Opsi
Vol. 19, No. 1, June 2026
p-ISSN 1693-2102
e-ISSN 2686-2352

From standards to practice: Applying ISO/IEC 27005:2022 for information security risk management in regional water company

Andi Hary Akbar [1], Heri Wijayanto [1], I Wayan Agus Arimbawa [1], Riza Prapascatama Agusdin [2,3*], Andika Rifai [3], Athaya Rizqia Fitriani [3]

[1]Informatics Department, Universitas Mataram, Nusa Tenggara Barat 83116, Indonesia
[2]Sirindhon International Institute of Technology, Thammasat University, Pathum Thani 12121, Thailand
[3]Informatics Department, Universitas Pembangunan Nasional Veteran Yogyakarta, Yogyakarta 55283, Indonesia

***Corresponding Author**: rizapra@upnyk.ac.id

Article history:
Received: 10 November 2025
Revised: 4 December 2025
Accepted: 12 December 2025
Published: 30 July 2026

Keywords:
Information security risk management
Information technology assets
ISO/IEC 27001:2022
ISO/IEC 27005:2022
Regional water company

ABSTRACT

Regional water companies have increasingly adopted information technology to support their operations. However, the absence of formalized information security risk management procedures can lead to substantial operational disruptions and financial losses. Therefore, this study aims to conduct a systematic risk assessment of a regional water company based on its IT assets, utilizing the ISO/IEC 27005:2022 standard. Data collection through semi-structured interviews and questionnaires with the company's IT department identified 31 assets, which were subsequently used for risk mapping and assessment. The assessment identified a total of 265 risk scenarios, categorized into 10 High (3.77%), 68 Medium (25.66%), and 187 Low (70.57%) level risks. Following the evaluation where all risks were deemed unacceptable, risk modification was recommended as treatment for all risk scenarios. Based on the results of the risk assessment, control recommendations were developed according to ISO/IEC 27001:2022 to assist the company in managing and mitigating risks. The implementation of the two ISO standards aligns to comprehensively map risks and provide a structured mitigation plan. These results are expected to assist the company in establishing formal risk management procedures and maintain business process continuity and effectiveness.

DOI:
https://doi.org/10.31315/opsi.v19i1.15917

1. INTRODUCTION

The utilization of Information Technology (IT) in the era of Industry 4.0 has been widely adopted by most companies. Effective use of IT is believed to significantly influence organizational development through knowledge enhancement, information dissemination, and innovation [1]. This is driven by the fact that companies leveraging IT are able to obtain information and process data more rapidly, accurately, and efficiently [2], [3]. IT products such as software design and system optimization play a crucial role in reducing processing time and increasing operational efficiency [3].

While the use of information technology offers many benefits, leading to increased dependence on it, the use of IT also creates new information security risks [4], [5]. Some of these risks include data breaches [6], malware attacks [7] including viruses and ransomware [8], system disruptions [9], and the theft of important information [10]. These information security risks can lead to problems for organizations [11], including operational disruptions, financial losses [10], and damage to their reputation [12]. Information security risk is an important issue in infrastructure sectors, such as water supply utilities, given their role in public services [13]. Public service companies need to constantly maintain system security so that it always runs optimally, efficiently, and sustainably [14]. These organizations use IT for various operational aspects [15], including new installations, meter reading, service complaints, service information, billing information, and electronic procurement systems.

For this risk context, a specific case can be observed in a regional water company located in Mataram City, West Lombok. This company previously experienced a malware attack that significantly disrupted its business processes and resulted in financial losses. The malware attack prevented customers from paying their bills that were due in the near future, resulting in the company not receiving the amount of money it should have. This disruption also reduced customer trust because the security of private data could not be guaranteed when the system was infected with malware. This condition was further worsened by the absence of formal procedures or adequate standard documentation for information security risk management within the organization. The lack of such guidelines reflects a weakness in the current risk mitigation and incident response mechanisms [16]. Incident responses tend to be reactive and heavily dependent on individual experience, increasing the likelihood of repeat incidents and hindering effective decision-making. The absence of a systematic approach also makes it difficult for organizations to prioritize risks, assign responsibilities, and implement long-term preventive measures. Therefore, a standardized and systematic framework is needed so that risk management activities can be carried out in a clear, measurable, and replicable manner.

Consequently, the absence of formal guidelines can be addressed by applying a structured and systematic approach, such as using widely recognized standards to provide the necessary guidance [17], [18]. While various standards and frameworks exist, including NIST SP 800-30 [19], Fair Analysis of Information Risk (FAIR) [20], and Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) [21]. The ISO/IEC 27000 series is also recognized as the primary international standard for information security management systems [22]. Within this series, ISO/IEC 27005 specifically provides detailed guidance for the information security risk management process [23]. Therefore, this research uses the latest version of this standard, ISO/IEC 27005:2022 [24].

Unlike the 2018 version often cited in previous studies [25], the ISO/IEC 27005:2022 edition offers clear advantages by shifting from a cyclical model to a more flexible iterative process and simplifying workflows by turning risk acceptance into a clear decision point. In addition, the updated standard explicitly includes specific components for documented information and directly aligns its structure with the security controls of ISO/IEC 27001:2022. This comprehensive alignment facilitates seamless integration between risk assessment results and treatment plans, providing a robust framework that is particularly beneficial for organizations establishing formal risk management procedures for the first time. Therefore, this study refers to ISO/IEC 27001:2022 [26], specifically Annex A, as a reference for relevant control recommendations [27].

