International Journal Software Engineering and Computer Science (IJSECS)
5 (2), 2025, 587-598
Published Online August 2025 in IJSECS (http://www.journal.lembagakita.org/index.php/ijsecs)
P-ISSN: 2776-4869, E-ISSN: 2776-3242. DOI: https://doi.org/10.35870/ijsecs.v5i2.4549.

RESEARCH ARTICLE Open Access

Risk Management Evaluation Based on ISO/IEC 27005 Framework: A Case Study of ABC Company IT Workshop Room

Muhammad Ferdi Kurniawan *
Bachelor of Informatics Study Program, Faculty of Science and Business, Universitas LIA, South Jakarta City, Special Capital Region of Jakarta, Indonesia.
Corresponding Email: ferdi.kurniawan@universitaslia.ac.id.

Triana Dewi Salma
Bachelor of Informatics Study Program, Faculty of Science and Business, Universitas LIA, South Jakarta City, Special Capital Region of Jakarta, Indonesia.
Email: triana.salma@universitaslia.ac.id.

Received: June 17, 2025; Accepted: June 30, 2025; Published: August 1, 2025.

Abstract: ABC Company operates as a technology firm based in France, maintaining its research and development operations in Jakarta. The company produces digital security technologies—biometrics, facial recognition systems, and digital identity solutions—alongside telecommunications and payment products including SIM cards, banking cards, and smart cards. Given how much the company relies on technology and secure information handling, it needs strong systems and infrastructure, especially when dealing with sensitive data. Yet no one has conducted a risk management assessment of the IT workshop room. Several problems have emerged with the physical security of this important area, such as people misusing access privileges and assets going missing. This research evaluates how the company manages information security risks by first identifying what's causing these problems through a fishbone diagram that looks at people, technology, and processes. We then assessed risks using the ISO/IEC 27005:2018 standard across 12 assets, examining threats, current controls, weak points, and what treatments are needed. Our analysis shows three assets (A5, A6, A7) carry high risk, three others (A4, A9, A12) have medium risk, and six assets (A1, A2, A3, A8, A10, A11) present low risk. Using these results, we developed specific recommendations for handling risks associated with each asset to improve information security throughout the company.

Keywords: Risk Management; Information Security; Information Technology; ISO/IEC 27005:2018.

1. Introduction

The rapid advancement of digital technology has pushed companies to continuously innovate, particularly when it comes to information security and digital systems. Intense business competition in our globalized world demands the right technological implementation through information system-based corporate strategies to make the most of limited resources [1]. ABC Company, headquartered in France with its Research and Development Center in Jakarta, stands as one of the technology firms producing digital security products like biometrics, face recognition, and digital identity systems. The company also manufactures telecommunications and payment devices, including SIM cards, bank cards, and various smart cards.

As an organization heavily dependent on information systems and technology, data security becomes absolutely critical to its operations. The products and services the company delivers involve processing and storing sensitive data, which means they need reliable security systems from both technical and non-technical perspectives. One area that deserves special attention is the IT workshop space, where critical operational activities take place. ABC Company has implemented a tiered security system based on employee accreditation and work zones divided into three levels:

1) Level 1 is designated for office teams working in general areas and zones that the public can also access.
2) Level 2 can only be accessed by R&D team members involved in level 2 projects who have authorization to enter rooms in that zone.
3) Level 3 maintains the highest security level, covering access to rooms, networks, and data, and only those holding level 3 cards can enter.

The IT Workshop room represents one of the level 3 areas, used by IT teams and security teams to carry out critical activities. Access to this room is restricted to members of both teams during daily operations. The room also includes a storage area for the company's operational assets, including PCs, laptops, backup tape servers, and security team assets.

However, no risk management assessment has been conducted for this IT workshop space until now. Risk management represents a systematic process for identifying and evaluating potential risks within a company to determine appropriate handling measures [2]. Several incidents, from access misuse to asset loss, have revealed weak physical security in this area. This situation indicates that the company lacks an adequate risk management system to protect important assets in the IT space. To identify root problems and existing risk potential, this research uses a fishbone diagram approach focusing on three main areas: people, technology, and process. We then conducted risk assessment based on the ISO/IEC 27005:2018 standard, which includes identifying assets, threats, vulnerabilities, along with relevant controls and treatments. ISO/IEC 27005:2018 provides guidance for managing information security risks, specifically designed to support implementation of Information Security Management System (ISMS) requirements based on the ISO/IEC 27001 standard [3].

