Information Security Risk Strategy at PT. X Using NIST SP 800-30

I G. N. M. Putra Eryawan[a1], Gusti M. Arya Sasmita[a2], A. A. KT. Agung Cahyawan Wiranatha[a3]
[a]Department of Information Technology, Faculty of Engineering, Udayana University
Bukit Jimbaran, Bali, Indonesia, phone. (0361) 701806
e-mail: [1]putraeryawan53@gmail.com, [2]aryasasmita@it.unud.ac.id,
[3]agung.cahyawan@unud.ac.id

Abstrak

Keamanan informasi merupakan aspek vital yang harus diperhatikan dalam penggunaan perangkat teknologi informasi oleh pengguna aktif. Perusahaan PT. X menjalankan proses bisnis menerapkan teknologi informasi terhubung aspek distribusi melalui perencanaan sumber daya perusahaan. Aset terbentuk teknologi informasi, yang dimiliki meliputi infrastruktur TI, sistem informasi, operasi prosedur, infrastruktur jaringan. Aset ini memiliki potensi ancaman risiko yang menyebabkan kerusakan/gangguan menghasilkan kerugian. Masalah ini timbul untuk menanggulangi melalui tindakan responsif dengan strategi risiko. Pemilihan metode NIST SP 800-30*, memiliki perspektif* penilaian risiko yang *fleksibel untuk organisasi dan berstandar federasi keamanan Amerika. Penelitian ini dibagi tiga tahap utama yaitu penilaian risiko sebagai menentukan besaran risiko, mitigasi risiko sebagai perencanaan menanggulangi risiko, dan evaluasi risiko yang diwujudkan berupa laporan strategi risiko. Hasil penelitian berdasarkan empat aset menunjukkan jumlah nilai risiko berdasarkan perhitungan matriks likelihood dan impact terhadap ancaman yang tertinggi pada level low senilai 14, medium senilai 12, dan high senilai 4 dikategorikan cukup baik.*

Kata kunci: *Strategi Risiko, Keamanan Informasi, NIST SP 800-30, Risk*

Abstract

Information security is a vital aspect that must be considered in use of information technology devices by active users. PT. X runs a business that applies information technology related to distribution aspects through company resource planning. Information technology formed assets IT infrastructure, information systems, operating procedures, and network infrastructure. This asset has a potential threat that causes disruption resulting losses. This problem arises to cope through the response to the risk strategy. NIST SP 800-30 method has a flexible risk perspective for the organization and federation standards of American security. Research is divided into risk measurement as a risk, risk mitigation as risk planning, and risk evaluation embodied risk reports. Results of the research show the value of risk through the calculation of the likelihood and impact matrix of the highest threat is at a low level is 14, medium at 12, and high of 4 are categorized good enough.

Keywords*: Risk Strategy, Information Security, NIST SP 800-30, Risk*

1. Introduction

Information in the current era of globalization is increasingly developing, increasingly racing with technological developments that continue to run. Indications are more and more individuals and organizations are relying on IS/IT as part of their daily needs [1]. So the safety factor is a quite serious concern as the main anticipation of safety in supporting information technology infrastructure and users [2].

Operational management through corporate governance infrastructure, of course there is also a security management infrastructure for access control that is still minimal monitored, making it possible at any time for a sudden threat that cannot be thought of through internal or even external threats [3] - [4]. According to Sarno and Iffano, there is no standard reference on what standards will be used or chosen for companies in conducting information security risk management audits so based on view aspects according to the needs of investigators [5]. Evaluation in the selection of strategies for managing information security, controls must have high reliability, in order to improve and minimize the risk of loss that may arise [1] - [6].

PT. X embodies information technology through IT infrastructure in carrying out company management operations. Management activities carried out by entering, processing, managing, and reporting supported by the IT system builders. Information part of the data that is formed is an important part in facing business competition. Referring to achieving the company's vision and mission so that operations do not hinder from disruption, so the information shall be guaranteed security against the risk of loss. PT. X has not yet implemented a risk strategy for its system builders, therefore it is necessary to carry out a risk strategy for information security. The risk strategy is expected to show the quantity of repair costs for development planning.

Analysis of risk strategies referring to risk management for research by Monika Evelin Johan, et al. determined by the NIST SP 800-30 method. The vulnerability process using the newly frozen NIST SP 800-26 and recommendations provided only the status of control measures [7] - [8]. Research by Dian Ayu Permatasari, et al, which emphasizes the initial process in threatening risks. The analysis emphasizes the risk of the NIST SP 800-30 only at the risk screening stage. Vulnerability identification is still using NIST SP 800-26 which has just been frozen and the recommendation is not at the risk mitigation stage [9]- [8]. The achievement of this research with an emphasis on the NIST SP 800-30 method through the latest published support for vulnerability testing using NIST SP 800-53A Revision 4 and following the standard process to the risk mitigation stage to see the amount of risk costs at PT. X.

