Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Information Security Planning with Risk Management Using ISO 31000:2018 at E-Commerce XYZ

Euggelion Kevin Usmany [1], Nilo Legowo [2*]
[1] *Master of Information System Management, BINUS Graduate Program, Bina Nusantara University, Indonesia*
[2] *Professor, Master of Information System Management, BINUS Graduate Program, Bina Nusantara University, Indonesia*
* *Corresponding Author: euggelion.usmany@binus.ac.id*

ARTICLE INFO

Received: 30 Dec 2024

Revised: 12 Feb 2025

Accepted: 26 Feb 2025

ABSTRACT

In the digital era, businesses must manage both opportunities and risks effectively. E-commerce XYZ, an e- procurement provider, faces information security challenges due to the lack of a formal risk management framework. This study applies ISO/IEC 31000:2018 to design a strategy for identifying, evaluating, and mitigating risks. Data were collected through interviews and questionnaires with the Head of Services and Infrastructure Department. Key risks include irregular log reviews, multiple tabs in the CMS, and limited log history. Medium-level risks involve infrastructure disruptions (e.g., fires, earthquakes) and weaknesses in access management, such as poor password policies. Low-level risks include phishing, malware, and insufficient security training for non-technical staff. Recommendations focus on improving access control, log management, backups, and implementing regular security training. These measures aim to enhance e-commerce XYZ's risk management, ensuring operational resilience and building stakeholder trust.

Keywords: Risk Management, Information Security, E-commerce XYZ, Risk Mitigation, ISO 31000: 2018.

INTRODUCTION

In the ever-evolving digital era, technology has become integral to daily life and business operations, presenting both opportunities and complex risks. As technological advancements continue, system complexity and associated risks increase (Almuarif, 2023). Without effective risk management, businesses face vulnerabilities that can threaten operational sustainability (Suharyani & Djumarno, 2023). These types of vulnerabilities pose a threat to the security of an organization's information assets. For example, human errors or mistakes in data handling, such as careless work practices or lack of training, are vulnerabilities that can compromise the integrity of information. Many insider vulnerabilities, whether accidental or intentionally exploited, can also be considered as insider threats (Humphreys, 2008). E-commerce XYZ, a technology company providing comprehensive e-procurement solutions, operates two critical information systems: System A (an integrated e-commerce system with advanced features such as budget control, streamlined approval processes, and integrated payment systems) and System B (an internal configuration management system designed to manage and configure System A). Despite implementing routine security measures, such as data encryption, penetration testing, and regular backups, e-commerce XYZ has yet to formalize a risk management framework, creating vulnerabilities in their information security management.

Several security incidents have occurred, such as in April 2023, when multiple users of System A reported losing account access and funds in a single day. Although e-commerce XYZ responded quickly by enhancing account withdrawal security, the incident negatively impacted its reputation in the e-commerce sector. A similar incident reoccurred in May 2024, with a user losing account access, though no funds were compromised. Additionally, unauthorized access in System B was reported when a single superuser account was shared among multiple users, complicating accountability for system configuration changes. E-commerce XYZ is a technology company that offers comprehensive e-procurement solutions, relying on two primary information systems: System A, an integrated e-commerce platform with advanced features such as budget control, streamlined approval processes, and a secure payment system, and System B, an internal configuration management system responsible for overseeing and

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

managing System A. Although the company has implemented essential security measures, including encryption, penetration testing, and regular data backups, it has not yet established a formal risk management framework, leaving significant gaps in its security posture and increasing its vulnerability to potential threats.

Over the past few years, E-commerce XYZ has faced multiple security incidents. In April 2023, several users of System A reported losing access to their accounts, with some experiencing financial losses. While the company acted quickly by tightening security around account withdrawals, the event negatively impacted its reputation in the e-commerce sector. A similar incident occurred in May 2024, where a user again lost account access, though no funds were compromised. Additionally, System B was found to have unauthorized access incidents due to a single superuser account being shared among multiple employees, making it difficult to track accountability in system configuration management (Vorst et al., 2018).

To mitigate these risks, E-commerce XYZ introduced a temporary access request system, allowing users to request elevated permissions as needed, which are revoked once the task is completed. However, vulnerabilities persist, such as the lack of role-specific user accounts, a limited log history that only tracks account creation rather than modifications, and the absence of regular log reviews. Additionally, inadequate documentation of security incidents has made it more difficult for the company to assess past breaches and implement stronger preventive measures (White, 2011).

Since risks are part of unavoidable business operations, implementing structured risk management is very important to prevent unpredictable disruptions that can interfere company's goals. Without a systematic process to identify, evaluate, and mitigate risks, E-commerce XYZ might struggle to ensure the company's stability. This research examines the application of ISO 31000:2018, an internationally recognized risk management framework, to assist the company in assessing potential threats, improving its security protocols, and strengthening overall resilience. Also, Effective risk management could minimize the financial potential and operations loss, builds stakeholder trust, and ensures business continuity (Idayani et al., 2024).

