Syntax Literate: Jurnal Ilmiah Indonesia p–ISSN: 2541-0849 e-ISSN: 2548-1398
Vol. 7, No. 12, Desember 2022

Risk Assessment at it Company by Focusing on Information Security Area Using Iso 27001:2022

Athallariq Rafii Nugroho[1*], Nilo Legowo[2]
[1,2]Master of Information System Management, Bina Nusantara University, Jakarta, Indonesia
Email: [1*]athallariq.nugroho@binus.ac.id, [2]nlegowo@binus.edu

Abstract

Modern technology companies should prioritize information security by focusing on system vulnerabilities and adopting a risk management approach based on the ISO/IEC 27001:2022 standard. This method needs to be implemented through several stages of risk assessment to ensure and measure the extent to which the organization effectively addresses information security issues. The assessment approach involves the three stages of identifying, analyzing and evaluating risks and mapping them to the controls specified in ISO/IEC 27001:2022. The implementation shows that the IT risk assessment of the company has a percentage of 86.87% as low risk, 6.06% as medium risk, and 7.07% as High risk. IT Software companies can be considered safe because most risk assessment findings are low, which means they are in the safe category. In practice, regular monitoring of the implementation of risk assessments in line with the ISO/IEC 27001:2022 standard is still very much needed.

Kata kunci: Risk; Risk Assessment; Information Security; Risk Management; ISO 27001

Introduction

In the current digital era, technology development is rapid, making all businesses and the wider community dependent on technology and the internet. Advances in technological change that occur alone can occur in just hours, minutes, or seconds, especially those related to internet-based technology. So that business activities can be carried out more quickly and efficiently. One of the positive impacts is the increasing use of Software as a Service (SaaS) to support business needs. However, behind all the conveniences and opportunities obtained, there must be seriousness in managing technology. Some factors must be considered in the management of information technology so as not to cause things that are not wanted. One of the factors of concern and having a risk is a factor in information security. This is because technology information and communication may experience interference or problems with information as one of the main objects experiencing security information problems with security information. The security of this information concerns confidentiality, wholeness, and availability. Information systems must evaluate information security to find gaps in secure information. A deficiency information security section.

How to cite:	Athallariq Rafii Nugroho, Nilo Legowo (2002) Risk Assessment at it Company by Focusing on Information Security Area Using Iso 27001:2022, *(7) 12 Desember,*
E-ISSN:	2548-1398
Published by:	Ridwan Institute

All digital information is vulnerable to cyberattacks. According to honeynet project from BSSN, there were 9.6% more cyberattacks in Indonesia in 2021 than in 2020. The two most frequent types of cyberattack are ransomware and data breaches. Therefore, to manage these security concerns, a company must adopt an information security strategy by creating a complete framework that enables an information security program's development, institutionalization, assessment, and improvement. The information security strategy must support the organization’s broad strategic plans, with its content traced back to these higher-level sources.

According to, cyberattacks are attacks on computer or telecommunication networks against other computer or telecommunication networks, such as websites. Internally, IT Software Company still has many information security weaknesses. Information security risk, especially in information technology-based companies, is considerable. Therefore, the Company needs to pay attention to risks related to ISMS. The Information Security Management System (ISMS) is designed according to international standards, which provide the basis for implementing an information security strategy to secure the confidentiality, integrity, and availability of information by implementing a more effective and efficient risk management process. There are still many employees of IT Software Company who were hit by phishing, which resulted in IT Software Company experiencing data loss by hackers, disrupted operations, financial losses, system downtime, and a loss of customer reputation in one of its business products. Based on this, risk identification was carried out, including employee abuse of confidential data, misuse of access to account sharing, lack of documentation, system downtime, etc. Departing from risk identification, it is hoped that later risk Treatment will be prepared to reduce impact. According to, The ISO/IEC 27001 standard is frequently used to identify whether information system security has to be implemented. To create an Information Security Management System (ISMS), it is necessary to adhere to the requirements outlined in ISO/IEC 27001:2022., The ISO/IEC 27001 standard is frequently used to identify whether information system security has to be implemented. To create an Information Security Management System (ISMS), it is necessary to adhere to the requirements outlined in ISO/IEC 27001:2022.

IT Software Company took an approach to one of the information security standards, namely ISO 27001:2022, which was chosen as one of the frameworks used. Based on the ISO 27001:2022 standard, an organization or business can manage and control information security risks to the organization or business while safeguarding the confidentiality, integrity, and availability of information. So, the authors aim to be able to help management and other stakeholders manage information security at IT Software Company by obtaining a basic understanding of risk management signing the scope of Business Software Applications complying with ISO 27001 standards. This study aims to identify the risks that occur in IT Software Company, relating to information security, determines ISO/IEC 27001:2022 controls by handling information security risks at IT Software Company, and measures the level of information security risk at IT Software Company.

Information System and Information Security

Information systems combine various information technology components that produce information to obtain a single line of communication within an organization or group. Information systems comprise interconnected components that collaborate to gather, manipulate, retain, and present data to facilitate decision-making, collaboration, organization, examination, and visualization. Information systems can be used in various organizational processes, including aggregation, dissemination, and management, to help an organization achieve its objectives. Security Information systems can be described as operational systems consisting of all kinds of mechanisms to protect the system from various threats that negatively impact information security and system security. So, it can be concluded that information systems are interconnected components that collect, process, store, and distribute information for decision-making and organizational operations, which combine people, technology, and organized procedures.