The method that can be used to carry out a risk strategy in information management is NIST SP 800-30. The choice of the NIST SP 800-30 method is due to its shortcomings as a risk management stream [10]. A framework that can determine information control risks complemented by information management recommendations. Aspect guarantees it in terms of security, confidentiality, integrity, data and data used for development, improvement, and evaluation evaluation [11].

Research with the NIST SP 800-30 method to see the level of risk of information security on the implementation of IS or IT at PT. X, which is expected to be a development life cycle carried out by the IT Division at PT. X. The NIST SP 800-30 method is equipped with a strategic control process in terms of financing processing that adapts to organizational conditions while adhering to guidelines. This research as the aim to determine the risk level of vulnerability information by using NIST SP 800-30, so as to develop risk control strategy steps with control recommendations equipped with financing to be used as a reference for improving information security at PT. X [3] - [12].

2. Research Method

This research method serves as a step in defining research in a process flow to ensure an orderly, systematic, and directed direction [13]. The underlying process flow for implementing risk strategies follows from the NIST SP 800-30 guidelines.

2.1 Methodology Flow

The methodology flows through a defined stage process. The process flow is presented in Figure 1.

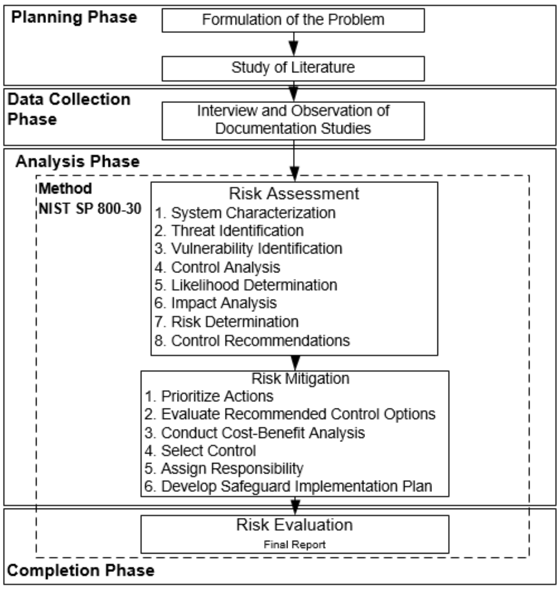

Figure 1. Methodology Flow

Figure 1 shows the research flow in the analysis of information security risk strategies at PT. X. The first stages of flow is the Planning Phase, through the process of formulating the problem at PT. X. This stage is to formulate problems in the field and the process of studying literature by looking for references, theoretical sources, supporting data in strengthening research studies. The second stage is data collection by conducting interview observation of documentation studies at PT. X. [9]. The second stage is to visit and find out about current IT risk issues. The third stage is analyzing and the fourth stage is the completion phase which is part of the NIST SP 800-30 method [9] - [11]. The NIST SP 800-30 stage is divided into three parts, including the assessment stage to assess risk, the risk mitigation stage as control, The risk evaluation stage is in preparing the final risk report, each of which has a detailed process.[10].

The first part of the risk assessment is identifying risks with eight processes including the first process of characterizing the system to find out the components that make up the system including hardware and software, the second process of identifying threats in detecting opportunities for threats that occur, the third process of identifying vulnerabilities through an assessment of the authorized party by the controller and IT supervisors, the fourth process of control analysis in determining the threat of vulnerability, the fifth process of determining likelihood as ensuring the probability of the likelihood that is vulnerable to threatening, the sixth process carries out an impact analysis to determine the resulting impact on the threat of vulnerability, the seventh process of determining risk as ensuring the level of risk to the vulnerability threat, and the last process carries out control recommendations which specified in the NIST SP 800-53 standard [10].

The second part is risk mitigation as the implementation of appropriate repair control. There are six processes in this part of the process, including prioritizing action as a risk level action rating for action, providing recommendations for control options referring to NIST SP 800-30, conducting cost-benefit analysis in determining control costs against the level of risk, selecting controls to select the appropriate control conditions, and the final process of assigning responsibility in dividing the parties responsible for implementing risk mitigation [10]. The last part of the risk evaluation is the final process of the completion stage, as the implementation of a risk strategy for the implementation of risk control. This implementation is carried out in a determined period by considering the decision on the readiness for implementation that involves senior management [10]. The final document defines the findings as a continuous development life cycle [10].

