E-ISSN: 2988-585X (Online)

Journal of Elektronik Sistem Informasi (JESII)

Volume 3 No 1 June 2025

DOI: 10.31848/jesii.v3i1.4093

Information Technology Risk Management Of Abc Aplication At University Using Iso 31000:2018

Widi Linggih Jaelani[1], Ahsani Takwim[2], Titania Sari[3], Diyah Wijayanti[4], Satrya Fajri Pratama[5]

[1,2,3,4]Department of Informatics, University Technology Bandung, Indonesia

[5]Sheffield Hallam University, United Kingdom

Article Info

Article history:

Received May 20,25
Revised Jun 29,25
Accepted Jun 30,25

Keywords:

Information Technology
Risk Management
ISO 31000
Cybersecurity
Vulnerability Assessment

ABSTRACT

Information technology (IT) plays a critical role in supporting operations and decision-making in higher education institutions. At University Technology Bandung (UTB), reliance on IT systems for academic administration, online learning, and data management has increased the risk of security incidents such as clickjacking, unrestricted file uploads, cross-site scripting (XSS), misconfiguration, excessive data exposure, and server downtime. This study applies the ISO 31000:2018 risk management framework to systematically identify, assess, and analyze IT security risks in UTB information systems. Using a 5x5 risk matrix, risks were evaluated based on probability and impact, revealing that moderate risks dominate, primarily from clickjacking, XSS, unrestricted file upload, and server downtime incidents, while misconfiguration and excessive data exposure represent low-level risks requiring ongoing monitoring. Common causes include weak input/output validation, insecure system configurations, and inadequate access controls and data sanitization. Proposed mitigation efforts focus on rigorous source code review before publication, regular penetration testing every 3 to 6 months, and increased awareness of security policies and potential incidents. The findings aim to enhance IT risk management practices at UTB, contributing to stronger governance and the protection of institutional data amid growing digital transformation.

Corresponding Author:

Widi Linggih Jaelani
Department of Informatics, Faculty of Creative Industries, University Technology Bandung, Indonesia
Jln. Soekarno-Hatta 378 Bandung, Jawa Barat, Indonesia.
Email: jaelaniwidi@gmail.com

1. INTRODUCTION

Information technology has become the main backbone in supporting operations and decision-making in higher education institutions. University Technology Bandung (UTB), as one of the higher education institutions in the city of Bandung, utilizes IT for various aspects, such as academic administration, online learning, and student data management. However, under these conditions, it leads to an increased dependence on IT and raises the potential risks, such as system disruptions, data breaches, and cyberattacks. Therefore, a systematic framework is needed to identify, analyze, and manage these risks effectively and efficiently.

ISO 31000 is an international standard that provides general principles and guidelines in risk management that can be applied to various types of organizations, including higher education institutions. This standard emphasizes the importance of integrating risk management into all organizational processes, with a focus on achieving strategic objectives [1], [2]. In the context of University Technology Bandung, the implementation of ISO 31000 is expected

to provide a structured approach to managing IT risks, as well as enhancing the reliability of information systems and the overall data security of the institution.

Several studies indicate that the implementation of ISO 31000-based risk management can enhance risk awareness, operational efficiency, and more accurate decision-making [3], [4]. Thus, this research aims to evaluate and design an information technology risk management strategy at University Technology Bandung based on the ISO 31000 framework. The results of this research are expected to make a tangible contribution to strengthening IT governance and supporting the achievement of the university's vision and mission in the era of digital transformation.

2. METHOD

This research uses a descriptive qualitative approach with a case study method at University Technology Bandung, following established practices in IT risk research [5]. The main objective of this research is to identify, analyze, and evaluate existing information technology (IT) risks, as well as to provide risk management recommendations in accordance with the ISO 31000 framework, which has been widely adopted in various organizational risk studies [6].