Information security is an effort to protect information assets from potential threats. Information security indirectly ensures business continuity, reduces emerging risks, and allows you to optimize return on investment. Meanwhile, Information security involves protecting information from various potential dangers to ensure the continuation of corporate operations, mitigate business risks, and optimise the return on investment and commercial prospects. Information security is an attempt to protect sensitive information from potential harm. As a result, as more and more business information is shared, aggregated, and stored, the risk of loss, theft, or misuse of data increases. Information security is the use of technology, knowledge, and awareness to safeguard the privacy, availability, and accuracy of information and all of its essential components, such as the hardware, software, and devices that use, store, process, and send information. Information security protects the organization’s resources' availability, confidentiality, integrity, and accountability. In addition, information security is an essential concern to companies to keep all information in the company well controlled. Information systems are interconnected components collected, processed, stored, and distributed to support the company in making the best decisions.. In addition, information security is an essential concern to companies to keep all information in the company well controlled. Information systems are interconnected components collected, processed, stored, and distributed to support the company in making the best decisions.

Information security encompasses many measures to safeguard assets, maintain uninterrupted corporate operations, mitigate risk, and maximize return on investment by managing and regulating linked information systems. Information system security aims to protect information assets from dangers posed by careless individuals. Information security can indirectly guarantee business continuity and optimise return on investment. The risk of damage increases with the amount of firm information collected and controlled; therefore, a standard operating procedure (SOP) for information system security is required to assist in the process of handling and prevention in the event of an attack incident so that the attack incident can be prevented and responded to quickly and satisfactorily.

A threat is an action or event that can harm the company with losses in the form of money/costs, effort, business opportunities, and good reputation, and the worst loss is to make the company bankrupt. Threats to information system security are people, organizations, mechanisms, or events that could damage an organization's information assets. Threats are divided into internal and external categories. A threat is any event that, if it occurs, could cause damage to the system and result in a loss of confidentiality, availability, or integrity. Threats can be dangerous, like modifications, intentional exposure to sensitive information, or unintentional exposure, such as errors in transaction calculations or file deletion.

Vulnerability is when people, communities, assets, or systems are more susceptible to hazards due to various social, economic, physical, and environmental factors or processes. Vulnerability is a weakness in a system that threats can exploit. Reduce the vulnerability aspects of the system. Threat to the system. Vulnerability can be assessed according to the level of risk towards the organization, both internally and externally. Low ratings can be applied to vulnerabilities with low levels of damage and exposure.

A Risk Matrix is a matrix employed to assess the degree of risk based on the quantity of occurrences and the resulting consequences. Utilizing a Risk Matrix facilitates the categorization of prevailing risks in the decision-making process undertaken by management, enhancing its efficiency. These methods are essential as they fall into the partial and quantitative techniques categories. Risk assessors are frequently employed within a matrix of risk operations to develop a coherent relationship between the outcome and the Likelihood of the risk assessment of identified risks or potential harm.

Risk is an assessment made by a person or the application of specific knowledge about uncertainty. Meanwhile, risk is uncertainty that harms expectations or goals to be achieved. In addition, risk is defined as an uncertainty that can impact goals. Risk is uncertainty that harms expectations or goals to be achieved. In addition, risk is defined as an uncertainty that can impact goals. The definition of risk is an opportunity or potential that, if not handled appropriately, could have an impact on a goal and result in losses. It can be divided into numerous categories: Strategic Risk, Financial Risk, Compliance, Reputational Risk, and Operational Risk.

Risk management minimizes the potential for unwanted results resulting from daily activities and decisions. Information technology risk management is a process used to identify threats and vulnerabilities to information resources used by organizations. IT managers carry it out to achieve business goals, reduce risks, stabilize costs to achieve benefits, and preserve IT. Meanwhile, others define risk as the possibility of unwanted or unfavorable results, including the possibility of suffering loss, injury, or fire. In terms of risk, no method can guarantee that harmful consequences can be avoided 100 per cent at a particular time unless the actions do not involve activities that contain an element of risk.

Risk Management is a field of science that discusses how an organization applies measures in mapping various existing problems by placing various management approaches comprehensively. Meanwhile, risk management is a series of procedures and methodologies used to identify, measure, monitor, and control risks arising from bank business activities. Risk management is a filter or early warning system for the bank's business activities.

It can be said that risk is the assessment of uncertainty that harms expectations or goals. Risk management is a field of science that assists organizations in overcoming existing problems by applying a comprehensive management approach. Risk management includes procedures and methodologies to identify, measure, monitor, and control risks arising from the bank's business activities, which serve as an early warning system.

Risk assessment is estimating the risk score of auditable units within a company. This risk assessment identifies, measures, and determines the priority of risks so that most resources are directed to areas worth auditing with High-risk scores or weights. Risk assessment could be defined as a systematic procedure that involves evaluating security within a given framework, providing targeted suggestions, and making decision guidance in a project by employing risk analysis, risk projections, and other important information that may impact the process of making decisions. According to, risk assessment is the process of identifying, evaluating, and estimating the level of risk in a given circumstance and it involves comparing the identified risk with established benchmarks or criteria, and establishing the level of risk that is considered acceptable. Performance evaluation can be carried out through three stages of risk assessment:. Performance evaluation can be carried out through three stages of risk assessment.