Previous studies combining these standards for risk assessment and management left several gaps. Putra and Suwito [25] combined ISO/IEC 27005:2018 with NIST SP 800-30, but this earlier version lacks the direct structural alignment that the 2022 edition provides. Kurniawan and Salma [28] confirmed the standard's value in identifying risks, yet they did not ground their control recommendations in ISO 27001, which weakens the objectivity and completeness of their mitigation strategies.

Two gaps stand out. Researchers have rarely applied ISO/IEC 27005:2022 within regional water companies, particularly organizations that are only beginning to build formal risk management procedures. Some studies also skip direct integration with ISO/IEC 27001 controls, a gap that limits how practical their recommendations become.

The objective of this research is to assess information security risk at the regional water company using the ISO/IEC 27005:2022 framework, map the resulting risks to determine treatment priorities, and recommend controls drawn from ISO/IEC 27001:2022. These steps will help the company build formal procedures for information security risk management and sustain the continuity and effectiveness of its business processes.

2. METHODS

This research began with a preliminary study stage to identify and validate the research problem at the regional water company. Initial semi-structured interviews with managers and technical staff from the company's IT department confirmed that despite previous security incidents, the organization lacked formal risk management procedures. This finding justified the application of the ISO/IEC 27005:2022 standard framework as the methodological basis for the study.

To ensure accurate data acquisition, we used specific data collection tools. Semi-structured interviews were conducted to identify critical assets and map business processes, with the data collected using a spreadsheet form designed to be filled out independently. This file included clear instructions and used a combination of checklists for checking assets and blank spaces for providing specific details. Through this form, respondents also rated how often threats might happen (likelihood) and estimated the potential impact on operations using a scale from 1 (Minor) to 5 (Catastrophic).

The main methodology of this research adopted the risk management process from ISO/IEC 27005:2022. The research workflow, as illustrated in Figure 1, followed systematic standard stages: starting with context establishment, continuing with risk assessment and risk treatment, and ending with providing control recommendations [24]. Control recommendations were based on Annex A of ISO/IEC 27001:2022 [26]. The risk assessment process under this standard is structured into several sequential stages, which are detailed in the following sections.

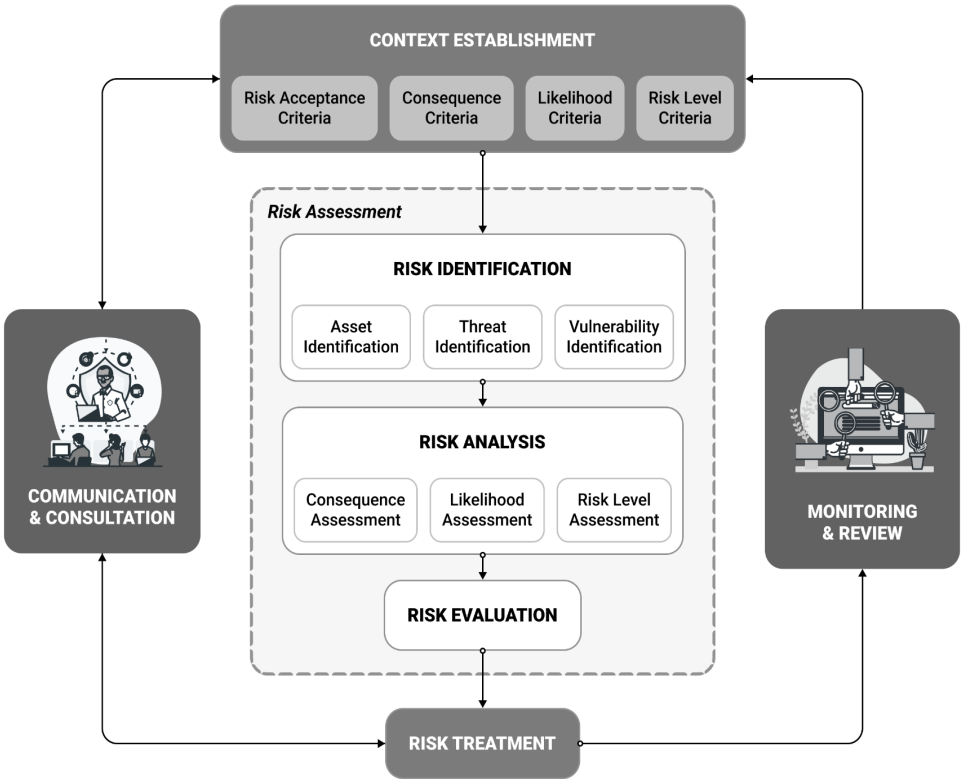

Figure 1. Research process based on ISO/IEC 27005:2022

2.1. Context Establishment

The context establishment stage aimed to set the scope and basic risk criteria at the regional water company. Through discussions and analysis of company documents, specific risk criteria were established to ensure a consistent assessment process [24].

First, to standardize the decision-making process regarding risk treatment, specific acceptance criteria were defined. Standardized decision-making models provide a robust basis for determining complex priority levels and reducing subjectivity [29]. These criteria were developed based on ISO/IEC 27005:2022 guidelines and modified to align with the company's risk appetite. The detailed classifications for risk acceptance are presented in Table 1.