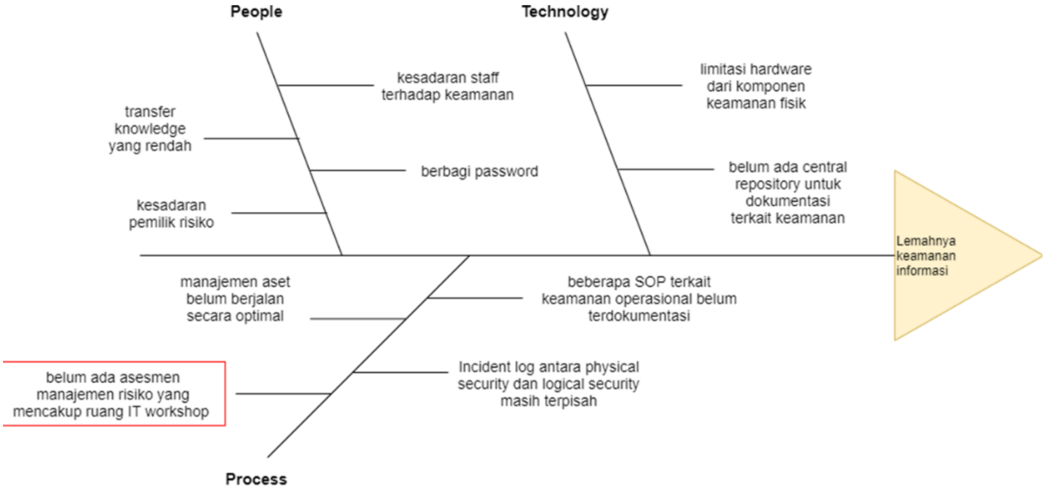

People
Technology
kesadaran staff terhadap keamanan
transfer knowledge yang rendah
berbagi password
kesadaran pemilik risiko
limitasi hardware dari komponen keamanan fisik
belum ada central repository untuk dokumentasi terkait keamanan
Lemahnya keamanan informasi
manajemen aset belum berjalan secara optimal
beberapa SOP terkait keamanan operasional belum terdokumentasi
belum ada asesmen manajemen risiko yang mencakup ruang IT workshop
Incident log antara physical security dan logical security masih terpisah
Process

Figure 1. Fishbone Diagram.

2. Related Work

Information security risk management has emerged as a critical concern for technology companies aiming to safeguard their valuable assets and preserve data integrity. Numerous researchers have investigated the application of international standards, with ISO/IEC 27005 receiving particular attention as a structured methodology for risk identification and management. Recent work by Sinaga and Taan (2024) showed that ISO/IEC 27001:2022 implementation assisted organizations in addressing information system security management difficulties, particularly in process evaluation and identifying implementation barriers [10]. Their findings indicated that systematic governance approaches can substantially improve risk management outcomes. In a related study, Isnaini *et al.* (2023) examined ISO/IEC 27005:2019 effectiveness for risk assessment in public service applications, specifically village service systems [7]. The authors found that standard implementation revealed previously hidden vulnerabilities while providing actionable mitigation strategies. The governmental sector has also benefited from ISO/IEC 27005 implementation, as demonstrated by Fahrurozi *et al.* (2020) in their Ministry of Defense Data and Information Center case study [11]. Their work illustrated how risk-based approaches offer broad perspectives on information security threats. Building on classification frameworks, Agrawal (2017) established methods for categorizing information assets according to risk levels within ISO/IEC 27005 parameters [12]. Meanwhile, Mahardika *et al.* (2019) explored ISO 31000:2018 integration with ISO/IEC 27001, demonstrating enhanced risk management capabilities in information technology environments [8].

Alternative analytical approaches have gained traction in recent years. Handayani *et al.* (2019) applied Failure Mode Effect and Analysis (FMEA) methodology within ISO 27001 frameworks for information system risk evaluation [6]. Their research demonstrated successful integration between different analytical methods and established security standards. The educational sector has provided valuable insights, with Agustino (2018) documenting physical component weaknesses and operational procedure gaps in institutional settings [4]. These findings revealed that physical security vulnerabilities often create exploitable entry points for unauthorized access. Physical security research has expanded beyond traditional boundaries. Ningrum *et al.* (2024) investigated how inadequate physical design contributes to security breaches and potential data compromise [9]. Using the Information System Security Index (KAMI) approach, they analyzed university information systems and found significant correlations between physical security measures and overall system protection levels. Complementing these findings, Fahrudin *et al.* (2022) employed NIST SP 800-30 frameworks to assess employee data security risks, offering alternative perspectives on organizational sensitive information protection [5].

Methodological diversity characterizes current risk assessment research. Ariyani and Sudarma (2016) successfully implemented ISO/IEC 27005 for management information system security analysis, providing practical guidance for risk identification and management processes [13][16]. Government-specific applications received attention from Patiño *et al.* (2018), who developed specialized ICT risk management methodologies for governmental entities using ISO/IEC 27005 foundations [15]. Their work highlighted standard adaptability across different organizational structures. Theoretical foundations have also advanced through ontological research. Agrawal (2016) constructed ontological frameworks for ISO/IEC 27005:2011 risk management standards, establishing clearer relationships between standard components [14]. Such theoretical work helps standardize terminology and conceptual understanding across information security risk management practices. Contemporary cybersecurity research increasingly emphasizes balanced approaches. Handri *et al.* (2023) evaluated People, Process, and Technology priorities within NIST Cybersecurity Framework implementation for e-government applications [17]. Their analysis revealed that human factors often represent both the most crucial and most challenging aspects of security system management.