The primary aim of identifying risk is to systematically identify and analyze all potential hazards, intending to devise effective strategies to eliminate or mitigate significant risks. Identifying risks is foundational in conducting risk evaluation and analysis. Risk identification is a deep process determining what, how, and why conditions or events may occur. The risk identification process is to find, recognize and describe risks that may help or prevent the organization from achieving its goals.

After carrying out risk identification, the next stage is risk analysis. Risk analysis is to understand the nature of risk and its characteristics, including the level of risk where appropriate, by assessing the possible harm's severity and the risk's Likelihood of materializing. The Likelihood of an event occurring is determined extremely subjectively depending on reason and experience. Nevertheless, certain risks are simple to quantify. It is tough to determine the probabilities of an infrequent occurrence.

Thus, it is crucial at this point. To get the best guess, we can prioritize later with adequate planning and risk management for implementation. Difficulty in risk measurement is decisive. Certain dangers do not always have the chance of arising due to the statistical information accessible. Additionally, it can be challenging to assess the intensity of an impact on immaterial assets. Risk analysis is a process to comprehend the nature of risk and to determine the level of risk. Risk analysis process with the basis of the level of risk in the risk matrix in Table.

Table 1. Risk Matrix

			Impact		
			Low	Medium	High
			1	2	3
Likelihood	Rare	1	1 = Low	2 = Low	3 = Medium
	Possible	2	2 = Low	4 = Medium	6 = High
	Probable	3	3 = Medium	6 = High	9 = High

Risk evaluation compares risk analysis results with risk criteria to determine whether the risk and magnitude are acceptable or tolerable. The process commonly used to define risk management will compare the risk level against determined standards, target levels of risk, and other criteria. Risk evaluation is the comparison of analysis of risk outcomes with established risk parameters to ascertain the acceptability or tolerability of the risk and its level. Evaluation objectives are to know the highest-level priority to the lowest and determine which risks are followed up with treatment and whichever risk is monitored. Evaluation objectives are to know the highest-level priority to the lowest and determine which risks are followed up with treatment and whichever risk is monitored.

Risk treatment is a methodical and rational approach that encompasses identifying hazards, determining attitudes and policies, establishing solutions, and implementing monitoring and assessment for every activity or process inside an organization. Risk treatment is a multifaceted decision-making process that draws upon information derived from risk and exposure assessment. According to there are methods of treatment risks, namely.

Table 2. Risk Treatment Description

No.	Risk Treatment	Description
1	Risk Modification	To mitigate the risk level, it is imperative to implement appropriate controls. This will enable a reassessment of the residual risk, ensuring that it falls within an acceptable range.
2	Risk Retention	The decision to continue accepting the risk by not installing further safeguards must be taken after a thorough appraisal of the risk.

3	Risk Avoidance	Refusing to engage in activities or being exposed to conditions that present a specific danger is advisable.
4	Risk Sharing	The risk transfer to a more capable party is advisable based on a thorough risk evaluation.

In the context of a research project on information security risk evaluation using ISO/IEC 27001: 2022, a literature review is conducted as one of the research methodologies used. The first research from [40] concluded that “We have developed an ISMS framework for data centres based on Appendix A ISO 27001. By applying this framework, management is expected to identify, manage, and reduce all information security threats. This framework has more advantages than others designed for government offices and telecommunications companies”.

The second research from said that “The primary aim of this study is to offer suggestions for enhancing the Information Security Management System (ISMS) at the XYZ Ministry in the DRC. This study uses the Index and ISO 27001 evaluation tool developed by our organization as an internal audit instrument for organizational purposes. Additional investigation can take the shape of designing and implementing an integral component of the evaluation procedure”. Also, the third research from said that “According to a series of assessments aimed at determining the level of organizational maturity, it has been observed that the implementation of the Information Security Management System, or ISMS, for short, might become intricate and costly if not comprehended adequately. The human factors present a notable vulnerability in implementing IT security management systems”. Organizational maturity, it has been observed that the implementation of the Information Security Management System, or ISMS, for short, might become intricate and costly if not comprehended adequately. The human factors present a notable vulnerability in implementing IT security management systems”.

The fourth research from concluded that “According to a series of assessments aimed at determining the level of organizational maturity, it has been observed that the implementation of the Information Security Management System, or ISMS, for short, might become intricate and costly if not comprehended adequately. The human factors present a notable vulnerability in implementing IT security management systems”. And the fifth research from said that Risk management is a significant organizational problem for IT governance and computer security. This paper discusses IT risk management at universities because security threats can begin to damage information technology assets and impact the organization. This study still has limitations in access control analysis and creates management risk based on information security”. organization. This study still has limitations in access control analysis and creates management risk based on information security”.

The sixth research from tell that Risk management is a significant organizational problem for IT governance and computer security. This paper discusses IT risk management at universities because security threats can begin to damage information technology assets and impact the organization. This study still has limitations in access control analysis and creates management risk based on information security". The seventh research from concluded that Information security can be achieved by applying appropriate controls, such as policies, processes, procedures, organizational structure, and software and hardware activities. Identifying and choosing the most effective information security control is challenging for the organization".

The eighth research from tell that We propose a more measurable gap analysis method to plan the Information Security Management System (ISMS) using AHP. The highest priority for the XYZ Institute is overseeing security controls in Appendix A. 11 ISO/IEC 27001: 2013 (physical and environmental security). The list generated from this analysis will help the organization prioritize its efforts and resources to the most valuable information security factors. Also, the ninth research from concluded that "a practical methodology for the performance assessment of information security (ISMS) based on ISO 27001 and ISO 27002 standards. Organizations with varied sizes and traits can apply this approach to identify shortcomings and opportunities for improvement. Assessment can be done regularly to capture organizational changes that impact ISMS goals".