Table 1. Risk acceptance criteria

Level	Description
Low	Acceptable risk with minor treatment
Medium	Acceptable risk with monitoring, control recommendations, and handling
High	Risks not accepted, requiring handling and control recommendations

Following the acceptance criteria, the potential impact of risks on business operations was quantified. The consequence criteria were adapted from the ISO/IEC 27005:2022 standard and adjusted through discussions with management to cover operational, financial, reputational, and service aspects. Table 2 details the specific parameters used to measure these consequences.

Table 2. Consequence criteria

Consequences	Operational	Financial	Reputation	Company Services
Catastrophic (5)	Business process delay > 300 minutes	Loss > IDR 500,000,000	Severe reputational damage, national media coverage	Halts ≥ 5 company service processes
Critical (4)	Business process delay 181-300 minutes	Loss IDR 300,000,001 - 500,000,000	Significant reputational damage, local media coverage	Halts 4 company service processes
Serious (3)	Business process delay 61-180 minutes	Loss IDR 100,000,001 - 300,000,000	Moderate reputational damage affecting a small number of customers	Halts 3 company service processes
Significant (2)	Business process delay 31-60 minutes	Loss IDR 50,000,001 - 100,000,000	Minor reputational damage, limited to internal or small groups	Halts 2 company service processes
Minor (1)	Business process delay ≤ 30 minutes	Loss ≤ IDR 50,000,000	No impact on company reputation	Halts < 1 company service process

In parallel with the consequence analysis, the probability of risk likelihood was assessed. The likelihood criteria were primarily adopted from the ISO/IEC 27005:2022 guidelines and subsequently validated by the company. This validation ensured that the frequency scales reflected the actual occurrence of specific threats and vulnerabilities as recorded in the company's historical incident logs, rather than relying on general security perceptions. By formulating and reviewing the possibility of risks occurring, it is possible to understand the preventive measures that can be taken [30]. Table 3 outlines the scale used to estimate this likelihood.

Table 3. Likelihood criteria

Likelihood	Description
Almost Certain (5)	Occurs >12 times a year
Very Likely (4)	Occurs 10-12 times a year
Likely (3)	Occurs 6-9 times a year
Rather Unlikely (2)	Occurs 2-5 times a year
Unlikely (1)	Occurs once a year

Finally, to determine the overall severity of each identified risk scenario, the values from the likelihood and consequence criteria are combined. This combination forms a mapping tool that dictates the final risk level, as adapted from the ISO standard to fit the organization's context. To mitigate risk, it is necessary to identify and rank each risk that could affect the company's IT assets using the level criteria [31]. Table 4 illustrates the risk level matrix used for this calculation.

Table 4. Risk level matrix

Likelihood	Consequences				
	Catastrophic (5)	**Critical (4)**	**Serious (3)**	**Significant (2)**	**Minor (1)**
Almost Certain (5)	High	High	High	Medium	Medium
Very Likely (4)	High	High	Medium	Medium	Medium
Likely (3)	High	High	Medium	Medium	Medium
Rather Unlikely (2)	Medium	Medium	Medium	Low	Low
Unlikely (1)	Medium	Low	Low	Low	Low

2.2. Risk Identification

The risk identification stage aimed to determine potential risk scenarios based on company assets. This process began with asset identification, covering various categories such as information, hardware, software, networks, personnel, and site. Next, threat identification was conducted based on standard classifications, including physical, natural, infrastructure failure, technical, human action, service violations, and organizational threats. Lastly, vulnerability identification was performed, focusing on weaknesses that could be exploited by threats to cause a negative impact on the company.

2.3. Risk Analysis

After all risks were identified, the next stage was risk analysis. This stage aimed to better understand the characteristics of each risk scenario [32]. Likelihood assessment, as the first step, aimed to evaluate the chance of a risk occurring within one year. The next stage was the consequence assessment, which determined the impact the company would feel if a risk occurs. The impact value for each asset was determined through confirmation with the company. Once the likelihood and impact data for each risk were obtained, the next step was to determine the risk level by considering the risk matrix.

2.4. Risk Evaluation

The third stage of the risk assessment aims to determine which risks are acceptable and which are not acceptable to the organization [33]. The risk acceptance criteria play a crucial role in evaluating each identified risk. The results of the risk evaluation then serve as the basis for determining the most appropriate risk treatment for each identified risk in the subsequent stage.

2.5. Risk Treatment

The next stage was risk treatment. Based on the characteristics and levels of each scenario, the appropriate risk treatment was then determined [34]. There were four main treatment options: risk mitigation or modification, risk avoidance, risk sharing, and risk retention [24]. After a treatment option was selected, specific control recommendations were developed to implement it. This research used Annex A of ISO/IEC 27001:2022 as a reference for controls, which covers organizational, personnel, physical, and technological categories [26]. The selection of controls was based on their relevance to the threat and vulnerability characteristics, which sometimes resulted in the duplication of control recommendations across different risk scenarios.

2.6. Communication, Consultation, Monitoring, and Review

The communication, consultation, monitoring, and review processes were conducted continuously throughout the research. Communication and consultation were performed iteratively with the company to validate each finding and ensure the results reflected the company's actual condition [24]. Meanwhile, monitoring and review involved the researcher showing the data processing progress to the company. This progress was then re-validated through the communication process. This step was crucial for maintaining methodological accuracy and the relevance of the results.

3. RESULTS

The information security risk assessment for the regional water company was conducted based on the methodology and risk criteria established in the previous section. The findings are presented sequentially

according to the ISO/IEC 27005:2022 framework, encompassing risk identification, analysis, evaluation, and treatment.