The application of ISO 31000:2018 provides high defense against cyber threats, using its well-structured methodology such as early threat detection and ongoing risk evaluation, company can reduce many cyber risks they may encounter and give them better solution to mitigate unexpected risk (Brayn et al., 2024). In this case, e-commerce XYZ is expected to improve its risk maturity, optimize the business process, and improving their adaptability to changing industry demands by integrating ISO 3100:2018 into their risk management framework.

LITERATURE REVIEW

Upon facing modern technology that changed rapidly, the biggest challenge for organizations are protecting their information systems. Information security is vital in technology management, as it involves safeguarding data and system infrastructure from threats such as unauthorized access, data breaches, and operational disruptions. Managing these risks effectively is essential, and ISO 31000:2018 offers a structured framework to navigate uncertainties while improving decision-making and organizational resilience (Vorst et al., 2018). This standard uses risk management as a systematic approach to identifying, assessing, and mitigating risks while conserving organizational value. It emphasizes the need for an integrated, adaptable, and timely risk management process. Organizations are encouraged to costumize their risk management strategies to their specific operational and governance needs, align with their business objectives (British Standard, 2018). Due to its flexibility, ISO 31000 is widely applicable, particularly to cope with the multifaceted nature of information security risks, which may arise from both internal vulnerabilities and external cyber threats.

There are many advantages offered by ISO 31000:2018. In the context of information security, ISO 31000 provides a structured methodology for assessing information system risks, including several possible system vulnerabilities such as unauthorized system access, data breaches, and service outages, considering internal factors (e.g., system weaknesses) and external factors (e.g., cyber attacks). Other advantages offered by using this system are data confidentiality, high integrity, and good system availability (Tamsir et al., 2022). After the system analyzes each threat, it then evaluates the likelihood and potential impact of these threats. Then, the company can use the risk evaluation to determine appropriate countermeasures, using various existing benchmarks. Handling this risk

involves choosing the right strategy—such as avoidance, mitigation, transfer, or acceptance—to minimize potential disruptions (Vorst et al., 2018).

Numerous studies highlight the application of ISO 31000:2018 in improving information security. For example, Wiradarma and Sasmita (2019) utilized this framework alongside the OWASP guidelines to evaluate IT system vulnerabilities and identifying previously overlooked security risks. Similarly, Lubis et al. (2023) applied ISO 31000 to analyze security risks within a university registration system. From this study, Lubis identify critical issues in the system like unauthorized access and potential data loss. The two studies show the importance of a structured risk management approach in securing critical information systems and ensuring operational resilience. Argadinata et al. (Argadinata et al., 2023) also explored ISO 31000's implementation in higher education institutions, showcasing its adaptability across various organizational settings through methods such as direct observation and stakeholder interviews.

To support its implementation, Putri and Wijaya (2022) implemented ISO 31000 in XYZ e-commerce and categorized risks into three levels: low, medium, and high. High risks include full storage and server downtime. This problem was then overcome by increasing system stability by backing up data regularly and making periodic system repairs and updates. Nugraha and Istambul (2019) examined the adoption of ISO 31000 in government IT infrastructure, emphasizing its critical role in maintaining seamless operations by addressing technology-related risks comprehensively. Additionally, several complementary risk management frameworks can also be integrated with ISO 31000:2018 to support its performance. One that can be paired well is COSO ERM which focuses on internal control and governance structures (Grob & Cheng, 2021). This framework provides a synergistic overview that allows organizations to develop a more comprehensive and structured risk management strategy. In this regard, COSO ERM's structured approach to risk identification, response, and monitoring is closely aligned with the principles of ISO 31000, which ensures a comprehensive security strategy that includes technical protections and leadership involvement (Brown & Osborne, 2013).

The main advantage of ISO 31000 is that this system can be applied to management at every level of decision-making within the company. This can certainly help build a proactive risk awareness culture so that companies can anticipate security threats and align their information security practices with their long-term goals (Skačkauskienė, 2022). This includes implementing preventive security measures, such as increasing control access, and having well-prepared incident response plans and documentation of every incident that happens to assist the company against potential cyber threats in the future. Furthermore, ISO 31000:2018 promotes evaluation and monitoring continuity to ensure the risk management strategies are still effective and can adapt to the growing security challenges in this digital era (Kusuma, 2024).

In conclusion, ISO 31000:2018 provides organizations with a comprehensive and adaptable framework for managing information security risks. This system helps managing system risk effectively by offering clear principles, a structured framework, and effective processes, this standard helps businesses overcome security uncertainties while strengthening their resilience and operational stability. Applying ISO 31000:2018 might help the organization protect its information assets and build trust among the stakeholders, also reaching the company objective more effectively.