And the tenth research from said "ISO 27001 help organization to do calculate the level of maturity according security system technology's gap analysis. And the result of implementation gives some recommendation related to manage the risk management system of information technology security of organization and mapping the organization needs to choose a implementation control for security of information systems aspects". Security of information systems aspects". Based on all research above, ISO/IEC 27001 can be important of access control analysis and identifying effective controls. Besides that, it can be used as a regular performance assessment to identify shortcomings and opportunities for improvement related to company's information security.

ISO 27001:2022 Framework

ISO 27001:2022 is a globally recognized standard that evaluates system specifications and measures system performance in terms of reliability and accuracy to protect information. Meanwhile, ISO 27001:2022 is the standard widely recognized and acknowledged globally as a comprehensive framework for effectively managing organizational information security risks. This standard provides a clear set of guidelines and methodologies that companies can use to ensure the practical implementation of robust information security practices. Furthermore, Information Security Management Systems maintain the confidentiality and integrity of information availability by applying risk management processes and assure interested parties that these risks have been adequately managed. ISO/IEC 27001:2022 has 4 control themes and 93 controls.93 controls.

So, ISO 27001:2022 is a globally recognized standard that evaluates the specification and performance of systems to protect information. This standard provides a comprehensive framework for managing information security risks in organizations, ensuring solid practices, and maintaining confidentiality and integrity through the risk management process.

Research Method

The implementation method is based on ISO/IEC 27001:2022 and combined with risk assessment in ISO/IEC 31000:2013. In ISO/IEC 27001:2022, the author refers to clause 9 (Performance Evaluation). In the risk assessment in ISO/IEC 31000:2018, the author refers to the risk assessment, which is divided into three stages (Risk Identification, Risk Analysis, and Risk Evaluation). Based on the description of the theory, the framework is arranged as follows:

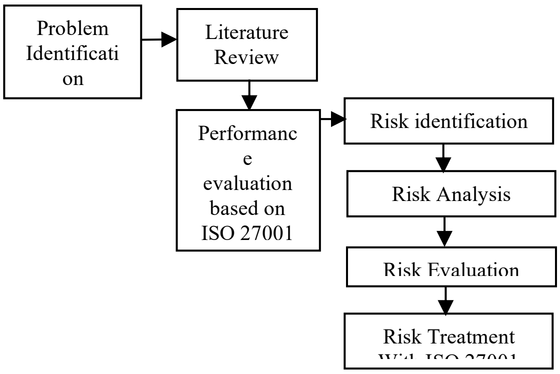

Figure 1. Research framework

The steps taken in this research are to identify the condition of information security risks at the company IT Software Company using interview sessions with some IT stakeholders and to find out the extent of the application of information security implemented. These stages are carried out through interviews with IT Infrastructure, IT Security, Engineers, and Project Managers related to the information security aspect. Detailed steps in Figure 1 are processed with problem identification carried out at an IT Software Company related to identifying the root cause of a problem in the information security system, especially the information security risk section. The next phase is a literature study conducted to add solutions for problem-solving. The content of the literature study is taken from published articles and journals as well as books and relevant international standards that have been published. The next phase does performance evaluation based on ISO 27001 (clause 9) which pertains to continuously monitoring, measuring, analyzing, and evaluating an organization's Information Security Management System (ISMS) to ensure its effectiveness and ongoing maintenance. This clause facilitates the ongoing evaluation of organizational performance about the prescribed standards, aiming for continuous improvement.

The next process is to do risk identification to identify risks that include threats and vulnerabilities. After entering risk analysis, select the analysis and measurement methods using the matrix from Table 1. Risk Matrix to ensure valid results and describe the risk analysis performed. The last phase goes to risk evaluation by doing the treatment. In this phase, the risk assessment measurement matrix outlines the procedure for identifying and evaluating potential risks. It includes a designated individual responsible for overseeing the monitoring and measurement activities. The subsequent individual is responsible for analyzing and reassessing the audit's scope. Subsequently, in this phase, ascertain the outcomes of the risk evaluation by the pre-established matrix. Furthermore, it is essential to ascertain the ongoing implementation of risk reduction measures. In addition, the ISO/IEC 27001:2022 implements treatment measures. It is imperative to communicate the findings of the audited risk assessment to the appropriate management personnel as part of the outcome.

Results And Discussion

After completing the interview session with some stakeholders, the identification of potential risks at the IT Software Company has been given. The potential risk identification results require risk expertise to review. The result shows forty information security risks at the company. Based on risk identification, it was divided into 99 risks that were mapped with a combination of threat and vulnerability. Also, the author determines the mapped results based on the threats and vulnerabilities that have the potential to raise these risks. Then, the risk identification that has been mapped must be reviewed by risk experts. An example of the results of risk identification with a medium-high risk score can be seen in Table 3.