2.2 Data Collection

Primary data collection is carried out with parties who have the authority to maintain the IT establishment [11] - [4]. IT controllers and Supervisors play an important role in collecting data at PT. X. Observation as secondary data collection to determine the findings of relevant indicators in the field [11] - [10]. Conditions assessed in terms of organizational profile, performance areas, key notes, applied IT utilization, service integration, and organizational quality standards, assets, milestones, and form of assessment questions refers to NIST SP 800-30 [10]. An example of a sample assessment question is presented in Table 1.

Table 1. NIST Assessment Questions SP 800-30

No	Questions	Comments	Subject	Documentation
1	Forms of information systems run by the company PT. X?	Zeta information system is a system engaged in distribution in distributing business processes from production to consumers.	Supervisor IT	

Table 1 is a sample that refers to the questionnaire on the NIST SP 800-30. The data obtained from this result is intended as supporting material and consideration for the next process. The respondent's statement needs to be supported by objective relevant documentation.

2.3 Theoretical Framework

NIST 800-30 risk theory, the implementation of the process risk management through the NIST SP 800-30 guideline, namely risk assessment by taking eight stages that must be passed, risk mitigation with 6 stages must be passed and risk evaluation (risk evaluation) by forming the composition of this final report [10]. The allotment of supporting guidelines is in line with NIST SP 800-30, namely NIST SP 800-26 to determine vulnerability identification [10]. Since 2015, NIST SP 800-26 replaced to NIST SP 800-53A Rev. 4 as the standard guide to assess the security and privacy controls in assessing the vulnerability identification.[14]. This refers to the control recommendations updated also with NIST 800-53 Revision 4 for relevant adjustments to NIST SP 800-53A Rev. 4 related to security and privacy controls as a form of information security assessment in an organization [14]. The model form guides this document following a harmonious approach to the complement of the ISO/IEC 30001 and 27005 standards [15] - [16].

3. Literature Study

Literature studies contain libraries that are used as references in research. Sources are obtained from books, the internet, or journals that have legitimacy. Some of the literature used are risk strategies, information security, the NIST SP 800-30 method, and method support guides.

3.1 Risk Strategies

Risk strategy is related to management or management in giving consideration of decisions to reduce disruption or damage that can cause losses as a form of security protection to balance financial costs [6]. The risk strategy is managed in an ongoing manner, through mitigation assessment and evaluation activities [6].

3.2 Information Security

Information security is protecting data collection from various threats to ensure the continuity of an organization's business processes, minimizing risks and maximizing performance. Information security aspects determine the sustainability of an organization's business operational activities [17]. Some elements of information security consist of 3 aspects (ISO 27000), including:

a. Confidentiality is the point where information is not readily available or may be closed to individuals, processes or entities that do not have access rights.[17] - [18].

b. Integrity is a matter that must be ensured that the information or data is maintained intact. This means that data should not be modified illegally [17] - [18].
c. Availability is available with a guarantee for each information system as serving its purpose, information must be available when needed [17] - [18].

3.3 NIST SP 800-30 Method

NIST SP 800-30 is a document standard method published by the National Institute of Standards and Technology as a framework method for determining risk strategies in its management. NIST SP 800-30 there are three main stages, namely risk assessment [10] - [19], risk mitigation and risk:

a. Risk Assessment is a stage of the process of determining risk. The form of processes carried out includes the characterization of the system, identification of threats, vulnerabilities identification, control analysis, determination of the likelihood, impact analysis, risk assessment, control recommendations [10].
b. Risk Mitigation, namely the stages of determining the plan for implementing security controls. Forms of the process including the priority of action, recommendations for control options, analysis of cost benefits, selection of controls, assignment of responsibilities [10].
c. Risk Evaluation, which is the result of a risk strategy with its management manifested in the report [10].

3.4 Supporting Guidelines

The method used has supporting guidelines in aligning the flow of research methods, including:

a. NIST SP 800-53A Revision 4 is a guideline as an assessment to identify the availability of security and privacy controls, this is provided by a questionnaire with the division of 18 groups [15].
b. NIST SP 800-53 Revision 4 is a supporting guideline as a recommendation for security and privacy control through recommendations tailored to the group [12].

4. Result and Discussion

The finding in this study include the process of implementing risk strategies by using NIST SP 800-30 method to providing recommendations for recommendations from the results of risk findings.