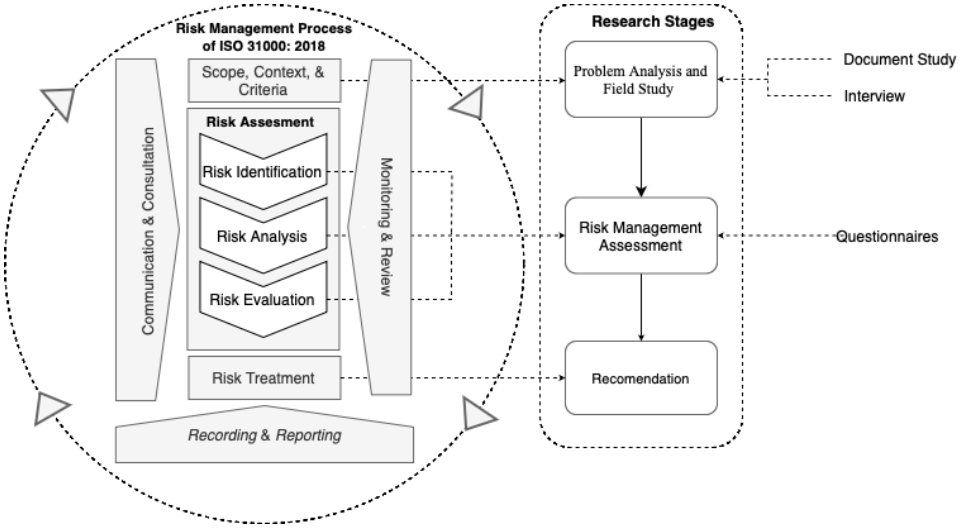
METHODS

This study uses ISO 31000:2018 as the core object of research to analyze risk management of information security in E-commerce XYZ. The methodology used in this study is using ISO 31000 on XYZ e-commerce to analyze existing problems, assess risks that arise, and propose mitigation strategies to develop practical recommendations for XYZ E-commerce. The entire process is represented visually in Figure 1 and elaborated in this section.

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Figure 1. Research Model



First of all, this study will focus on discussing the problem analysis and field research to identify potential information risks in XYZ E-commerce. The data collection method used for this study was conducted through in-depth interviews, distributing quisionaires, and document analysis to gain further understanding of the internal and external challenges faced by the company. Interviews and quisionaires were conducted with personels who are experienced in their fields within e-commerce XYZ, while relevant documents were used to gain a detailed picture of the organization's current risk management practices. This stage lays the groundwork for identifying critical risks associated with information security.

Risk identification aims to recognize and describe potential threats to information security. This study identified risks by analyzing IT and information system assets through a combination of interviews and questionnaires. The interviews targeted key personnel within e-commerce XYZ to gain deeper understanding of the organization, while the questionnaires involved the Head of the ICT Services and Infrastructure Department. The data collected focused on uncovering vulnerabilities and threats that could impact the confidentiality, integrity, and availability of the company's information systems.

The risk analysis stage evaluates the possibility and impact of identified risks. Possibility is assessed based on the frequency of occurrence, as detailed in Table 1, which categorizes it into five levels: Rare, Unlikely, Possible, Likely, and Certain. Impact is assessed by examining the severity of potential consequences, ranging from Insignificant to Catastrophic, as shown in Table 2 Both possibility and impact are scored, and the results are used to classify risks based on their severity.

Table 1. Possibility Assessment

Possibility		Description	Frequency per Year
Rating	Criteria		
1	Rarely	The risk almost never occurs	> 2 years
2	Unlikely	The risk rarely occurs	1 - 2 years
3	Possible	The risk occasionally occurs	7 – 12 months
4	Likely	The risk is likely to occur (frequently)	4 - 6 months
5	Certain	The risk almost always occurs	1 - 3 months

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 2. Impact Assessment

Impact Rating	Impact Criteria	Description
1	Insignificant	The risk does not disrupt activities or business processes within the institution.
2	Minor	Activities within the institution are slightly hindered but do not affect core activities.
3	Moderate	The risk disrupts the business processes within the institution, partially hindering activities.
4	Major	The risk hampers almost all business processes within the institution.
5	Catastrophic	The risk disrupts all business processes entirely, halting all internal activities.

The risk evaluation process determines the overall risk level by combining the possibility and impact assessments. The evaluation is conducted using the Risk Evaluation Matrix which classifies risks into three levels: low, medium, and high as described in Table 3.

Table 3. Risk Evaluate Matrix

Certain (5)	Medium	Medium	High	High	High
Likely (4)	Medium	Medium	Medium	High	High
Possible (3)	Low	Medium	Medium	Medium	High
Unlikely (2)	Low	Low	Medium	Medium	Medium
Rarely (1)	Low	Low	Low	Medium	Medium
Possibility / Impact	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)

Table 4. Risk Level Description

Risk Level	Description
High	High possibility and significant impact; current controls are ineffective.
Medium	Medium possibility and impact; existing controls partially effective.
Low	Low possibility and impact; current controls effectively mitigate threats.

If a threat is said to be "High-risk", management must take immediate action to address this threat. Additional security protection also needs to be applied because current controls are likely no longer effective. "Medium" risks indicate that current controls are effective but still needs continuous monitoring to prevent escalation. "Low" risks, on the other hand, are generally manageable with the existing controls that running.

