfg.2017.07.248.

[2] I. Appiah-Otoo and N. Song, “The impact of ICT on economic growth-Comparing rich and poor countries,” Telecomm Policy, vol. 45, no. 2, Mar. 2021, doi: 10.1016/j.telpol.2020.102082.

[3] D. W. Jorgenson and K. M. Vu, “The ICT revolution, world economic growth, and policy issues,” Telecomm Policy, vol. 40, no. 5, pp. 383–397, May 2016, doi: 10.1016/j.telpol.2016.01.002.

[4] Sharif, M. H. U., & Mohammed, M. A., “A literature review of financial losses statistics for cyber security and future trend,” World Journal of Advanced Research and Reviews, vol. 15, no. 1, pp. 138–156, Jul. 2022, doi: 10.30574/wjarr.2022.15.1.0573.

[5] ISO, ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls, 2022. [Online]. Available: https://www.iso.org/standard/75652.html.

[6] J. Masso, F. J. Pino, C. Pardo, F. García, and M. Piattini, “Risk management in the software life cycle: A systematic literature review,” Computer Standards and Interfaces, vol. 71. Elsevier B.V., Aug. 01, 2020. doi: 10.1016/j.csi.2020.103431.

[7] M. Niemimaa, J. Järveläinen, M. Heikkilä, and J. Heikkilä, “Business continuity of business models: Evaluating the resilience of business models for contingencies,” Int J Inf Manage, vol. 49, pp. 208–216, Dec. 2019, doi: 10.1016/j.ijinfomgt.2019.04.010.

[8] K. Charoenthammachoke, N. Leelawat, J. Tang, and A. Kodaka, “Business continuity management: A preliminary systematic literature review based on sciencedirect database,” Journal of Disaster Research, vol. 15, no. 5. Fuji Technology Press, pp. 546–555, 2020. doi: 10.20965/jdr.2020.p0546.

[9] M. Fahrurozi, S. A. Tarigan, M. A. Tanjung, and K. Mutijarsa, “The Use of ISO/IEC 27005: 2018 for Strengthening Information Security Management (A Case Study at Data and Information Center of Ministry of Defence),” in ICITEE 2020 - Proceedings of the 12th International Conference on Information Technology and Electrical Engineering, Oct. 2020, pp. 86–91. doi: 10.1109/ICITEE49829.2020.9271748.

[10] M. Brunner, C. Sauerwein, M. Felderer, and R. Breu, “Risk management practices in information security: Exploring the status quo in the DACH region,” Computer Security, vol. 92, May 2020, doi: 10.1016/j.cose.2020.101776.

[11] P. Wang and M. Ratchford, “Integrated methodology for information security risk assessment,” Advances in Intelligent Systems and

Computing, vol. 558, pp. 147–150, 2018, doi: 10.1007/978-3-319-54978-1_20.

[12] ISO, ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements, 2022. [Online]. Available: https://www.iso.org/standard/82875.html.

[13] M. E. Whitman and H. J. Mattord, "Principles of Information Security Sixth Edition," 2018. [Online]. Available: www.cengage.com.

[14] ISO, ISO/IEC 27005:2018, Information technology — Security techniques — Information security risk management, 2018.

[15] I. Akkiyat and N. Souissi, "Modelling risk management process according to ISO standard," International Journal of Recent Technology and Engineering, vol. 8, no. 2, pp. 5830–5835, Jul. 2019, doi: 10.35940/ijrte.B3751.078219.

[16] G. H. S. Rampini, H. Takia, and F. T. Berssaneti, "Critical success factors of risk management with the advent of ISO 31000 2018 - Descriptive and content analyzes," in Procedia Manufacturing, 2019, vol. 39, pp. 894–903. doi: 10.1016/j.promfg.2020.01.400.

[17] H. Setiawan, F. A. Putra, and A. R. Pradana, "Design of Information Security Risk Management Using ISO/IEC 27005 and NIST SP 800-30 Revision 1: A Case Study at Communication Data Applications of XYZ Institute," in In 2017 International Conference on Information Technology Systems and Innovation (ICITSI) (pp. 251-256). IEEE., 2018, pp. 251–256.

[18] M. al Fikri, F. A. Putra, Y. Suryanto, and K. Ramli, "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, 2019, vol. 161, pp. 1206–1215. doi: 10.1016/j.procs.2019.11.234.

[19] M. Ngamboé, P. Berthier, N. Ammari, K. Dyrda, and J. M. Fernandez, "Risk assessment of cyber-attacks on telemetry-enabled cardiac implantable electronic devices (CIED)," Int J Inf Secur, vol. 20, no. 4, pp. 621–645, Aug. 2021, doi: 10.1007/s10207-020-00522-7.

[20] I. M. M. Putra and K. Mutijarsa, "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, Apr. 2021, pp. 14–19. doi: 10.1109/EIConCIT50028.2021.9431865.

[21] O. Ali, A. Shrestha, A. Chatfield, and P. Murray, "Assessing information security risks in the cloud: A case study of Australian local government authorities," Gov Inf Q, vol. 37, no. 1, Jan. 2020, doi: 10.1016/j.giq.2019.101419.

[22] H. Okonofua and S. Rahman, "Evaluating the Risk Management Plan and Addressing Factors for Successes in Government Agencies," in Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018, Sep. 2018, pp. 1589–1592. doi: 10.1109/TrustCom/BigDataSE.2018.00230.

[23] NIST, "Guide for conducting risk assessments," Gaithersburg, MD, 2012. doi: 10.6028/NIST.SP.800-30r1.

[24] G. Stoneburner, A. Goguen, and A. Feringa, "Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology," 2012.

[25] OWAPS, "Upcoming OWASP Global Events," 2022. [Online]. Available: https://owasp.org/www-project-top-ten/#