4.1 Risk Assessment

The discussion of the results taken from the methodological steps carried out in the company organization PT. X. The results are shown from the NIST SP 800-30 method process [10]. elements related to the use of IT crucially in the form of hardware specifications to determine vital assets, network device architecture in terms of the existence of a data center that forms a network topology equipped with internet allocation details, the discovery of a software model applied to the organization, namely the zeta which is a distribution group business operation by PT. X part of enterprise resource planning which describes business processes, system architecture, information system forming specifications, has a physical security role in terms of tightening policy procedures, CCTV, fingerprint privileges. This finding serves as a sign for threats that can be defined as the identification of IT assets and the IT boundaries that are applied.

The second stage it’s the identification of threats, namely the assessment includes events that have occurred as a potential assessment of inherent direct vulnerability and classification of potential threats consisting of 3 aspects of human, environmental and IT infrastructure which refers to the considerations of the NIST SP 800-30 guidelines [10].

The third stage is the analysis of the self-assessment to determine the threats that produce risks. The acquisition of risk arises through the results of a questionnaire assessment of federal and organizational information security and privacy control guides in Sp nist. 800-53A Rev. 4 through the absence of potential controls in assessing vulnerability [15]. Grouping by topic self-assessment code is seen in Table 2.

Table 2. Question List of NIST SP 800-53A Rev. 4

Question Family	Code	Question Family	Code
Access Control	AC	Media Protection	MP
Awareness And Training	AT	Physical And Environmental Protection	PE
Audit And Accountability	AU	Planning	PL
Security Assessment And Authorization	CA	Program Management	PM
Configuration Management	CM	Personnel Security	PS
Contingency Planning	CP	Risk Assessment	RA
Identification And Authentication	IA	System And Services Acquisition	SA
Incident Response	IR	System And Communications Protection	SC
Maintenance	MA	System And Information Integrity	SI

The results of the process self-assessment will get the value of the control of vulnerability affected on the four main assets identified among IT infrastructure, Zeta application systems, PC Users, network infrastructure. The four assets are mapped according to the threat of access control. The fifth stage is the likelihood stage or assessment of trends or opportunities for the number of events to the assets. The assessment of the trend level is influenced by quantitative values which presented in Table 3.

Table 3. Likelihood Level Values

Level	Semi Quantitative Values		Description
	Scale Value	Number of Events	
High	1	> = 6 Times	A malfunction occurs more than 6 times in a year
Medium	0,5	3-5 Times	A malfunction occurs 3 or 5 times in one year
Low	0,1	= < 2 Times	A malfunction occurs less than once a year

The results of the assessment of the level of a tendency towards the appearance of a threatening asset with the number of times the threat occurred. The overall results of the four assets or total likelihood level values which presented in Table 4.

Table 4. Level Values Recapitulation of Likelihood

Likelihood Statements	Level Value Likelihood		
	Low	Medium	High
Infrastructure of IT	6	3	3
Zeta Information System	5	3	2
PC User	0	3	1
Network Infrastructure	3	0	1
Number of Results Statement for each trend level	14	9	7

Indicators in determining the impact analysis are influenced by the level of impact analysis value. The impact analysis value level is a statement of the level of the impact definition conditions. The form of the impact analysis value level is presented in Table 5.

Table 5. Values Level of Impact Analysis

Level	Semi Quantitative Values		Effect of Impact of Threats
	Scale Value	Value of Amount of Impact	
High	100	5 Involved	The effect of menace impacts involves the organization's operations, organizational assets, individuals, other

			organizations
			The effect of threat impacts involves the organization's operations, organizational assets, and individuals.
		3 Involved	The effect of threat impacts involves the organization's operations, organizational assets, and other organizations.
			The effect of the impact of threats involves the operations of the organization, other organizations, individuals
Medium	50	2 Involved	The effect of threat impacts involves the organization's operations, organizational assets.
Low	10	1 Involved	The effect of threat impacts involves organizational operations that cannot be ignored
		0	The effect of threat impacts involves organizational operations that can be ignored

The results of the threatening impact level analysis produce the magnitude of the consequences that can occur to the asset. The assessment of the results of the impact level recap from the statement obtained the results which showed in Table 6.

Table 6. Level of Impact Recapitulation Value

Impact Statements	Impac Level Value		
	Low	Medium	High
Infrastructure of IT	1	2	9
Zeta Information System	0	3	7
PC User	0	4	0
Network Infrastructure	0	2	2
Number of Results Statement for each trend level	1	11	18

The level of impact results in the number of threats categorized as high with a total value of a statement of low details of 1, medium of 11, high of 18. the seventh stage of the risk determinations. The process of determining risk through a matrix scale guided by NIST SP 800-30 matrix values with a level 3 scale of the likelihood and impact level presented in Table 7.