After identifying the risks, the next step is to address them. Here, the system will recommend effective steps to address the problem at hand. This process includes assessing the effectiveness of current security measures and introducing additional safeguards when necessary. Aligned with the principles of ISO 31000, this stage focuses on mitigating potential threats and strengthening the company's overall security management. Each risks are categorized and analyzed to determine appropriate control measures, ensuring that identified vulnerabilities are effectively addressed. The recommendations provided aim to fill existing security gaps and establish actionable strategies to enhance resilience against potential threats.

By systematically applying these steps, this study ensures that E-commerce XYZ adopts a structured approach to have the best risk management. Finally, its allow the company to manage its information about security risks more effectively while still implementing best practices for the industry, ultimately reinforcing its overall security framework.

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

RESULTS

Identification of information technology assets in XYZ e-commerce includes various categories that are important to support company operations. These assets are classified into physical assets, information assets, digital assets, and human resource assets. Each category contains specific assets directly connected to the company's core activities, ranging from network infrastructure and data storage to digital applications and skilled personnel. Table 5 below provides a detailed overview of the assets by category.

Table 5. Asset Identification

No	Asset Category	Asset	Asset Description
1	Physical Assets	Server and Network Infrastructure	Physical servers, networking devices, firewalls, routers, and other hardware used for system operations.
		Data Center	Physical facility where the company's servers and hardware are stored and operated.
2	Information Assets	User Data	Sensitive information including customer details, financial data, contracts, and transaction history.
		Vendor Data	Information related to vendors, including contract details, vendor performance, and communication data.
		Transaction Data	Records of all transactions made through the platform, including procurement of goods and services.
3	Digital Assets	Mobile Application (Android)	Mobile application used by users to access the e-procurement platform.
		Web Platform System A	Web platform for Information System A used for e-commerce and procurement activities.
		Web Platform System B	Web platform for Information System B used for internal configuration management (CMS) of System A.
		Database	Database that stores all information related to customers, vendors, and transactions.
4	Human Resource Assets	IT Employees	Company personnel responsible for managing and overseeing operations.
		Vendors	Third-party providers of essential services such as hosting, data management, or information security.

The above assets are critical to running a company's operations and services. Physical assets, such as servers and network infrastructure, serve as the foundation of technology. Information assets—including sensitive customer and vendor data—require strong security measures because they can be misused by anyone to commit crimes, while digital assets, such as e-commerce applications and web platforms, play a vital role to hold transactions issues and internal management. In addition, human resources and external vendors play a big role to the overall management, security, maintenance, as well as the user of these assets. A clear understanding of these asset categories provides a strong foundation for the subsequent risk identification process.

After identifying the main assets in E-commerce XYZ, the next step is to conduct a thorough risk identification process to see the potential risks that may arise. In this process, the company needs to identify the threats and vulnerabilities that can affect each asset so that the company can gain a comprehensive understanding of the risk exposure it poses. This process includes an assessment of internal and external threats, along with an evaluation of the vulnerabilities of each asset owned by E-commerce XYZ.

In this section, risk analysis is conducted by considering two main factors, namely threats and vulnerabilities. In this XYZ E-commerce study, risk assessment is focused on identifying potential threats that can affect the company's assets, while evaluating the weaknesses in its systems. Detailed details about these threats and vulnerabilities are provided in the following sections.

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Through the risk identification process, ten primary threats were identified and classified into four main categories: Cyber Attacks, Internal Fraud, Network Disruptions, and Natural Disasters. These threats pose significant risks to the company's critical assets, and their details are outlined in Table 6.

Table 6. Threat Identification

No	Threat Category	Threat	Threat Description
1	Cyber Attack	Phishing	Potential for e-commerce XYZ employees to become victims of phishing attacks, leading to credential leaks or other critical information breaches.
		Data Breach	Risk of sensitive customer or company data leakage due to weaknesses in data encryption or protection during transfer or storage.
		Hacking	Unauthorized access to systems or data by external parties.
		Malware	Malicious software that can steal data, damage systems, or take control of systems without user consent.
		Social Engineering	Psychological manipulation by external parties to obtain information or system access through employees or related parties.
2	Internal Fraud	Internal Fraud	Employees exploiting their access rights to commit fraud or data theft.
3	Network Disruption	Network Disruption	Disruptions at service providers that can affect e-commerce XYZ's service connectivity.
4	Natural Disaster	Fire	Natural disasters such as fire that can damage IT infrastructure and lead to company data loss.
		Earthquake	Natural disasters such as earthquakes that can damage IT infrastructure and lead to company data loss.
		Flood	Natural disasters such as floods that can damage IT infrastructure and lead to company data loss.

The data above shows that the threats received by XYZ e-commerce do not only come from internal sources, but also external sources. External threats include cyberattacks and natural disasters, while internal threats stem from fraudulent activities by employees. These threats could lead to significant impacts, ranging from data breaches to physical damage to IT infrastructure, ultimately disrupting operational continuity.

The vulnerability identification process at e-commerce XYZ highlights 14 vulnerabilities grouped into six main categories: Access and Authentication, System Configuration Management, Logging and Monitoring, Employee Awareness and Training, Vendor Risks, and Incident Documentation and Processes. These vulnerabilities could be exploited by threats to harm or disrupt the company's assets. Detailed descriptions of these vulnerabilities are provided in Table 7.