3.1. Risk Identification

This study identifies risk by combining interview findings and questionnaire results with the framework set out in ISO/IEC 27005:2022. These findings against the standard to confirm which risks apply to the organization's actual conditions. At this stage, determines the assets in use, the threats those assets face, and the vulnerabilities that could expose them to harm. Each identified asset, threat, and vulnerability then becomes the basis for assessing risk in the following stage.

3.1.1. Asset Identification

Asset identification was conducted through semi-structured interviews and validated using the structured spreadsheet instrument completed by the IT department. This systematic process resulted in the identification of 31 critical IT assets, which were subsequently grouped into hardware, software, information, network infrastructure, and personnel. Based on this categorization, it appears that hardware and infrastructure assets dominate the company's IT environment, accounting for a significant portion of the total assets. This dominance highlights the organization's high dependence on physical infrastructure to maintain regional water company operations. Table 5 delineates some of primary assets recognized during the assessment, alongside the individuals accountable for managing their specific risks.

Table 5. Asset identification

Asset ID	Asset	Risk Owner
A1	Customer Data	Hardware and Network Division
A2	Database Server	Hardware and Network Division
A3	Service Application	Data and Applications Division
A4	Router	Hardware and Network Division

3.1.2. Threat Identification

After identifying the assets, moved to the next stage: pinpointing threats capable of exploiting vulnerabilities within the regional water company's assets. Annex C of ISO/IEC 27005:2022 served as the initial reference point, offering a comprehensive catalog of threat categories against which the researcher could compare findings. The catalog against the interview and questionnaire results to retain only the threats relevant to the company's actual operational context. This filtering step ensured that the final threat list reflected conditions specific to the organization rather than a generic checklist drawn straight from the standard.

To ensure relevance to the company's specific environment, this list was validated using the structured spreadsheet instrument. The IT department reviewed the standard list and confirmed which threats were applicable to their actual operational conditions. This process resulted in 34 valid threats classified into several categories. These categories include physical and environmental threats such as fire and earthquakes, technical failures including hardware damage and loss of electrical power, compromise of functions or services, as well as human or organizational factors like violation of laws or regulations. Some of complete list of identified threats are detailed in Table 6.

Table 6. Threat identification

Threat ID	Threat
T1	Fire
T2	Earthquake
T3	Loss of Electrical Power
T4	Hardware Damage

3.1.3. Vulnerability Identification

The vulnerability identification stage was carried out to determine conditions or weaknesses that can be exploited by threats, in accordance with the definition of vulnerability in ISO/IEC 27005:2022. The identification process was performed using a semi-structured spreadsheet completed by the company's IT department based on the list of vulnerabilities recommended in ISO/IEC 27005:2022. This instrument allows the company to assess vulnerabilities that are relevant to its actual operational conditions and the characteristics of the assets they own.

The vulnerability identification aims to ensure that each threat detected in the previous stage can be associated with realistic and possible weak points within the company. The results of the identification show that there are 18 vulnerabilities grouped into four main categories, such as hardware vulnerabilities (e.g., vulnerability to moisture, dust, dirt), software vulnerabilities (e.g., inadequate or non-existent documentation), site-related vulnerabilities (e.g., locations in areas prone to natural disasters), and organizational vulnerabilities (e.g., audits that are not conducted regularly). Some of complete list of vulnerabilities is presented in Table 7, which is then used as the basis for constructing risk scenarios in the next stage.

Table 7. Vulnerability identification

Vulnerability ID	Vulnerability
V1	Vulnerability to moisture, dust, dirt
V2	Inadequate or non-existent documentation
V3	Locations in areas prone to natural disasters
V4	The formal process for reviewing access rights has not been developed, or its implementation is ineffective.
V5	Audits that are not conducted regularly

In accordance with the principles outlined in ISO/IEC 27005:2022, the combination of assets, threats, and vulnerabilities will form specific risk scenarios. Each scenario is formulated by associating the assets owned by the regional water company with the threats that may target them and the vulnerabilities that could enable those threats to occur. This approach ensures that the resulting risks are not hypothetical, but instead reflect realistic situations that may occur within the organization.

These risk scenarios form the basis for subsequent risk level assessment through the evaluation of consequences and likelihood in the risk analysis stage. The mapping provided in Table 8 offers a comprehensive overview of how different combinations of threats and vulnerabilities may affect the company's assets, thereby supporting a more structured classification of risks and the determination of appropriate treatment priorities.

Table 8. Risk scenario

Risk ID	Asset	Threat	Vulnerability	Risk
R1	Customer Data	Data Recovery Failure	Inadequate or non-existent documentation	Permanent data loss and operational disruption
R2	Database Server	Loss of Electrical Power	Inadequate configuration change control, vulnerability to voltage fluctuations, location in disaster-prone areas	Device damage and operational disruption
R3	Service Application	Input data from untrustworthy sources	Incorrect access rights allocation, inadequate documentation, and poor password management	Data theft and phishing

Risk ID	Asset	Threat	Vulnerability	Risk
R4	Router	Telecommunications device failure	Vulnerability to voltage variations and incomplete backup copies	Internet connection lost and data lost
R5	IT Team Member	Failure of service providers	Audits that are not conducted regularly and inadequate or insufficient service level agreements	Operations disrupted and reputation damaged
R6	Data Center Room	Loss of Electrical Power	Vulnerability to voltage variations and vulnerability to temperature variations	System down and operational delays