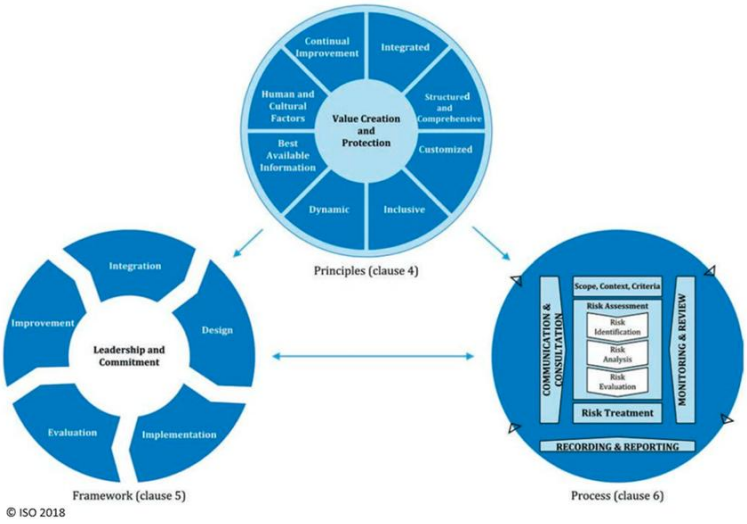

Figure 1. Risk management process (ISO 31000, 2018) [7]

2.1 Data Collection

Data is obtained through two main techniques:

a. In-depth interviews with relevant parties such as the head of the IT division, IT staff, and risk management.
b. Internal documentation such as information security policies, incident reports, and IT audits. According to [8], a combination of interviews and documentation is an effective technique for uncovering hidden risks in IT systems.

2.2 Risk Identification

Risk identification is carried out using the ISO 31000:2018 guidelines, which emphasize understanding the organizational context, including internal and external factors that affect IT risks [9].

2.3 Analysis and Evaluation Risk

Risk is analyzed based on the likelihood of occurrence and its impact. The risk matrix method is used to map and categorize the level of risk [10], the use of a risk matrix facilitates the visualization of risk handling priorities in information systems within the higher education environment.

2.4 Risk Management

After risks are identified and evaluated, handling strategies are implemented based on the four main approaches of ISO 31000: accepting, avoiding, reducing, or transferring risks [11].

2.5 Monitoring and Evaluation

This research also includes a continuous evaluation of the effectiveness of IT risk management strategies through the measurement of key performance indicators (KPIs) . These KPIs are used to assess improvements in system security, responsiveness to threats, and the overall reduction in risk exposure over time [12], [13].
The monitoring stage is carried out through a combination of methods, including:

a. System log analysis: Reviewing logs from web servers, firewalls, and intrusion detection systems to identify patterns and anomalies [14].
b. Periodic internal audits: Conducted at least every 6 months to evaluate policy compliance and effectiveness of implemented controls (ISO/IEC 27001, 2022) [5].
c. Incident reporting and documentation: Manual and automated reporting of incidents by IT staff.
d. Dashboard monitoring: Using monitoring tools to track system uptime, failed access attempts, and average response times.

Key indicators monitored include:

a. Number of security incidents
b. Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR)
c. Percentage of system uptime
d. Compliance rate with security controls

The review process is led by the IT Security and Risk Management Division and is scheduled on a biannual basis. Evaluation results are used to update the risk register, inform future control strategies, and support continual improvement as recommended by ISO 31000:2018 and ISO/IEC 27001:2022 [1], [5].

3. RESULT AND DISCUSSION

This stage aims to identify and evaluate potential information security risks that may affect the information systems (specifically the website) at University Technology Bandung, as well as to determine appropriate treatments based on the findings.

3.1. Incident

The following incidents represent common information security risks identified in the University Technology Bandung's information systems. These incidents range from web-based attacks like clickjacking and cross-site scripting to system vulnerabilities such as misconfiguration and server downtime. Understanding these incidents is essential for assessing and managing the university's IT security risks effectively.

Table 1 Incident

No	Incident
1	Clickjacking
2	Unrestricted File Upload
3	Cross Site Scripting
4	Misconfiguration
5	Excessive Data Exposure
6	Unrestricted File Upload Lead to XSS
7	Server Down

3.2. Impact Level Criteria

The impact level criteria categorize the severity of consequences resulting from an information security incident. These levels range from Information, which has minimal effect and is purely informational, to Critical, which represents severe disruptions potentially affecting entire servers or multiple systems. Defining impact levels helps organizations prioritize responses and allocate resources effectively to mitigate risks based on their potential damage.