Table 7. Vulnerability Identification

No	Vulnerability Category	Vulnerability	Vulnerability Description
1	Access and Authentication	Unauthorized Access	Access to systems or data by unauthorized individuals, both internal and external.
		Dependence on Super User Account	Reliance on a single super user account to perform many critical tasks, without proper task segregation or access control.
		Insufficient Password Management	Password management system that does not enforce the use of unique symbols and allows users to reuse old passwords when changing to a new one.

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

		Weakness in Multi-Factor Authentication (MFA) Weak Session Management	Insufficient Multi-Factor Authentication (MFA) increases the risk of unauthorized access if user credentials are compromised. The system does not properly manage sessions, allowing users to stay logged in indefinitely, increasing the risk of unauthorized access if the user's device is not secured.
2	Configuration and System Management	Lack of Version Control	Risks associated with the lack of an effective version control system in Information System B, causing difficulty in tracking changes and rolling back versions.
		Limited Backup and Recovery	Insufficient backup and recovery processes, including the lack of routine testing, can lead to data loss that may be unrecoverable in the event of a disaster.
		Multiple Tabs in CMS	CMS system allows users to open multiple tabs without validation, which may result in two users sharing accounts and using the system simultaneously without detection.
3	Logging and Monitoring	Limited Log History on CMS	Log history is limited to create logs only. There is no change log, making it difficult to track changes.
		No Regular Log Review or Monitoring	No process in place for the routine review or monitoring of logs in the System.
4	Employee Awareness and Training	Limited Security Training for Non-Technical Users	Non-technical employees may lack an understanding of the importance of information security practices, leading to human errors such as phishing or accidental data disclosure.
5	Vendor Risks	Vendor Risk	Dependence on external vendors who may lack proper security controls, potentially leading to data breaches or service disruptions.
6	Documentation and Incident Process	Lack of Incident Documentation	e-commerce does not record errors that have occurred, make it difficult to evaluate the same errors in the future.

The vulnerabilities outlined in Table 7 are divided into several key categories, including weaknesses in authentication mechanisms, deficiencies in configuration management, and lack of monitoring, employee training, and comprehensive incident documentation. In the table above, specific examples of each of the existing vulnerabilities are given, including reliance on a single superuser account, limited log history, and inadequate security training for non-technical employees. With the various threats and vulnerabilities present, this study has identified several factors that can pose potential risks that may affect the way the system works. These factors have been systematically categorized and organized into a structured risk table to provide a better perspective on the issue.

Table 8. Potential Risks

Code	Risk Category	Risk Type
R1	Cyber Attack	Phishing
R2		Data Breach
R3		Hacking
R4		Malware
R5		Social Engineering
R6	Fraud Internal	Fraud Internal
R7	Network Disruption	Network Disruption
R8	Natural Disaster	Fire
R9		Earthquake

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

R10		Flood
R11	Access and Authentication	Unauthorized Access
R12		Dependence on Super User Account
R13		Insufficient Password Management
R14		Weakness in Multi-Factor Authentication (MFA)
R15		Weak Session Management
R16	Configuration and System Management	Lack of Version Control
R17		Limited Backup and Recovery
R18		Multiple Tabs in CMS
R19	Logging and Monitoring	Limited Log History on System.
R20		No Regular Log Review or Monitoring
R21	Employee Awareness and Training	Limited Security Training for Non-Technical Users
R22	Vendor Risks	Vendor Risk
R23	Documentation and Incident Process	Lack of Incident Documentation

The risks presented in Table 8 comprise a wide range of threats, including cybersecurity issues such as phishing and hacking, as well as operational risks like internal fraud and reliance on superuser accounts. Additionally, risks associated with natural disasters, network disruptions, and weaknesses in access control and authentication management are also evident. Effectively addressing these risks requires a strong focus on system security, employee training, and the implementation of strong policies for recovery and incident documentation.

After knowing the potential risks that may attack the XYZ e-commerce information system, a detailed analysis can then be carried out to assess the severity, likelihood, and overall impact. This analysis plays an important role in solving the problem by determining the right mitigation strategy to manage each risk more effectively.

The company can analyze risk by evaluating the occurrence probability and the potential consequences of each identified risk. The data used in this assessment was obtained from the Head of the ICT Services and Infrastructure Department through a questionnaire. In this case, the Head of the ICT Services and Infrastructure Department provided valuable insights into the operational challenges and security threats facing his company. The findings from this evaluation are summarized in Table 9, which offers a comprehensive overview of the risks that could affect the organization.