3.2. Risk Analysis

At this stage, each identified risk scenario is evaluated using the ISO/IEC 27005:2022 methodology. The assessments of consequence and likelihood are determined based on the criteria established during the context establishment phase and formally validated by the company. The consequence values are determined by evaluating the impact of each risk on the organization's operational, financial, reputational, and service aspects, which represent an applied interpretation of the consequence assessment principles described in ISO/IEC 27005:2022. Meanwhile, the likelihood assessment reflects the expected frequency of risk occurrence based on the company's actual conditions, including historical incident records and the effectiveness of existing controls. These two values are then combined and mapped using the risk matrix in Table 4 through the Risk Priority Number (RPN), which is used to categorize risks into low, medium, and high levels. This approach is in line with the concept of asset-based risk assessment and utilizes the matrix described in ISO/IEC 27005:2022, where risk levels are determined through the combination of consequence and likelihood.

It is important to note that the resulting risk levels fully reflect the organization's specific context. For example, the risk of customer data loss is categorized as a low-level risk. In general, data loss is considered to have significant consequences in digital environments [35]. However, ISO/IEC 27005:2022 states that a risk may still be classified as low if its likelihood of occurrence is low, even when the consequence is high [24]. In the context of the regional water company, the likelihood of data loss was assessed as low based on historical incidents and the controls already implemented, resulting in a low overall risk level. Some of complete distribution of risk levels are presented in Table 9.

Table 9. Risk level assessment

Risk ID	Asset	Risk	Level
R1	Customer Data	Permanent data loss and operational disruption	Low
R2	Database Server	Device damage and operational disruption	High
R3	Service Application	Data theft and phishing	Low
R4	Router	Internet connection lost and data lost	High
R5	IT Team Member	Operations disrupted and reputation damaged	High
R6	Data Center Room	System down and operational delays	High

3.4. Risk Evaluation

The evaluation results indicate that all 265 identified risk scenarios were classified unacceptable by the company based on the defined risk acceptance criteria. This includes scenarios categorized as low and medium, as the organization aims to proactively anticipate all potential risks. Consequently, for every risk that is identified, risk treatment or mitigation is necessary. The implementation of these mitigation strategies is crucial to minimize potential losses during service distribution and guarantee operational continuity [36].

3.5. Risk Treatment

In this study, risk modification was selected as the treatment strategy for all 265 risk scenarios based on the risk acceptance criteria established in accordance with ISO/IEC 27005:2022 and formally validated by the company. During the context establishment stage, the organization defined low- and medium-level risks as

acceptable only if treatment is applied, whereas high-level risks were categorized as unacceptable and therefore also require mitigation. Consequently, no risk scenario qualified for acceptance without action. To operationalize the proposed risk treatment framework, targeted security measures were systematically extracted from Annex A of the ISO/IEC 27001:2022 standard. As showed in Table 10, this mapping establishes a precise alignment, guaranteeing that the recommended controls directly mitigate the unique threats and vulnerabilities characterizing each risk scenario.

This decision was further reinforced during the consultation sessions, where the company emphasized its objective to reduce both the likelihood and impact of all risks. This approach was driven by prior security incidents and the absence of an established formal risk management framework. As a result, none of the scenarios met the criteria for risk acceptance, risk sharing, or risk avoidance. Under these circumstances, risk modification emerges as the most appropriate strategy and is fully aligned with the guidance of ISO/IEC 27005:2022, which underscores the need for mitigation of all identified risk scenarios. Meanwhile, the application of ISO/IEC 27001:2022 controls provide a structured and internationally recognized foundation for implementing the required mitigation measures.

Table 10. Recommended controls

Risk ID	Affected Assets	Treatment	Recommended Controls (ISO/IEC 27001:2022 Clauses)
R1	Customer Data	Risk Modification	5.30 (ICT readiness for business continuity) 5.35 (Independent review of information security) 5.37 (Documented operating procedures) 8.13 (Information backup)
R2	Database Server	Risk Modification	5.30 (ICT readiness for business continuity) 7.5 (Protecting against physical and environmental threats) 7.8 (Equipment siting and protection) 7.11 (Supporting utilities) 7.12 (Cabling security) 7.13 (Equipment maintenance)
R3	Service Application	Risk Modification	5.35 (Independent review of information security) 5.37 (Documented operating procedures) 6.3 (Information security awareness, education and training) 6.8 (Reporting information security events) 8.26 (Application security requirements) 8.27 (Secure system architecture and engineering principles) 8.28 (Secure coding) 8.29 (Security testing in development and acceptance)
R4	Router	Risk Modification	5.30 (ICT readiness for business continuity) 7.5 (Protecting against physical and environmental threats) 7.6 (Working in secure areas) 7.8 (Equipment siting and protection) 7.12 (Cabling security) 7.13 (Equipment maintenance)
R5	IT Team Member	Risk Modification	5.18 (Access rights) 5.35 (Independent review of information security) 6.4 (Disciplinary process) 6.5 (Responsibilities after termination or change of employment) 8.2 (Privileged access rights) 8.3 (Restriction of access to information)