Table 2 Impact Level Criteria

Impact Level	Impact Level
Information	Causes a very low impact and is only informational in nature.
Low	Causes a low impact and disrupts some ongoing processes.
Medium	Causes a moderate impact and affects only the disrupted system
High	Causes a high impact and can disrupt other systems.
Critical	Causes a very high impact and can disrupt the server or other systems.

3.3. Threat Occurrence Probability Criteria

The criteria for threat occurrence probability define how often a specific threat is expected to happen within a given time frame, typically six months. These categories range from Very Rare, indicating the threat might occur less than once in six months, to Very Frequent, where the threat could happen more than six times within the same period. This classification assists in evaluating the likelihood of risks and helps prioritize mitigation efforts accordingly.

Table 3 Threat Occurrence Probability Criteria

Value	Probability (Frequency of Occurrence)
Very Rare	The threat is likely to occur less than once in 6 months
Rare	The threat is likely to occur 1 to 2 times in 6 months
Occasional	The threat is likely to occur 2 to 4 times in 6 months
Frequent	The threat is likely to occur 4 to 6 times in 6 months
Very Frequent	The threat is likely to occur more than 6 times in 6 months

3.4. Information Security Risk Value and Level

The value of information security risk is assessed based on the result of multiplying the likelihood of a threat occurring by the level of impact it may cause. Meanwhile, the level of information security risk is determined by categorizing the risk value to describe the degree of information security risk.

3.4.1. The Information Security Risk Value

The information security risk value is determined by multiplying the likelihood of a threat occurring by the impact level it would cause. This risk value helps quantify the severity of potential security incidents. The 5 by 5 Risk Analysis Matrix categorizes risks based on five levels of impact, from informational to critical, and five levels of likelihood, from very rare to almost certain. By mapping these two dimensions, organizations can assess, prioritize, and manage risks more effectively to ensure appropriate mitigation strategies are applied.

Table 4 Threat Occurrence Probability Criteria

Risk Analysis Matrix 5x5			Impact Level				
			1	2	3	4	5
			Information	Low	Medium	High	Critical
Likelihood Level	5	Almost Certain	5	10	15	20	25
	4	Likely	4	8	12	16	20
	3	Occasionally	3	6	9	12	15
	2	Rare	2	4	6	8	10
	1	Very Rare	1	2	3	4	5

3.4.1. Information Security Risk Level of the UTB Website

The risk level classifies the severity of information security risks based on the calculated risk values. These levels help prioritize responses by indicating the urgency and potential impact of risks. Each risk level corresponds to

a range of risk values and is visually represented by a specific color to facilitate quick recognition and decision-making.

Table 5 Information Security Risk

	Risk Level	Risk Value Range	Color
1	Information	1-3	Blue
2	Low	4-6	Green
3	Medium	8-10	Yellow
4	High	12-16	Orange
5	Critical	20-25	Red

3.4. Risk Acceptance and Treatment Criteria

Criteria are established to determine information security risks that can be accepted or treated based on their risk value or risk value groups.

Table 6 Risk Value

Risk Value	Risk Acceptance	Risk Management
1-6	Risk Accepted or Ignored	No control action needed; the threat to information assets is sufficiently monitored.
8-16	Risk Rejected	Risk control or mitigation is carried out by allocating available resources.
20-25	Risk Rejected or Transferred	Risk control is implemented as soon as possible, or the risk is transferred to another party.

Table 7 Information Security Risk Value

No	Incident	Risk Description	Risk Value	Control	Proposed Security Control
1	Clickjacking	Clickjacking occurs because the browser still allows framing from other domains and no defensive code is implemented in the UI to ensure the window is at the top level. This incident happens approximately once every six months and can lead to data theft or unintentional malware downloads by users.	5 (Medium)	Maintenance source code	Perform source code reviews before publishing and conduct regular penetration testing at least once every 3 to 6 months.
2	Unrestricted File Upload	Unrestricted File Upload occurs when the system fails to properly check or filter uploaded file types. This can happen approximately once every six months and may allow attackers to access server information or even take full control of the server.	5 (Medium)	Maintenance source code	Conduct source code reviews before deployment and perform regular penetration testing at least every 3 to 6 months.
3	Cross Site Scripting	Cross Site Scripting is a type of injection where malicious scripts are embedded into a	5 (Medium)	Maintenance source code	Perform source code reviews before publishing and