Table 9. Risk Analysis

Code	Risk Category	Risk Type	Risk Description	Possibility	Impact
R1	Cyber Attack	Phishing	Potential for e-commerce XYZ employees to become victims of phishing attacks, leading to credential leaks or other critical information breaches.	1	1
R2		Data Breach	Risk of sensitive customer or company data leakage due to weaknesses in data encryption or protection during transfer or storage.	1	1
R3		Hacking	Unauthorized access to systems or data by external parties.	1	1
R4		Malware	Malicious software that can steal data, damage systems, or take control of systems without user consent.	1	1

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

R5		Social Engineering	Psychological manipulation by external parties to obtain information or system access through employees or related parties.	1	1
R6	Fraud Internal	Fraud Internal	Employees exploiting their access rights to commit fraud or data theft.	1	1
R7	Network Disruption	Network Disruption	Disruptions at service providers that can affect e-commerce XYZ's service connectivity.	1	5
R8	Natural Disaster	Fire	Natural disasters such as fire that can damage IT infrastructure and lead to company data loss.	1	5
R9		Earthquake	Natural disasters such as earthquakes that can damage IT infrastructure and lead to company data loss.	1	5
R10		Flood	Natural disasters such as floods that can damage IT infrastructure and lead to company data loss.	1	5
R11	Access and Authentication	Unauthorized Access	Access to systems or data by unauthorized individuals, both internal and external.	1	1
R12		Dependence on Super User Account	Reliance on a single super user account to perform many critical tasks, without proper task segregation or access control.	1	3
R13		Insufficient Password Management	Password management system that does not enforce the use of unique symbols and allows users to reuse old passwords when changing to a new one.	1	4
R14		Weakness in Multi-Factor Authentication (MFA)	Insufficient Multi-Factor Authentication (MFA) increases the risk of unauthorized access if user credentials are compromised.	1	5
R15		Weak Session Management	The system does not properly manage sessions, allowing users to stay logged in indefinitely, increasing the risk of unauthorized access if the user's device is not secured.	2	5
R16	Configuration and System Management	Lack of Version Control	Risks associated with the lack of an effective version control system in Information System , causing difficulty in tracking changes and rolling back versions.	2	5
R17		Limited Backup and Recovery	Insufficient backup and recovery processes, including the lack of routine testing, can lead to data loss that may be unrecoverable in the event of a disaster.	1	1

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

R18		Multiple Tabs in CMS	CMS system allows users to open multiple tabs without validation, which may result in two users sharing accounts and using the system simultaneously without detection.	3	5
R19	Logging and Monitoring	Limited Log History on CMS	Log history is limited to create logs only. There is no change log, making it difficult to track changes.	3	5
R20		No Regular Log Review or Monitoring	No process in place for the routine review or monitoring of logs in CMS.	4	5
R21	Employee Awareness and Training	Limited Security Training for Non-Technical Users	Non-technical employees may lack an understanding of the importance of information security practices, leading to human errors such as phishing or accidental data disclosure.	1	1
R22	Vendor Risks	Vendor Risk	Dependence on external vendors who may lack proper security controls, potentially leading to data breaches or service disruptions.	1	1
R23	Documentation and Incident Process	Lack of Incident Documentation	After an incident, e-commerce XYZ does not properly document the event, making it difficult to evaluate future incidents.	2	5

The analysis reveals several high-impact risks requiring immediate attention, such as network disruptions, natural disasters, weak session management, and inadequate access controls. Risks such as reliance on super user accounts, weak password policies, and limited logging and monitoring also demand mitigation measures to reduce their potential impact.

The next step is the evaluation of the existing risks. Company can use pre-determined risk evaluation matrix to assess the possibility and impact of each risk. That way, they can determine the most effective priorities and mitigation actions. This evaluation serves as a decision-making tool to prioritize mitigation strategies.

Based on the results of the risk analysis, each identified risk is assessed using a risk evaluation matrix, considering both its possibility of occurance and the potential impact that may occur. This evaluation categorizes risks into three levels: high, medium, and low. High-level risks, marked in red, indicate a significant possibility and severe impact, requiring immediate intervention because existing controls are considered no longer effective. Medium risks, indicated in yellow, have a moderate probability and impact, indicating that the steps taken currently could be a solution to the problem, but still require increased efficiency. Low-level risks, indicated in green, cause minimal threats because existing controls are sufficient to manage them effectively. The structured classification in the risk evaluation matrix and Table 10 provides a clear overview of the risks, helping prioritize mitigation efforts and ensuring a more effective risk management approach.

Table 10. Risk Evaluate Matrix

Certain (5)					
Likely (4)					R20
Possible (3)					R18, R19

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Unlikely (2)					R15, R16, R23
Rarely (1)	R1, R2, R3, R4, R5, R6, R11, R17, R21, R22		R12	R13	R7, R8, R9, R10, R14
Possibility / Impact	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)

Table 11. Risk Evaluation

Code	Risk Type	Possibility	Impact	Risk Level
R20	No Regular Log Review or Monitoring	4	5	High
R18	Multiple Tabs in CMS	3	5	High
R19	Limited Log History on CMS	3	5	High
R15	Weak Session Management	2	5	Medium
R16	Lack of Version Control	2	5	Medium
R23	Lack of Incident Documentation	2	5	Medium
R7	Network Disruption	1	5	Medium
R8	Fire	1	5	Medium
R9	Earthquake	1	5	Medium
R10	Flood	1	5	Medium
R14	Weakness in Multi-Factor Authentication (MFA)	1	5	Medium
R13	Insufficient Password Management	1	4	Medium
R12	Dependence on Super User Account	1	3	Low
R1	Phising	1	1	Low
R2	Data Breach	1	1	Low
R3	Hacking	1	1	Low
R4	Malware	1	1	Low
R5	Social Engineering	1	1	Low
R6	Fraud Internal	1	1	Low
R11	Unauthorized Access	1	1	Low
R17	Limited Backup and Recovery	1	1	Low
R21	Limited Security Training for Non-Technical Users	1	1	Low
R22	Vendor Risk	1	1	Low