Risk ID	Affected Assets	Treatment	Recommended Controls (ISO/IEC 27001:2022 Clauses)
R6	Data Center Room	Risk Modification	8.5 (Secure authentication) 8.7 (Protection against malware) 8.16 (Monitoring activities) 5.15 (Access control) 5.18 (Access rights) 5.35 (Independent review of information security) 6.4 (Disciplinary process) 6.5 (Responsibilities after termination or change of employment) 6.8 (Security event reporting) 7.2 (Physical entry) 7.3 (Securing offices, rooms and facilities) 7.4 (Physical security monitoring) 8.3 (Information access restriction)

3.6. Results of Consultation and Data Validation

The main outcome of the ongoing communication and consultation as well as monitoring and review process is the validation and adjustment of risk assessment data. This process ensures that all criteria used have been adjusted and approved by the company to reflect the actual situation, such as the consequence criteria shown in Table 2 and the likelihood criteria in Table 3. In addition, the final risk level values for each scenario, detailed in Table 9, have also been confirmed at each stage and the criteria by the company. Therefore, the research results presented here are ensured to be more accurate, objective, and in line with the organization's priorities.

4. DISCUSSION

Based on the IT security risk assessment at the regional water company, it was found that low-level risks were dominant, accounting for 70.59% of total identified risks, followed by medium-level 25.66% and high-level risks 3.77%, as shown in Figure 2. Although high-level risks constitute the smallest portion, they carry a critical impact and a high probability of occurrence. For example, scenarios R2 and R265 in the Database Server and Data Centre Room pose the risk of equipment damage due to power fluctuations. If this occurs, the impact will be a total operational disruption to customer services due to system downtime, requiring priority mitigation measures in the form of procuring UPS and backup generators in accordance with ISO 27001 controls. Meanwhile, risk scenario R5 highlights the importance of a company's commitment to providing training to IT staff, which will increase staff awareness of IT risks. This will reinforce the fact that risk assessment in a company is not just an add-on, but a prerequisite for sustainable IT risk management [37].

Meanwhile, the dominance of low-level risks indicates that the vulnerabilities exploited by threats have a relatively small likelihood or impact on most assets. However, considering the organization’s role as a public utility provider, reliance on a “do nothing” approach is insufficient. Recognizing that even minor risks can accumulate to disrupt business operations, the company adopts a comprehensive risk management strategy. Rather than simply accepting these risks, the company prioritizes the implementation of controls for high and medium risks, while establishing a monitoring mechanism for low risks to prevent escalation. This structured approach supports the development of a formal, continuous information security risk management framework in the future. In addition, continuously analyzing key factors that affect performance is vital to maintaining the effectiveness of the risk management system over time [38].

Risk identification also shows that most assets are dominated by hardware category assets, which is in line with the research focus on IT infrastructure in regional water companies. This naturally results in a pattern of repetition in the types of threats and vulnerabilities relevant to various hardware assets. As a result, there is an overlap in the mitigation strategies and control recommendations from ISO/IEC 27001:2022 proposed for these assets, as detailed in Table 11. Clause 7.11, which occurs 20 times, highlights the key efficiency whereby a single strategic investment in power infrastructure can simultaneously reduce risk across multiple assets.

The findings of this study are consistent with previous studies [25], [28] that demonstrate the effectiveness of ISO/IEC 27005 in risk assessment. However, this study makes a new contribution by applying the latest

2022 version of the standard in the context of water utilities and integrating it with controls from ISO/IEC 27001:2022. The research results, which consist of detailed risk identification and structured control recommendations, successfully achieved the objective of providing practical guidance for regional water companies. In addition, the use of Annex A of ISO/IEC 27001 as the basis for control recommendations proved to be very useful. This standard provides a clear, standardized, and easy-to-implement list of security controls, without the need for complex internal framework development. The synergy between these ISO standards is beneficial, as they provide complementary frameworks. This offers a clear mapping of risks evaluated through ISO/IEC 27005 to mitigation controls in ISO/IEC 27001.

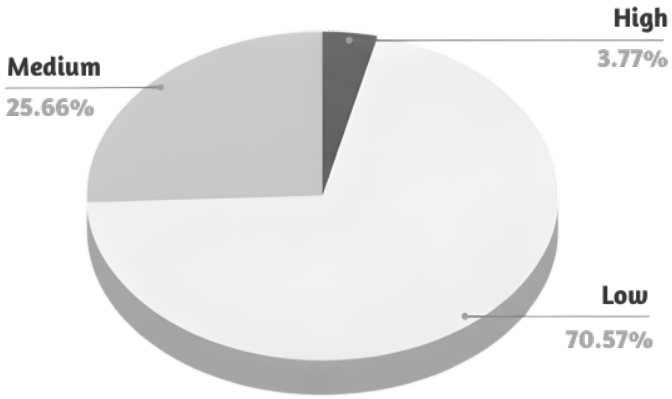

Figure 2. Risk level distribution

Table 11. Duplication of control recommendations

Clause	Frequency	Control
5.35	12 times	Independent review of information security
6.8	4 times	Information security event reporting
7.11	20 times	Supporting utilities
8.4	5 times	Access to source code

5. CONCLUSION

This study successfully used the ISO/IEC 27005:2022 standard to systematically assess information security risks at a regional water company. The results identified 265 risk scenarios with 10 high level risks, 68 medium level risks, and 187 low level risks based on the company's 31 IT assets. After evaluation, it was decided that all risks required treatment. This proves that ISO/IEC 27005:2022 is indeed effective as a structured guide in the context of risk assessment. In addition, combining this risk assessment process with the control recommendations from Annex A of ISO/IEC 27001:2022 has proven to provide a comprehensive and practical approach to handling risks. The combination of these two standards produces clear and actionable improvement recommendations, which are particularly suitable for companies that are just starting to establish formal information security risk management rules.