Table 7. Risk Level Matrix

Level Risk	Level Impact		
Level Likelihood	Low (10)	Medium (50)	High (10)
High (1.0)	Low (10)	Medium (50)	High(100)
Medium (0.5)	Low (5)	Medium (25)	Medium (50)
Low (0.1)	Low (1)	Low (5)	Low (10)

The resulting matrix values get a mapping of likelihood values with impact values. The overall results of the matrix assessment are based on the four main assets, namely IT infrastructure, Zeta application systems, PC Users, network infrastructure. Determination of risk with a level 3 scale is followed by level adjustment with risk strategy corrective actions guided by NIST SP 800-30. The risk strategy model for the suitability of the risk level is presented in Table 8.

Table 8. Level of Risk Strategic Action

Level Risk	Risk Corrective Actions
High	Corrective action immediately with corrective implementation
Medium	Corrective actions to be developed in the action plan for a certain period
Low	Actions can be deferred by the decision to accept the risk to be developed

The results for this risk level determination from calculation of the likelihood value matrix with the impact value.The results of each level of risk affect the control conditions of the risk strategy action. The results of the preparation of risk determination are recapitulated based on the findings of the four assets. The recapitulation form is presented in Table 9

Table 9. Level of Risk Recapitulation Value

Risk Statement	Level Risk Value		
	Low	Medium	High
Infrastructure of IT	6	3	3
Zeta Information System	5	5	0
PC User	0	4	0
Network Infrastructure	3	0	1
Number of Results Statement for each trend level	14	12	4

The level of risk results in an amount of risk categorized sufficiently with a total value of a breakdown statement of 14, medium of 12, high of 4. The visualization in a graph of the amount of risk is presented in Figure 2 which uses a bar chart for each asset in the left image and a column graph for each level of risk in the image on the right.

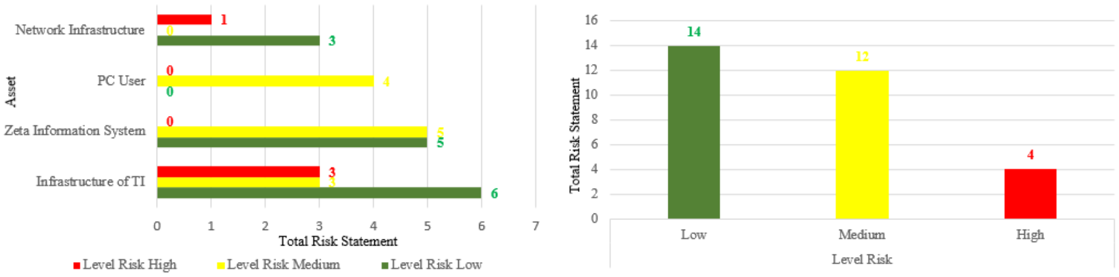

Figure 2. Results of Determination of Asset Risk (Right) and
Results of Total Level of Risk Determination (Left)

The eighth stage is the control recommendation process, namely the determination of adjusted supporting documents of NIST SP 800-53 Revision 4 [16]. This support is to guide the recommendation requirements that refer to the NIST SP 800-30 method based on the NIST SP 800-53A assessing questionnaire Revision 4 [15]. There are 18 groups of recommendations shown in Table 10 and the form of some of the appraisals taken 3 asset samples are described in Table 11 .

Table 10. Control Recommendation Group List NIST SP 800-53 Rev. 4

Question Family	Code	Question Family	Code
Access Control	AC	Media Protection	MP
Awareness And Training	AT	Physical And Environmental Protection	PE
Audit And Accountability	AU	Planning	PL
Security Assessment And Authorization	CA	Program Management	PM
Configuration Management	CM	Personnel Security	PS
Contingency Planning	CP	Risk Assessment	RA
Identification And Authentication	IA	System And Services Acquisition	SA
Incident Response	IR	System And Communications Protection	SC
Maintenance	MA	System And Information Integrity	SI