No	Incident	Risk Description	Risk Value	Control	Proposed Security Control
		website. This can occur approximately once every six months, potentially allowing attackers to gain full control of the website.			conduct regular penetration testing at least every 3 to 6 months.
4	Misconfiguration	Misconfiguration occurs due to inadequate security settings or the use of default configurations. This can happen approximately once every six months, allowing attackers to access information from errors in the web application.	3 (Information)	Maintenance source code	Review the source code before publishing and perform regular penetration testing at least every 3 to 6 months.
5	Excessive Data Exposure	Excessive Data Exposure occurs due to the lack of proper response standards for failed processes. This happens about once every six months, allowing attackers to view sensitive information from web application responses.	3 (Information)	Maintenance source code	Conduct source code reviews before publishing and perform regular penetration testing at least every 3 to 6 months.
6	Unrestricted File Upload	Unrestricted File Upload occurs when the system fails to properly check or filter uploaded file types. This can happen approximately once every six months and may allow attackers to access server information or even take full control of the server.	5 (Medium)	Maintenance source code	Conduct source code reviews before deployment and perform regular penetration testing at least every 3 to 6 months.
7	Server Down	The server fails to operate during periods of heavy traffic, occurring approximately four times within a six-month period. This results in interruptions to services and delays in processing across all systems.	2 (Low)	Awareness	Implement server monitoring and load balancing mechanisms to prevent downtime under heavy traffic. Conduct regular load testing, enhance system scalability, and train IT staff to respond quickly to server failure incidents.

The recommendation to perform source code reviews and penetration testing every 3 to 6 months is aligned with industry security best practices, particularly those outlined by the OWASP Testing Guide and the OWASP Application Security Verification Standard (ASVS). These guidelines emphasize the importance of regular assessments for applications with medium to high risk exposure. Specifically, ASVS Level 2 suggests that systems handling sensitive data or business-critical functions should undergo periodic code reviews and security testing, especially after major changes or deployments. This 3–6 month interval provides a practical balance between proactive mitigation and operational feasibility [15], [16].

Table 8 Evaluation of Identified Incidents Based on Likelihood and Impact

No	Incident	Likelihood Level	Impact Level	Risk Value	Risk Level
1	Clickjacking	2 (Rare)	5 (Critical)	10	Medium
2	Unrestricted File Upload	2 (Rare)	5 (Critical)	10	Medium
3	Cross Site Scripting (XSS)	2 (Rare)	5 (Critical)	10	Medium
4	Misconfiguration	1 (Very Rare)	3 (Medium)	3	Information
5	Excessive Data Exposure	1 (Very Rare)	3 (Medium)	3	Information
6	File Upload Leading to XSS	2 (Rare)	5 (Critical)	10	Medium
7	Clickjacking	2 (Rare)	5 (Critical)	10	Medium

3.5 Discussion and Comparison with Previous Studies

The results of this study show that the most dominant risks in UTB's IT systems are medium-level threats such as clickjacking, XSS, and unrestricted file uploads. These findings are consistent with those of Rahmadani et al. [10], who identified similar attack vectors as prevalent risks in university web systems. Additionally, the frequent occurrence of misconfiguration and excessive data exposure as low-level risks supports the observations of Permana et al. [8], which noted that such issues often result from weak governance and lack of policy enforcement.

Compared to Al-Shboul and Al-Hadid [9], who emphasized the role of institutional risk culture in shaping effective IT risk strategies, UTB's approach is still developing. However, the implementation of ISO 31000 in this study demonstrates the usefulness of structured risk mapping and mitigation planning in an academic environment. Unlike previous studies that focused solely on assessment, this research also proposes specific action plans including code reviews and scheduled penetration testing.

Therefore, this research contributes to the ongoing efforts in strengthening IT governance in higher education, particularly by offering a practical example of ISO 31000 implementation tailored to university systems.