High-level Risk including limited log review (R20), use of multiple tabs in the CMS (R18), and limited log history (R19), must be eliminated immediately by improving the efficiency of existing controls due to their significant impact on system continuity. Medium-level Risks: Risks such as network outages (R7), natural disasters (R8, R9, R10), and weaknesses in session management (R15) and password policies (R13) require improvements to existing controls to minimize the impact. Low-Level Risks: Risks like cyberattacks (R1, R2, R3, R4, R5), internal fraud (R6), and inadequate training (R21) are currently well-controlled but still require regular monitoring to prevent escalation. Mitigation strategies will prioritize addressing high-level risks, followed by preventive measures for medium-level risks. Existing controls for low-level risks will be maintained with periodic reviews to ensure sustained effectiveness. This approach ensures a focused and optimal risk management strategy for e-commerce.

After identifying, analyzing, and evaluating the risks, the next step is to design appropriate risk treatment strategies to reduce the possibility or impact of the identified risks. Risk treatment strategies include avoidance, reduction, transfer, or acceptance, tailored to the severity and priority of each risk. The ultimate goal is to ensure e-commerce XYZ has adequate controls to maintain operational stability and protect its critical assets.

Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 12. Risk Treatment

Code	Risk Type	Risk Level	Risk Treatment
R20	No Regular Log Review or Monitoring	High	Conduct periodic audits of log history to ensure unauthorized changes are detected.
R18	Multiple Tabs in CMS	High	Limit account sessions to only one browser tab.
R19	Limited Log History on CMS	High	Develop a log history feature covering create, change, and user logs to document every change in the system.
R15	Weak Session Management	Medium	Limit user sessions to a set period and restrict logins to a single session at a time.
R16	Lack of Version Control	Medium	Regularly back up data before and after changes and implement a change-tracking system.
R23	Lack of Incident Documentation	Medium	Document all incidents for reporting purposes.
R7	Network Disruption	Medium	Provide an alternative provider and regularly back up data.
R8	Fire	Medium	Provide backup infrastructure, spare servers, and fire extinguishing equipment like hydrants.
R9	Earthquake	Medium	Prepare backup infrastructure and servers to ensure business continuity.
R10	Flood	Medium	Provide backup infrastructure and servers, and place IT equipment in elevated areas safe from floods.
R14	Weakness in Multi-Factor Authentication (MFA)	Medium	Develop and enforce two-step authentication for user logins.
R13	Insufficient Password Management	Medium	Inform users to change passwords every 3 months and require combinations of numbers, letters, and symbols.
R12	Dependence on Super User Account	Low	Implement role-based access for accounts and revoke roles when access is no longer needed.
R1	Phising	Low	Avoid accessing suspicious websites.
R2	Data Breach	Low	Enhance data security, strengthen firewalls, and conduct penetration testing to identify vulnerabilities.
R3	Hacking	Low	Change passwords regularly, avoid accessing suspicious files or sites, and enhance firewall security.
R4	Malware	Low	Continuously improve firewall security, install and update antivirus software, and train staff on safe downloading practices.
R5	Social Engineering	Low	Conduct regular training on information security.
R6	Fraud Internal	Low	Deactivate accounts or revoke user roles if access is no longer needed and monitor user access regularly.
R11	Unauthorized Access	Low	Implement MFA and regularly train employees on information security.
R17	Limited Backup and Recovery	Low	Perform regular backups at least monthly and use the 3-2-1 backup strategy.
R21	Limited Security Training for Non-Technical Users	Low	Provide training sessions on information security.
R22	Vendor Risk	Low	Periodically evaluate vendor performance and prepare alternative vendors to mitigate potential disruptions.

XYZ e-commerce can implement ISO 31000:2018 to improve its ability to anticipate and mitigate internal and external threats, ultimately ensuring better operational stability and security of its critical assets. High-level risks,

such as limited log review (R20), the ability to open multiple tabs in the CMS (R18), and limited log history (R19), require stricter access controls and enhanced monitoring mechanisms to strengthen security measures. Medium-level risks, including network outages (R7), natural disasters (R8, R9, R10), and weak session management (R15), can be addressed by creating backup infrastructure and enhancing physical and digital security. Low-level risks, such as unauthorized access (R11) and vendor-related vulnerabilities (R22), are managed through regular reviews, enhanced training, and maintenance of existing controls as both troubleshooting solutions and prevention of recurring issues.