Table 11. Control Recommendations

No	Asset	Vulnerability	Risk Level	Recommendation (NIST SP 800-53 R. 4)
1.	Infrastructure	Does not specify	High	MA-5 Maintenance Personnel

	of IT	personnel or roles to be alerted if a processing failure occurs		The organization establishes a Maintenance authorization employees according to the role of the authorities with the suitability of technical competencies in maintaining information systems AU-5 Response To Audit Processing Failures The information system provides warnings to employees according to their role in taking action in auditing processing failure responses
2.	Zeta Information System	There is no initial training for employees to work according to their roles and duties as well as security awareness training on information systems	Medium	AT-3 Security Awareness and Training Policy and Procedures The organization documenting and developing policies and procedures for implementing security awareness education for each employee regarding security in operating the operating system, fostering a compliant attitude towards roles and responsibilities within it. AT-3 Security Awareness Training The organization provides role - based security
3.	Network Infrastructure	There is no management of the amount of bandwidth usage processing	Low	AU-2 Audit Events The organization reviews and updates firewall rules for events in the log-system that trigger potential entrance threats to malware attacks with an agreed period

4.2 Risk Mitigation

Risk mitigation strategies to prepare coping plans for the acquisition of risk values from the risk assessment stage. The mitigation process has a part of the process including priority of action, recommendations for control options, analysis of cost benefits, selection of controls, assignment of responsibilities, develop a safeguard implementation plan.

The initial stage in risk mitigation, namely priority action, is a process of the level risk scale ranks from high, followed by medium, and finally low. Ranking as a profit objective gives more attention to risks that are threaten to be acted upon.

second stage, evaluate recommended control options, namely the choice of mitigation measures against the type of risk with a level risk scale. This option is adjusted for the NIST SP 800-30 guidelines, there are options as follows:

a. The Risk assumption is to accept potential risks by continuing to run the program or by implementing controls to reduce risk to an accepted level [10] - [20].

b. Risk avoidance, namely avoiding risk that eliminating the causes of risk and the consequences [10] - [20].

c. Risk limitation, namely limiting certain risks by implementing evaluation and monitoring that can minimize the adverse effects of the risks that occur [10] - [20].

d. Risk transference, which is, transferring risk using the services of a third party to compensate for losses arising from the risk [10] - [20].

The results of the recapitulation of mitigation options for the four assets and threats of 30 through the mitigation options are shown in Table 12.

Table 12. Recapitulation Table for Risk Level Mitigation Options

Asset Aspect	Risk Level	Amount of Risk	Mitigation Options			
			Risk Assumption	Risk Avoidance	Risk Limitation	Risk Transference
Infrastruct	High	3	-	1	2	-

ure of IT	Medium	3	-	1	2	-
	Low	6	-	3	3	-
Zeta Information System	High	0	-	-	-	-
	Medium	5		2	3	-
	Low	5	-	1	3	1
PC User	High	0	-	-	-	-
	Medium	4	-	1	3	-
	Low	0	-	-	-	-
Network Infrastructure	High	1	-	1	-	-
	Medium	0	-	-	-	-
	Low	3	-	3	-	-
Total		30	-	13	16	1

The result of a statement of mitigation options with a total of 30 risk threats. The highest is the value of risk limitation mitigation options with a value of 16 and mitigation options of 1. Mitigation options that will not be taken because the statement does not match the risk threat. The recapitulation of the depiction of the value statement in the mitigation options table is visualized in a graph with the amount of risk presented in Figure 3 which uses a bar graph for each asset, where the image is on the left and a pie chart for each mitigation option is located on the right.

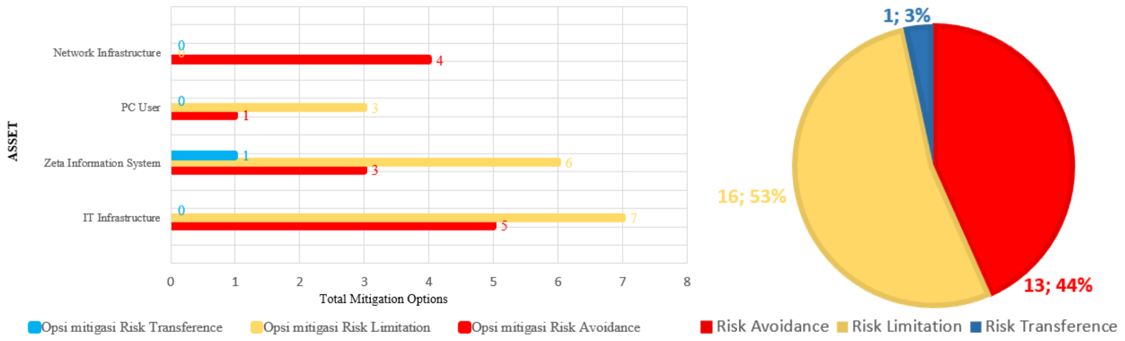

Figure 3. Recap of Asset Mitigation Options (Left) and
Recap of Risk Level Mitigation Options (Right)

The third stage is to conduct a cost-benefit analysis is to do the cost-benefit of analysis in determining control costs to be incurred in order to minimize the risk of higher losses.The application of cost measures adjusted to the latest prices in the risk strategy implementation period. 30 risk statements through mitigation control options to be overcome which have the same way or can be said to have an integrated control aspect, namely the control recommendation choice model in terms of financing. This unit of control is a cost-benefit analysis step in reducing large cost benefits to reduce the risks issued [3].