The main benefit of this research is that it provides an initial overview of risks and control recommendations for regional water companies, as well as serving as a reference for similar non-IT companies. However, it should be noted that this research was only conducted in one company. For further research, it is recommended that these findings be reviewed in more companies and that the residual risks that may still exist after controls are implemented be analyzed. For further steps in subsequent research, it may be considered to design risk management when risk controls have already been implemented in the company.

ACKNOWLEDGMENT

The authors would like to extend their gratitude to the regional water company based in Mataram City, West Lombok for their support and willingness to collaborate by providing access to sensitive asset data for research purposes. This contribution significantly enhanced the quality and execution of this study.

REFERENCES

[1] I. Appiah-Otoo and N. Song, "The impact of ICT on economic growth-comparing rich and poor countries," *Telecomm Policy*, vol. 45, no. 2, p. 102082, Mar. 2021, doi: 10.1016/j.telpol.2020.102082.

[2] 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.

[3] R. Prasetyo and A. Komariah, "CNC programming software design to optimizing batik stamping time," *OPSI*, vol. 14, no. 1, p. 21, Jun. 2021, doi: 10.31315/opsi.v14i1.4700.

[4] I. Keshta and A. Odeh, "Security and privacy of electronic health records: Concerns and challenges," *Egyptian Informatics Journal*, vol. 22, no. 2, pp. 177–183, 2021, doi: 10.1016/j.eij.2020.07.003.

[5] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, "Digital transformation and cybersecurity challenges for businesses resilience: issues and recommendations," *Sensors*, vol. 23, no. 15, pp. 1–20, 2023, doi: 10.3390/s23156666.

[6] H. Riggs *et al.*, "Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure," *Sensors*, vol. 23, no. 8, p. 4060, Apr. 2023, doi: 10.3390/s23084060.

[7] T. R. Reshmi, "Information security breaches due to ransomware attacks - A systematic literature review," *International Journal of Information Management Data Insights*, vol. 1, no. 2, p. 100013, Nov. 2021, doi: 10.1016/j.jjimei.2021.100013.

[8] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, pp. 48–52, Jul. 2018, doi: 10.1016/j.maturitas.2018.04.008.

[9] S. Saeed, S. A. Suayyid, M. S. Al-Ghamdi, H. Al-Muhaisen, and A. M. Almuhaideb, "A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience," *Sensors*, vol. 23, no. 16, p. 7273, Aug. 2023, doi: 10.3390/s23167273.

[10] J. A. Tanimu and W. Abada, "Addressing cybersecurity challenges in robotics: A comprehensive overview," *Cyber Security and Applications*, vol. 3, p. 100074, 2024, doi: 10.1016/j.csa.2024.100074.

[11] S. Zurawski, Z. Ciekanowski, Y. Pauliuchuk, and E. Ratter, "The impact of supply chain security management on the functioning of modern organizations," *European Research Studies Journal*, vol. XXVIII, no. Issue 1, pp. 44–56, Feb. 2025, doi: 10.35808/ersj/3889.

[12] E. A. Al-Qarni, "Cybersecurity in healthcare: A review of recent attacks and mitigation strategies," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 5, pp. 135–140, 2023, doi: 10.14569/IJACSA.2023.0140513.

[13] A. Bello, S. Jahan, F. Farid, and F. Ahamed, "A systemic review of the cybersecurity challenges in Australian water infrastructure management," *Water (Basel)*, vol. 15, no. 1, p. 168, Dec. 2022, doi: 10.3390/w15010168.

[14] A. Muzakir, A. T. Wahyudi, Y. D. Astanti, and C. D. Kusmindari, "Optimizing work movements to reduce injury risk: Application development with Methods-Time Measurement and WebQual analysis," *OPSI*, vol. 17, no. 2, p. 302, Dec. 2024, doi: 10.31315/opsi.v17i2.13478.

[15] N. S. Grigg, "Digital transformation in water utilities: Status, challenges, and prospects," *Smart Cities*, vol. 8, no. 3, p. 99, Jun. 2025, doi: 10.3390/smartcities8030099.

[16] A. Tereso, C. Santos, and J. Faria, "Risk management practices in the purchasing system of an automotive company," *Systems*, vol. 13, no. 6, p. 444, Jun. 2025, doi: 10.3390/systems13060444.

[17] J. V. Barraza de la Paz, L. A. Rodríguez-Picón, V. Morales-Rocha, and S. V. Torres-Argüelles, "A systematic review of risk management methodologies for complex organizations in industry 4.0 and 5.0," Systems, vol. 11, no. 5, p. 218, 2023, doi: 10.3390/systems11050218.

[18] H. Taherdoost, "Understanding cybersecurity frameworks and information security standards—A review and comprehensive overview," *Electronics (Switzerland)*, vol. 11, no. 14, p. 2181, 2022, doi: 10.3390/electronics11142181.

[19] R. Sheh, K. Geappen, and D. Harriss, "Autonomous cybersecurity and AI risk management for uncrewed systems: Challenges and opportunities using the NIST frameworks," in *XPONENTIAL 2024*, Arlington, Virginia, USA: Association for Unmanned Vehicle Systems International, 2024, pp. 46–67. doi: 10.52202/075106-0003.