CONCLUSION

Implementing the best risk management framework is important to control threats, ISO 31000:2018 can show the level of risk so that companies can handle it more effectively, it provides practical recommendations to enhance information security at E-commerce XYZ. High-level risks like multiple tab access in the CMS, require immediate action due to their potential impact on system security, such as uncontrolled user activity, limited log history that restricts auditing and tracking, and the absence of regular log reviews. Medium-level risks primarily affect infrastructure, disaster preparedness, and access control, with threats like network disruptions, fires, earthquakes, and floods posing risks to IT operations and system stability. Weak access controls, including poor password policies, ineffective Multi-Factor Authentication (MFA), and session vulnerabilities, further expose the system to unauthorized access, while the lack of version control and incident documentation complicates recovery and evaluation processes. Low-level risks, including common cyber threats such as phishing, malware, hacking, and social engineering, can be managed through strong internal controls and continuous monitoring. Additionally, awareness gaps among non-technical employees, risks of internal fraud, and vendor dependencies require regular training programs and periodic assessments. The study emphasizes the importance of addressing high-risk threats first, followed by preventive strategies for medium-level risks and ongoing reviews for low-level risks, ensuring a structured approach that strengthens E-commerce XYZ's resilience against security challenges.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] Almuarif, A. (2023). Peran Perencanaan Strategis dalam Organisasi. Al-Marsus : Jurnal Manajemen Pendidikan Islam, 1(2), 164. https://doi.org/10.30983/al-marsus.v1i2.6455

[2] Argadinata, H., Wiyono, B. B., Imron, A., Mustiningsih, & Pramudya, Moch. F. (2023). Identifying Risks Based on ISO 31000:2018 Using Risk Factors at Public Universities of Legal Entities (pp. 43–60). https://doi.org/10.2991/978-2-38476-156-2_7

[3] British Standard. (2018). BSI Standards Publication Risk management — Guidelines (Second Edition). BSI Standard Publication.

[4] Brown, L., & Osborne, S. P. (2013). Risk and Innovation. Public Management Review, 15(2), 186–208. https://doi.org/10.1080/14719037.2012.707681

[5] Grob, M., & Cheng, V. (2021). Committee of Sponsoring Organizations of the Treadway Commission By Enterprise Risk Management ENTERPRISE RISK MANAGEMENT FOR CLOUD COMPUTING.

[6] Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. Information Security Technical Report, 13(4), 247–255. https://doi.org/10.1016/j.istr.2008.10.010

[7] Idayani, R. W., Nadlifatin, R., Subriadi, A. P., & Gumasing, J. J. (2024). A Comprehensive Review on How Cyber Risk Will Affect the Use of Fintech. Procedia Computer Science, 234, 1356–1363. https://doi.org/10.1016/j.procs.2024.03.134

[8] Kusuma, C. (2024). Perbandingan COSO ERM-Integrated Framework Dengan ISO 31000: 2009 Risk Management Principles and Guidelines. CRMS. https://crmsindonesia.org/publications/perbandingan-coso-erm-integrated-framework-dengan-iso-31000-2009-risk-management-principles-and-guidelines/

Research Article

[9] Lubis, F. S., Praditha, V. S., Lubis, M., Safitra, M. F., & Ramadhan, Y. Z. (2023). IT Risk Analysis Based on Risk Management Using ISO 31000: Case study Registration Application at University XYZ. Proceedings of the 2023 9th International Conference on Industrial and Business Engineering, 522–528. https://doi.org/10.1145/3629378.3629464

[10] Nugraha, U., & Istambul, R. (2019). Implementation of ISO 31000 for Information Technology Risk Management in the Government Environment. International Journal of Advanced Science and Technology, 28(6), 140–145.

[11] Putri, V. R., & Wijaya, A. F. (2022). Information Technology Risk Management Analysis Using ISO: 31000 at PT. XYZ. Journal of Information Systems and Informatics, 4(3), 574–588. https://doi.org/10.51519/journalisi.v4i3.288

[12] Skačkauskienė, I. (2022). Research on management theory: A development review and bibliometric analysis. Problems and Perspectives in Management, 20(2), 335–347. https://doi.org/10.21511/ppm.20(2).2022.28

[13] Suharyani, Y. D., & Djumarno, D. (2023). Perencanaan strategis dan pembangunan berkelanjutan. Jurnal Ilmiah Global Education, 4(2), 767–778. https://doi.org/10.55681/jige.v4i2.827

[14] Vorst, C. R., Priyarsono, D. S., & Budiman, A. (2018). Manajemen Risiko Berbasis SNI ISO 31000. https://perpustakaan.bsn.go.id/repository/ca09e618c360ecd38f4f0ccfc828a2ff.pdf

[15] White, G. B. (2011). The community cyber security maturity model. IEEE International Conference on Technologies for Homeland Security (HST), 173–178. https://doi.org/10.1109/THS.2011.6107866

[16] Wiradarma, A. A. B. A., & Sasmita, G. M. A. (2019). IT Risk Management Based on ISO 31000 and OWASP Framework using OSINT at the Information Gathering Stage (Case Study: X Company). International Journal of Computer Network and Information Security, 11(12), 17–29. https://doi.org/10.5815/ijcnis.2019.12.03