The fourth stage carries out the process of Select-control implementation of the selected control adjustments as the right implementation to run in the company PT. X through the standardization requirements of the NIST SP 800-53 Rev. 4. Select-control provides a statement for each item, this is considered a statement of review of the implementation of priority action items, aspects of mitigation options with the subsequent assignment of responsibility for managing risk reduction.

The fifth stage in the distribution of the party is hold in control has the authority that is responsible for implementing the risk strategy. These findings include President Directors, Managers, Controllers, and IT Supervisors.

Last stage in risk mitigation is Develop Safeguard Implementation Plan by compiling a list of implementations that will be proposed in the implementation of risk management as a risk strategy decision.

The form of results from the risk mitigation stage of the process of prioritizing actions, recommended evaluating control options, perform cost-benefit analysis of select control, assign responsibilities, which results in a develop arrangement of a safeguard implementation plan. Some examples of develop safeguard implementation plans are presented in Table 13.

Table 13. Control Implementation Plan

No	Asset	Vulnerability	Risk Level	Select Controls	Cost-Benefit		Mitigation Options	Assign Responsibility
					Item	Cost		
1.	Infrastructure of TI	Does not specify personnel or roles to be alerted if a processing failure occurs	High	The company determines the policy of responsibility of each individual sector which is divided into sub-divisions with individual abilities. Like the person in charge, IT support is divided into communication networks, application development, data asset development	Implementation and formal documentation of the policy formation of the role of responsibility is divided by each sub-section in the division viz • 1 employee network • 1 employee in the data asset field • 1 application field employee	Rp. 8.250.000	Risk Avoidance	Project Leader, Controller Staff, IT Supervisor
2.	Zeta system information	There is no initial training for employees to work according to their roles and duties as well as security awareness training on information systems	Medium	The company establishes formal development training for information technology system updates and coordination of sharing discussions between divisions or other individuals	Establish sharing discussion coordination between employees and periodic training related to discipline security compliance	Rp. 2.775.000	Risk Avoidance	Controller Staff, IT Supervisor
3.	Network Infrastructure	There is no management of the amount of bandwidth usage processing	Low	The company regulates the bandwidth control rule divided into each connection and divides and regulates the mechanism of communication channel types, such as Wi-Fi and LAN networks	Implementation of configuration bandwidth control rule limits by IT employees	Rp. 0	Risk Avoidance	IT Supervisor

4.3 Evaluation Risk

The completion stage which is the final part of the NIST SP 800-30 method. This risk evaluation process, as a result of the preparation of the final document on the implementation of the risk control assessment strategy [10]. This final document is formed from the findings of each stage of the NIST SP 800-30 method. The final report produced, determines the consideration of the implementation readiness decisions involving users of the IT system at PT. X. This information security risk strategy must ensure that it is relevant to the aspects of security, confidentiality, integrity, availability of data used for continuous development, improvement and evaluation [11] - [19].

5. Conclusion

Information on security risk strategies using the NIST SP 800-30 method in this study has been implemented quite well. The value process determines the vital assets that are threatened in the use of IT at PT. X. Acquisition of information technology assets that affect aspects of company information security. PT. X there are four assets including IT infrastructure, Zeta information systems, PC users, network infrastructure. The findings of this study are based on four identified assets, there are 30 threats which include 19, medium 17, and high 4 identified risk levels. The results of the dominant risk level on the low scale state that the risk value is quite good, seen from low level 14 high, but almost close to medium level 12, and far from high level 4. control recommendations given to risky threats are the implementation of improvement control through recapitulation. the results of 30 risk mitigation control, risk limitation 16, risk avoidance 13, and risk transfer 1 are categorized as good because they dominate the application of risk limitation from other controls. to defend from distraction. Mitigation controls to reduce the threat of risk by complementing the availability of appropriate security controls to avoid disruption or damage through control recommendations

References

[1] C. A. Wahyuningtyas, I. K. A. Purnawan, N. Made, and I. Marini, “Audit Tata Kelola TI Perusahaan X Dengan COBIT 5,” vol. 7, no. 3, pp. 244–252, 2019.