[20] S. Ksibi, F. Jaidi, and A. Bouhoula, "A comprehensive quantified approach for security risk management in e-health systems," in *Proceedings of the 17th International Joint Conference on e-Business and Telecommunications*, SCITEPRESS - Science and Technology Publications, 2020, pp. 652–657. doi: 10.5220/0009893806520657.

[21] S. Memon, S. Memon, L. Das, and B. R. Memon, "Cyber security risk assessment methods for smart healthcare," in *2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC)*, IEEE, Jan. 2024, pp. 1–6. doi: 10.1109/KHI-HTC60760.2024.10481961.

[22] H. Boyes and M. D. Higgins, "An overview of information and cyber security standards," *Journal of ICT Standardization*, vol. 12, no. 1, pp. 95–134, Sep. 2024, doi: 10.13052/jicts2245-800X.1215.

[23] N. Alsafwani, Y. Fazea, and F. Alnajjar, "Strategic approaches in network communication and information security risk assessment," *Information*, vol. 15, no. 6, p. 353, Jun. 2024, doi: 10.3390/info15060353.

[24] ISO/IEC 27005 Fourth edition, "Information security, cybersecurity and privacy protection — Guidance on managing information security risks," 2022. [Online]. Available: www.iso.org

[25] A. P. Putra and B. Soewito, "Integrated methodology for information security risk management using ISO 27005:2018 and NIST SP 800-30 for insurance sector," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 4, pp. 1–9, 2023, doi: 10.14569/IJACSA.2023.0140468.

[26] ISO/IEC 27001 Third edition, "Information security, cybersecurity and privacy protection — Information security management systems — Requirements," 2022. [Online]. Available: www.iso.org

[27] B. Reuben-Owoh and E. Haig, "A systematic review of voluntary cybersecurity standards and frameworks," *Int J Inf Secur*, vol. 24, no. 5, p. 206, Oct. 2025, doi: 10.1007/s10207-025-01121-0.

[28] M. F. Kurniawan and T. D. Salma, "Risk management evaluation based on ISO/IEC 27005 framework: A case study of ABC company IT workshop room," *International Journal Software Engineering and Computer Science (IJSECS)*, vol. 5, no. 2, pp. 587–598, 2025, doi: 10.35870/ijsecs.v5i2.4549.

[29] M. Djunaidi and R. D. Gunari, "Analysis of factors affecting consumer satisfaction using SEM (structural equation modeling) method," *OPSI*, vol. 15, no. 1, p. 85, Jun. 2022, doi: 10.31315/opsi.v15i1.6808.

[30] T. Puspitasari and I. Ismianti, "Analysis of potential hazards and control in PT XYZ's production process with the HIRADC method," *OPSI*, vol. 16, no. 1, p. 11, Jun. 2023, doi: 10.31315/opsi.v16i1.9289.

[31] P. Y. Pratama, N. Azmi, and I. P. Sari, "Proposed Design of Assistant Tools to Reduce the Risk of Disorders (MSDS) Operator of Weaving Work Station CV XYZ," OPSI, vol. 15, no. 2, p. 216, 2022, doi: 10.31315/opsi.v15i2.7724.

[32] I. M. M. Putra and K. Mutijarsa, "Designing information security risk management on Bali regional police command center based on ISO 27005," in *2021 3rd East Indonesia Conference on Computer and Information Technology (EIConCIT)*, IEEE, Apr. 2021, pp. 14–19. doi: 10.1109/EIConCIT50028.2021.9431865.

[33] P. Benedek and F. Bognár, "Compliance risk assessment – Results of a comprehensive literature review," *Acta Polytechnica Hungarica*, vol. 21, no. 6, pp. 243–262, 2024, doi: 10.12700/APH.21.6.2024.6.13.

[34] A. Amiruddin, H. G. Afiansyah, and H. A. Nugroho, "Cyber-risk management planning using NIST CSF v1.1, NIST SP 800-53 rev. 5, and CIS controls v8," in *2021 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)*, IEEE, Oct. 2021, pp. 19–24. doi: 10.1109/ICIMCIS53775.2021.9699337.

[35] B. Ghimire and D. B. Rawat, "Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things," *IEEE Internet Things J*, vol. 9, no. 11, pp. 8229–8249, 2022.

[36] S. Sutrisno and P. Puryani, "Development of multi-criteria decision making model in packed beverage industry using global criterion method," *OPSI*, vol. 14, no. 2, p. 197, Dec. 2021, doi: 10.31315/opsi.v14i2.5365.

[37] P. H. Kasih, K. Rahmawati, I. Ismianti, Astrid Wahyu Adventri Wibowo, and Hasan Mastrisiswadi, "Vulnerabilities and risk mitigation in Indonesia's halal poultry chain: Bridging compliance and practice," *OPSI*, vol. 18, no. 1, pp. 34–45, Jun. 2025, doi: 10.31315/opsi.v18i1.14892.

[38] G. Samodro, "Pendekatan house of risk untuk penilaian risiko alur penyediaan dan pendistribusian obat (Studi kasus pada apotek ABC)," *OPSI*, vol. 13, no. 2, p. 92, Dec. 2020, doi: 10.31315/opsi.v13i2.3970.

DECLARATION OF AI-TOOL USAGE

The authors declare that generative AI tools were not used to create or write the core content of this manuscript. However, Claude AI was utilized solely for language editing and grammar/sentence correction.