Table 3. Example of risk identification results

No.	Risk description	Threat description	Vulnerability description
1	A decrease in system security after the implementation of changes is conducted	Inconsistency and quality of the results of the implementation of activities	Inadequacy/inadequacy of the rules/provisions/standards for the implementation of activities
2	Implementation of the changes made by the unauthorized person	Changing/removing information by unauthorized people	Inadequacy/Inadequacy Review of Audit Log
3	Incidents and problems related to providing information services and security are not identified/appropriately resolved.	Failure to provide services for users	Inadequacy/inadequacy of system analysis
4	Corporate data leakage intentionally/unintentionally by internal and external parties	Access to information by unauthorized people	Inadequacy/inadequacy of the rules/provisions/standards for the implementation of activities

5	Termination of business operations	Business continuity	Inadequacy/inadequacy of planning and preparation for disaster recovery
6	Rules related to information security are not conducted consistently by company personnel.	Inconsistency and quality of the results of the implementation of activities	Inadequacy/inadequacy of the rules/provisions/standards for the implementation of activities
7	Rules related to information security are not conducted consistently by company personnel.	Inconsistency and quality of the results of the implementation of activities	Inconsistency in the implementation of activities based on the rules/provisions/standards that have been set
8	Dissemination of company data to outside parties by the company's internal personnel	Misuse of company data	Inadequacy/inadequacy of the rules/provisions/standards for the implementation of activities
9	Dissemination of company data to outside parties by the company's internal personnel	Misuse of positions/authority for illegal activities, such as embezzlement/lower (fraud), theft/sales of company information, etc.	Inadequacy/inadequacy of control and monitoring of management rights management
10	Dissemination of company data to outside parties by the company's internal personnel	Loss/theft of company information (other than through cyber/cyberattack attacks), for example, due to negligence of personnel, espionage actions, or social engineering	Inadequacy/inadequacy of controlling and monitoring human resource activities related to information security
11	Information in the main application is illegally modified	Changing/removing information by unauthorized people	Inadequacy/Inadequacy Review of Audit Log
12	Information in the main application is illegally modified	Misuse of positions/authority for illegal activities, such as embezzlement/lower (fraud), theft/sales of company information, etc.	Inadequacy/Inadequacy Review of Audit Log
13	Lawsuits/penalties/withdrawal of permits/cooperation against the company	Non -compliance with regulations/provisions/agreements from/with external/government parties	Inadequacy/inadequacy of control and monitoring of company compliance with regulations/provisions/agreements from/with external/government parties

At this stage, after risk identification is finished. The risks contained in IT Software Company are analyzed by focusing on the assessment score for impact and Likelihood that combined become the risk score. The process starts with the results of risk analysis by conducting interview techniques to conduct risk assessments. Then, the author carries out the stages for determining the risk with the following process:

Interview process to determine the threat and vulnerability of a risk. Assessing the magnitude of the impact value that occurs from a risk by looking at the impact measurement scale between Low (1) / Medium (2) / High (3). predetermined risk matrix

/ 3. Assess the likelihood of a risk occurring by looking at the likelihood scale between Rare (1)/ Possible (2)/ Probable (3). After the impact and likelihood values have been obtained. Then multiply the two values to find out the value of the risk amount. The assessment can be based on the risk matrix from table 1. After the risk value is obtained through the calculation of table 4.1, the process of determining whether the value obtained is in the low/medium/high risk category. Where medium and high risks require further action.

After determining the value and category of risk obtained through the above process, calculations can be made to determine the total risk for each category at IT Software Company for the scope of Business Software Application using the following formula:

$$\text{Percentage of Finding Categories: } \frac{"Number\ of\ Finding\ Per\ Categories"}{"Total\ Number\ of\ Findings"} X\ 100\%$$

Risk findings for each category in IT Software Company based on the results of risk analysis are figured out on table 4 below.

Table 4. Percentage of risk analysis

Category	Description	Total Risk	Percentage (%)
Low	At present, there is no immediate course of action to be pursued.	86	86.87
Medium	The need for action and continuous monitoring may be necessary.	6	6.06
High	Urgent intervention is necessary	7	7.07

Based on risk analysis, authors do risk evaluation to know what the best method for risk treatment is based on Table 2. The focus for risk treatment for risk that has risk scores of Medium and High only. Because that risk needs to be extra controlled to minimize the risk score, by judgment calls and approval from stakeholders, the results for Medium and High-risk scores can be seen in Table 6.

Table 5. List of risks that have unacceptable status

No.	Risk description	Risk level			Risk Treatment
		Impact	Likelihood	Risk Score	
1	A decrease in system security after the implementation of changes is conducted	3 = High	2 = Possible	6 = High	Risk modification
2	Implementation of the changes made by the unauthorized person	3 = High	2 = Possible	6 = High	Risk modification

3	Incidents and problems related to the provision of information services and security are not identified/ resolved properly	2 = Medium	2 = Possible	4 = Medium	Risk modification
4	Corporate data leakage intentionally/unintentionally by internal and external parties	2 = Medium	2 = Possible	4 = Medium	Risk modification
5	Termination of business operations	3 = High	1 = Rare	3 = Medium	Risk sharing
6	Rules related to information security are not conducted consistently by company personnel	3 = High	3 = Probable	9 = High	Risk modification
7	Rules related to information security are not conducted consistently by company personnel	3 = High	3 = Probable	9 = High	Risk modification
8	Dissemination of company data to outside parties by the company's internal personnel	3 = High	3 = Probable	9 = High	Risk modification
9	Dissemination of company data to outside parties by the company's internal personnel	3 = High	2 = Possible	6 = High	Risk modification
10	Dissemination of company data to outside parties by the company's internal personnel	2 = Medium	2 = Possible	4 = Medium	Risk modification
11	Information in the main application is illegally modified	3 = High	2 = Possible	6 = High	Risk modification
12	Information in the main application is illegally modified	3 = High	1 = Rare	3 = Medium	Risk modification
13	Lawsuits/penalties/withdrawal of permits/cooperation against the company	3 = High	1 = Rare	3 = Medium	Risk modification