4. CONCLUSION

This document contains the results of incident identification and information security risk analysis that may potentially affect the information systems at University Technology Bandung (UTB). Based on the ISO 31000:2018 standard, risk assessments were conducted on various incidents such as clickjacking, unrestricted file upload, cross-site scripting (XSS), misconfiguration, excessive data exposure, and potential server downtime. Key findings: Medium risks (risk value 5–8) are the most dominant, associated with incidents such as clickjacking, XSS, unrestricted file upload, and server downtime. Information (risk value 3) stems from incidents such as misconfiguration and excessive data exposure, although they still require monitoring. Common causes of these risks include weak input/output validation, insecure system configurations, lack of access restrictions, and insufficient data sanitization. All identified risks have been analyzed using a 5x5 risk matrix based on likelihood and impact. Proposed mitigation efforts: Perform thorough reviews and maintenance of source code before publication. Conduct periodic penetration testing every 3 to 6 months. Increase awareness of potential incidents and ensure the implementation of appropriate information security policies.

ACKNOWLEDGEMENTS

Thank you to all parties who have supported this research so that it can be completed properly. Especially for the parents who have always supported and guided me in this research. I'm very grateful.

REFERENCES

[1] ISO, "ISO 31000:2018 – Risk management – Guidelines, International Organization for Standardization," *Geneva*, 2018.

[2] H. Berg, "Applying ISO 31000 to IT Risk Management: Lessons from European Organizations," *Information & Computer Security*, vol. 30, no. 1, pp. 85–101, 2022.

[3] P. Hopkin, *Fundamentals of Risk Management Understanding, evaluating and implementing effective risk maagement*, 5th ed. London, 2018.

[4] P. J. Baraloni, M. M. Glick, and S. A. Wilson, "The effectiveness of ISO 31000 implementation in higher education institutions," *Journal of Risk and Governance*, vol. 12, pp. 87–96, 2020.

[5] I. 27001:2022 – I. S. ISO/IEC, "Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements, International Organization for Standardization," *Geneva*, 2022.

[6] R. K. Yin, "Case Study Research and Applications: Design and Methods," *Thousand Oaks, CA: Sage Publications*, 2018.

[7] S. H. Björnsdottir, P. Jensson, S. E. Thorsteinsson, I. M. Dokas, and R. J. de Boer, "Benchmarking ISO Risk Management Systems to Assess Efficacy and Help Identify Hidden Organizational Risk," *Sustainability (Switzerland)*, vol. 14, no. 9, pp. 1–33, 2022, doi: 10.3390/su14094937.

[8] A. N. Permana, M. F. Ramadhani, and R. Hidayat, "Information Risk Identification in University Information System Using ISO 31000: A Case Study," *Jurnal Sistem Informasi*, vol. 17, no. 3, pp. 250–258, 2021.

[9] S. H. Al-Shboul and M. T. Al-Hadid, "Implementing ISO 31000 for IT Risk Management in Higher Education," *Journal of Risk and Financial Management*, vol. 14, no. 11, pp. 1–18, 2021.

[10] R. Rahmadani, T. Sari, and A. K. Darmawan, "Assessment of IT Risks in Higher Education Using ISO 31000 Risk Matrix," *Journal of Information Systems Engineering and Business Intelligence*, vol. 7, no. 2, pp. 83–91, 2021.

[11] S. . F. Nugroho and D. Susanto, "Risk Treatment Strategy Based on ISO 31000 for IT Governance in University," *International Journal of Information Systems and Technologies*, vol. 10, no. 1, pp. 12–20, 2023.

[12] E. Harisun, "Risk Management Analysis of Key Performance Indicators (IKU) of the Faculty of Engineering , Khairun University," vol. 2025, pp. 82–98, 2025.

[13] S. T. Harrop, "Integrating KPIs into IT Risk Management for Higher Education Institutions," *International Journal of Information Security and Education*, vol. 10, no. 3, pp. 55–62, 2020.

[14] A. Rusu and S. Dragomir, "Effective Risk Monitoring Techniques in Information Security Management," *Journal of Information Systems Management*, vol. 14, no. 3, pp. 28–34, 2021.

[15] "OWASP Testing Guide v4," *OWASP Foundation*, 2014.

[16] O. Foundation, "OWASP Application Security Verification Standard 4.0.3 OWASP Foundation," *OWASP Foundation*, 2021.