[2] G. M. A. S. Anak Agung Bagus Arya Wiradarma, “IT Risk Management Based on ISO 31000 and OWASP Framework using OSINT at the Information Gathering Stage (Case Study: X Company),” *Int. J. Comput. Netw. Inf. Secur.*, vol. 11, no. 12, pp. 17–29, 2019.

[3] N. P. S. Merta Suryani, G. M. A. Sasmita, and I. K. A. Purnawan, “Audit of accounting information system using COBIT 4.1 focus on deliver and support domain,” *J. Theor. Appl. Inf. Technol.*, vol. 78, no. 3, pp. 456–463, 2015.

[4] A. David Purba, I. K. Adi Purnawan, and I. P. Agus Eka Pratama, “Audit Keamanan TI Menggunakan Standar ISO/IEC 27002 dengan COBIT 5,” *J. Ilm. Merpati (Menara Penelit. Akad. Teknol. Informasi)*, vol. 6, no. 3, p. 148, 2018.

[5] A. D. Herman Afandi, “Audit Kemanan Informasi Menggunakan Iso 27002 Pada Data Center Pt.Gigipatra Multimedia,” *J. Teknol. Inf. Magister Darmajaya*, vol. 1, no. 02, pp. 175–191, 2015.

[6] Arum, “Manajemen Risiko Strategis,” *Business Lounge Journal*, 2013. [Online]. Available: https://www.blj.co.id/2013/02/23/manajemen-risiko-strategis-1/. [Accessed: 04-Feb-2020].

[7] M. E. Johan, M. F. Rizqon, and I. J. S. Suroso, “University information system security risk assessment using NIST 800-30,” *Int. J. Recent Technol. Eng.*, vol. 8, no. 3, pp. 8380–8385, 2019.

[8] E. Supristiowadi and Y. G. Sucahyo, “Manajemen Risiko Keamanan Informasi pada Sistem Aplikasi Keuangan Tingkat Instansi (SAKTI) Kementerian Keuangan,” *Indones. Treas. Rev. J. Perbendaharaan, Keuang. Negara dan Kebijak. Publik*, vol. 3, no. 1, pp. 23–33, 2018.

[9] D. A. Permatasari, W. Hayuhardhika, N. Putra, and A. R. Perdanakusuma, “Analisis Manajemen Risiko Sistem Informasi E-LKPJ pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur,” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 6, 2019.

[10] G. Stoneburner, A. Gougen, and A. Feringa, *NIST SP 800-30 - Risk Management Guide for Information Technology Systems*, vol. 1. 2002.

[11] W. Syafitri, “Perancangan Manajemen Risiko Keamanan Informasi Dengan Menggunakan Metode NIST 800-30:Studi Kasus Sistem Informasi Akademik (SIMAK) Universitas Islam Negeri Sultan Syarif Kasim Riau,” Universitas Indonesia, 2014.

[12] I. K. A. Purnawan, “Pedoman Tata Kelola Teknologi Informasi Menggunakan It Governance Design Frame Work (Cobit) Pada PT. X,” *Lontar Komput. J. Ilm. Teknol.*

Inf., vol. 6, no. 3, p. 200, 2015.

[13] P. . Prof. Sukardi, *Metodologi Penelitian Pendidikan Tindakan Kelas: Implementasi dan Pengembangannya*. Jakarta: Bumi Aksara, 2015.

[14] M. Swanson, *NIST Special Publication 800-26 : Security Self-Assessment Guide for Information Technology Systems*, vol. 191. 2001.

[15] Penny Pritzker, “NIST SP 800-53A, R4: Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans,” *NIST Spec. Publ. 800-53A, Revis. 4*, no. December 2014, pp. 1–487, 2014.

[16] Rebecca M. Blank, “NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations,” *NIST SP-800-53 Ar4*, p. 400+, 2013.

[17] A. A. Pradana, “Evaluasi manajemen risiko..., Achmad Arthur Pradana R, FASILKOM, 2017,” Univeritas Indonesia, 2017.

[18] RigCERT, “ISO/IEC 27001 - INFORMATION SECURITY,” 2018. [Online]. Available: www.rigcert.org/iso_iec_27001-12.htm. [Accessed: 20-Dec-2019].

[19] U. Nugraha, “Pada Perguruan Tinggi Menggunakan Kerangka Kerja Nist Sp 800-300,” in *Seminar Nasional Telekomunikasi dan Informatika*, 2016, no. Selisik, pp. 121–126.

[20] T. P. SDPPPI, “Pengelolaan Risiko Pengembangan Desa Broadband di Indonesia Pengelolaan Risiko Pengembangan Desa Broadband di Indonesia,” Yogyakarta, 2016.