After the mapped risk treatment is done, the next process is to do risk treatment by defining the appropriate control for all risks that need treatment and mapping the control with ISO 27001:2022 Control. The result of this process can be shown below:

Table 6. Risk Treatment

No.	Risk description	Risk control description	ISO 27001:2022 Control
1	A decrease in system security after the implementation of changes is conducted	Security standards are compiled in full and adequate	5.8 Information security in project management 8.26 Application security requirements 8.27 Secure system architecture and engineering principles 8.29 Security testing in development and acceptance
2	Implementation of the changes made by the unauthorized person	Monitoring of the log implementation log is conducted periodically	8.15 Logging
3	Incidents and problems related to providing information services and security are not identified/appropriately resolved.	The mechanism of reporting, recording, and solving incidents and problems is compiled in full and adequate	5.37 Documented operating procedures 6.8 Reporting information security events 5.25 Assessment and decision on information security events 5.26 Response to information security incidents

			5.27 Learning from information security incidents 5.28 Collection of evidence
4	Corporate data leakage intentionally/unintentionally by internal and external parties	VPN access is given only to personnel who have received approval from the authorities	6.7 Remote working
5	Termination of business operations	Make DRC on the cloud	5.29 Information security during disruption
6	Rules related to information security are not conducted consistently by company personnel.	Mechanisms for planning, implementing, and reporting audit results are prepared in complete and adequate	8.34 Protection of information systems during audit testing 5.35 Independent review of information security 5.36 Compliance with policies, rules and standards for information security 8.8 Management of technical vulnerabilities
7	Rules related to information security are not conducted consistently by company personnel.	The audit of the implementation of information security is conducted regularly	8.34 Protection of information systems during audit testing 5.35 Independent review of information security 5.36 Compliance with policies, rules and standards for information security 8.8 Management of technical vulnerabilities
8	Dissemination of company data to outside parties by the company's internal personnel	Rules/provisions related to the delivery of information and use of electronic messaging arranged in full and adequate	5.14 Information transfer 6.6 Confidentiality or non-disclosure agreements
9	Dissemination of company data to outside parties by the company's internal personnel	Access for auditors to obtain audit data is limited by the scope and audit period	8.34 Protection of information systems during audit testing
10	Dissemination of company data to outside parties by the company's internal personnel	• Socialization/ training related to information security is conducted regularly. • Enforcement of personnel activities that resulted in leakage of company information conducted by the authorities. • Employee recruitment is conducted through background checks	5.4 Management responsibilities 6.3 Information security awareness, education and training 5.17 Authentication information 8.1 User endpoint devices 7.7 Clear desk and clear screen 8.19 Installation of software on operational systems 5.14 Information transfer 5.32 Intellectual property rights 6.2 Terms and conditions of employment 6.4 Disciplinary process 6.1 Screening 6.5 Responsibilities after termination or change of employment
11	Information in the main application is illegally modified	• Information modification activities in the application are recorded in the Audit Trail and reviewed regularly. • Information modification activities in the database are recorded in the trail audit and reviewed regularly. • Log files are protected and can only be accessed by authorized personnel	8.15 Logging 5.33 Protection of records
12	Information in the main application is illegally modified	System administrator activities are recorded in the trail audit and regularly reviewed	8.15 Logging

13	Lawsuits/penalties/withdrawal of permits/cooperation against the company	• Legislation is identified as a reference in conducting company compliance. • Obligations that must be met (against the Certification Agency or external parties) are identified as a reference in conducting company compliance	5.31 Legal, statutory, regulatory and contractual requirements 5.32 Intellectual property rights

Conclusion

Based on the results of this study, several conclusions can be drawn, namely, the risk assessment of IT Software Company for the focus on business software applications shows that 86.87% of the risk is identified as low risk, 6.06% as Medium risk, and 7.07% as High risk. Based on the security category, customer data at IT Software Company is included in the safe category. This is shown by the total medium risk of six and the total High risk of 7. The application of the international standard ISO / IEC 27001: 2013 is very helpful for companies in mapping the various risks that arise related to information system security management, so that the risks that arise and their impact can be minimised properly. Based on the research results that have been concluded, there are suggestions for further research so that the risk assessment that has been carried out can be measured against the residual risk of risks that have been mitigated against risks that have been mapped with the ISO 27001: 2022 standard. This is necessary in order to measure the risks that have been mitigated to determine the effectiveness of implementation in an organization

BIBLIOGRAPHY

M. A. Manuhutu et al., Pengantar Forensik Teknologi Informasi. Yayasan Kita Menulis, 2021.

I. Y. Sari et al., Keamanan Data dan Informasi. Yayasan Kita Menulis, 2020.

S. Siswanti, “Penilaian Kematangan Proses Keamanan Sistem Informasi Pendaftaran Pasien Menggunakan Framework Cobit 4.1,” SATIN-Sains dan Teknologi Informasi, vol. 9, no. 1, pp. 123–133, 2021.

N. R. Mosteanu, “Artificial intelligence and cyber security–face to face with cyber attack–a maltese case of risk management approach,” Ecoforum Journal, vol. 9, no. 2, 2020.

M. Farhat, V., B., R. Raysman, and J. Canale, “Cyber Attacks: Prevention and Proactive Responses. Practical Law.”

A. F. Basyarahil, H. M. Astuti, and B. C. Hidayanto, “Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya,” Jurnal Teknik ITS, vol. 6, no. 1, pp. 116–121, 2017.

C. Chazar, “Standar Manajemen Keamanan Informasi Berbasis ISO/IEC 27001: 2015,” Jurnal Informasi, 2015.

J. Seah and R. Ridho, "PERANCANGAN SISTEM INFORMASI PERSEDIAAN SUKU CADANG UNTUK ALAT BERAT BERBASIS DESKTOP PADA CV BATAM JAYA," JURNAL COMASIE, 2020.

I. Ava Dianta, E. Zusrony, and S. Tinggi Elektronika dan Komputer, "Analisis Pengaruh Sistem Keamanan Informasi Perbankan pada Nasabah Pengguna Internet Banking Analysis of Influence of Banking Information Security System to Internet Banking User Customer," Intensif, vol. 3, no. 1, pp. 2549–6824, 2019.

A. N. Puriwigati and U. M. Buana, "Sistem Informasi Manajemen-Keamanan Informasi," May, 2020.

ISO, "ISO/IEC 27001: 2013." 2013. [Online]. Available: https://www.iso.org/

S. Amraoui, M. Elmaallam, B. H., and K. A, "Information Systems Risk Management: Litterature Review," Computer and Information Science, vol. 12, no. 3, p. 1, 2019, doi: 10.5539/cis.v12n3p1.

R. Akbar, S. Jarot, and P. Firman, "ICIMTech 2020:," in International Conference on Information Management and Technology : 13-14 August 2020, 2020.

A. C. Laksono and Y. Prayudi, "Threat Modeling Menggunakan Pendekatan STRIDE dan DREAD untuk Mengetahui Risiko dan Mitigasi Keamanan pada Sistem Informasi Akademik," 2021.

P. D. Intika and U. M. Buana, "Sistem Informasi Manajemen: Perkembangan Sistem Pengembangan Sistem Informasi Dosen Pengampu," 2020.

M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study," Arab J Sci Eng, vol. 45, no. 4, pp. 3171–3189, 2020, doi: doi.org/10.1007/s13369-019-04319-2.

R. Hidayat and Y. Widara, "MITIGATION MODEL FOR RISK HANDLING," ISLAMIC EDUCATION INSTITUTIONS, vol. 1, no. 1, 2023.

E. K. Szczepaniuk, Hubert. Szczepaniuk, Tomasz. Rokicki, and B. Klepacki, "Information security assessment in public administration," Comput Secur, vol. 90, 2020, doi: 10.1016/j.cose.2019.101709.

American Bureau of Shipping, "RELIABILITY-CENTERED MAINTENANCE," 2004.

N. Kovačević, A. Stojiljković, and M. Kovač, "Application of the matrix approach in risk assessment," Operational Research in Engineering Sciences: Theory and Applications, vol. 2, no. 3, pp. 55–64, Dec. 2019, doi: 10.31181/oresta1903055k.

R. Ilyas, "Analisis Risiko Pembiayaan Bank Syariah," BISNIS : Jurnal Bisnis dan Manajemen Islam, vol. 7, no. 2, p. 189, 2019, doi: 10.21043/bisnis.v7i2.6019.

N. A. Prisidiyani and A. H. Prasetyo, "Pedoman Risiko, Struktur Risiko, dan Asesmen Risiko PT XYZ Tahun 2022-2023," Journal of Emerging Business Management and Entrepreneurship Studies, vol. 2, no. 2, pp. 86–108, 2022, doi: 10.34149/jebmes.v2i2.77.

M. A. Pranatha, Moeljadi, and E. Hernawati, "Penerapan Enterprise Risk Management Dalam," Ekonomi dan Bisnis, vol. 5, no. 1, pp. 17–42, 2018.

K. B. Mahardika, A. F. Wijaya, and A. D. Cahyono, "MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000 : 2018 (STUDI KASUS: CV. XY)," Sebatik, vol. 23, no. 1, 2019.

D. L. Fitrani, “Assessment and Development of Access Control Information Security Governance Based on ISO 27001:2013 at XYZ University,” Jurnal Teknik Informatika dan Sistem Informasi, vol. 9, no. 2, pp. 891–907, 2022.

B. S. Deva and R. Jayadi, “Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan System Integrator Menggunakan Metode Octave Allegro,” J. Teknol. dan Inf., 2022.

F. Pradana, F. A. Bachtiar, and B. Priyambadha, “Pengaruh Elemen Gamification Terhadap Hasil Belajar Siswa Pada E-Learning Pemrograman Java,” Semnasteknomedia, no. February, pp. 7–12, 2018.

W. C. Pamungkas and F. T. Saputra, “Evaluasi Keamanan Informasi Pada SMA N 1 Sentolo Berdasarkan Indeks Keamanan Informasi (KAMI) ISO/IEC 27001:2013,” J. Sist. Komput. dan Inform, vol. 1, no. 2, p. 101, 2020, doi: 10.30865/json.v1i2.1924.

Ahmad Suhaimi, M.A, “Studi Manajeman Risiko Pada Bank Syariah Indonesia (Bsi),” Jurnal Manajemen Risiko, vol. 2, no. I, pp. 73–78, 2021, doi: 10.33541/mr.v2ii.3438.

J. G. Landol, The Security Risk Assessment Handbook. Abingdon: CRC Press, 2021.

N. Legowo and Y. Juhartoyo, “Risk Management; Risk Assessment of Information Technology Security System at Bank Using ISO 27001,” Journal of System and Management Sciences, vol. 12, no. 3, pp. 181–199, 2022, doi: 10.33168/JSMS.2022.0310.

T. R. Peltier, Risk management: The facilitated risk analysis and assessment process. 2013. doi: 10.1201/b15573.

H. Sarvari, A. Valipour, N. Yahya, N. M. D. Noor, M. Beer, and N. Banaitiene, “Approaches to risk identification in public–private partnership projects: Malaysian private partners’ overview,” Adm Sci, vol. 9, no. 1, Mar. 2019, doi: 10.3390/admsci9010017.

I. P. A. E. Pratama and M. T. S. Pratika, “Manajemen Risiko Teknologi Informasi Terkait Manipulasi dan Peretasan Sistem pada Bank XYZ Tahun 2020 Menggunakan ISO 31000:2018,” Jurnal Telematika, vol. 15, no. 2, pp. 63–70, 2020.

I. Putu, A. Eka, P. #1, and T. S. Pratika, “Manajemen Risiko Teknologi Informasi Terkait Manipulasi dan Peretasan Sistem pada Bank XYZ Tahun 2020 Menggunakan ISO 31000:2018,” Jurnal Telematika, vol. 15, no. 2, 2020.

ISO, “ISO/IEC 31000: 2018,” vol. 95, no. 7, pp. 777–778, 2018, doi: 10.5594/j09750.

S. Jikrillah, M. Ziyad, and D. Stiadi, “ANALISIS MANAJEMEN RISIKO TERHADAP KEBERLANGSUNGAN USAHA UMKM DI KOTA BANJARMASIN,” 2021.

R. Hidayat and Y. Widara, “MITIGATION MODEL FOR RISK HANDLING IN ISLAMIC EDUCATION INSTITUTIONS,” 2023.

Y. Bruinen de Bruin et al., “Initial impacts of global risk mitigation measures taken during the combatting of the COVID-19 pandemic,” Saf Sci, vol. 128, Aug. 2020, doi: 10.1016/j.ssci.2020.104773.

D. Achmadi, Y. Suryanto, and K. Ramli, “On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center,” 2018 International Workshop on Big Data and Information Security, IWBIS 2018, pp. 149–157, 2018, doi: 10.1109/IWBIS.2018.8471700.

F. Wijayanti, D. I. Sensuse, A. A. Putera, and A. Syahrizal, "Assessment of Information Security Management System: A Case Study of Data Recovery Center in Ministry XYZ," 2020 3rd International Conference on Computer and Informatics Engineering, IC2IE 2020, pp. 393–398, 2020, doi: 10.1109/IC2IE50715.2020.9274574.

J. Velasco, R. Ullauri, L. Pilicita, B. Jacome, P. Saa, and O. Moscoso-Zea, "Benefits of implementing an ISMS according to the ISO 27001 standard in the ecuadorian manufacturing industry," Proceedings - 3rd International Conference on Information Systems and Computer Science, INCISCOS 2018, vol. 2018-Decem, pp. 294–300, 2018, doi: 10.1109/INCISCOS.2018.00049.

A. Nechai, E. Pavlova, T. Batova, and V. Petrov, "Implementation of Information Security System in Service and Trade," IOP Conf Ser Mater Sci Eng, vol. 940, no. 1, 2020, doi: 10.1088/1757-899X/940/1/012048.

N. Mumtaz, "Analysis of information security through asset management in academic institutes of Pakistan," 2015 International Conference on Information and Communication Technologies, ICICT 2015, 2016, doi: 10.1109/ICICT.2015.7469581.

Angraini, Megawati, and L. Haris, "Risk Assessment on Information Asset an academic Application Using ISO 27001," 2018 6th International Conference on Cyber and IT Service Management, CITSM 2018, no. Citsm, pp. 1–4, 2019, doi: 10.1109/CITSM.2018.8674294.

H. Khajouei, M. Kazemi, and S. H. Moosavirad, "Ranking information security controls by using fuzzy analytic hierarchy process," Information Systems and e-Business Management, vol. 15, no. 1, pp. 1–19, 2017, doi: 10.1007/s10257-016-0306-y.

O. C. Briliyant, J. Widhi Candra, and S. Rebeca Tamba, "ISMS Planning Based On ISO / IEC 27001 : 2013 Using Analytical Hierarchy Process at Gap Analysis Phase (Case Study : XYZ Institute)," 1th International Conference on Telecommunication Systems Services and Applications (TSSA), vol. 4, no. 4, pp. 4–9, 2016.

V. Monev, "Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002," 2020 34th International Conference on Information Technologies, InfoTech 2020 - Proceedings, no. September, pp. 17–18, 2020, doi: 10.1109/InfoTech49733.2020.9211066.

C. Hsu, T. Wang, and A. Lu, "The impact of ISO 27001 certification on firm performance," Proceedings of the Annual Hawaii International Conference on System Sciences, vol. 2016-March, pp. 4842–4848, 2016, doi: 10.1109/HICSS.2016.600.

A. Y. Eskaluspita, "ISO 27001:2013 for Laboratory Management Information System at School of Applied Science Telkom University," in IOP Conference Series: Materials Science and Engineering, IOP Publishing Ltd, Aug. 2020. doi: 10.1088/1757-899X/879/1/012074.

Y. Kurii and I. Opirskyy, "Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001:2013," 2022.