Several research gaps persist despite extensive investigation in information security risk management. Most existing studies address general standard implementation without considering unique characteristics of IT workshop environments, which present distinct challenges regarding access control, asset management, and operational procedures. Additionally, literature lacks examples of fishbone diagram integration with ISO/IEC 27005 for root cause analysis in physical security scenarios. Furthermore, holistic approaches that balance people, technology, and process elements specifically within multinational technology company IT workshop settings remain underexplored. The present research addresses these gaps by combining fishbone diagram analysis with ISO/IEC 27005:2018 methodologies to identify and manage information security risks in IT workshop environments. The study particularly focuses on integrating people, technology, and process dimensions within technology companies that employ multi-layered security architectures.

3. Research Method

The Risk Management Process was conducted based on ISO/IEC 27005:2018. ISO 27005 is a framework specifically designed and structured as a systematic method for identifying information security risks, aimed at helping organizations recognize potential threats, understand information asset vulnerabilities, and assess the likelihood and impact that may arise, thereby supporting comprehensive and measurable risk management [18]. The assessment stages conducted include: problem identification, asset determination, risk evaluation, existing control evaluation, appropriate control selection, and conclusion drawing with recommendation provision. Data collection and processing were performed through interview methods, completion of assessment checklists structured based on control objectives from ISO/IEC 27005:2018, and analysis of company internal documents. Interviews were conducted with three main sources: Security Manager, IT Operational Manager, and HR Director from Company XYZ. In the risk handling process, discussions were held with these three sources to validate findings. The validation results serve as the basis for management to determine risk handling steps, whether to accept, reduce, prevent, or transfer risks, in accordance with established risk acceptance criteria.

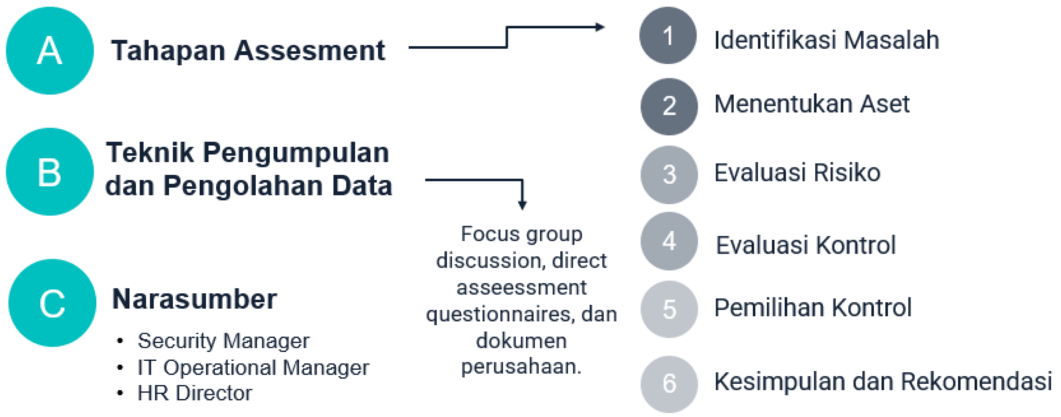


Figure 2. Research Stages.

4. Result and Discussion

4.1 Results

4.1.1 Problem Identification and Asset Determination

Determination is the initial stage in risk assessment that determines the scope of evaluation of IT assets, especially applications, by determining the data to be assessed, the impact value and frequency, the level of threat likelihood (low, medium, high), and risk calculation criteria [19].

Table 1. Problem Identification and Asset Determination

No	Asset	Threat	Control	Vulnerability
1	Physical Security Team – Laptop	• Device problems • Access privilege abuse • Device theft • Data theft • Vandalism	No control	• Has shared admin password • Sometimes borrowed by other teams outside physical security team • Does not use Kensington lock
2	Physical Security Team – PC	• Device problems • Access privilege abuse • Device theft • Data theft • Vandalism • Access control server configuration errors • Full repository	No control	• Has shared admin password • Functions as access control system server, if CPU error occurs then access control manager application cannot be accessed • Functions as local repository for access control data, alarm system, and surveillance system
3	IT Team - Laptop	• Device problems • Access privilege abuse • Device theft • Data theft • Vandalism	No control	Does not activate lock screen
4	IT Team - PC	• Device problems • Access privilege abuse • Vandalism • Invalid asset data • CCTV not operating	PC storage area monitored 24 hours by CCTV	• Does not activate lock screen • Asset management not performed properly • PCs stored in storage not updated in asset management
5	Access Control	• Device problems • Access privilege abuse • Vandalism	• Dual authentication access (card + fingerprint)	• Security breach (infiltration)

		• Configuration errors • Full storage media • Power access interrupted • Backup battery capacity depleted • Incomplete/corrupted system log history	• Limited access for security and IT staff only • System log and activity history always downloaded and backed up monthly	• If power outage, biometric device only lasts 2 hours with backup battery • Access control manager application has complex configuration • Login to access control manager application set to auto login • Access control Log (history) cannot record history comprehensively • No formal SOP for data backup and system maintenance
6	Alarm System	• Device problems • Configuration errors • Procedure abuse • Full storage media • Power access interrupted • Vandalism • Incomplete/corrupted system log history	• System log and activity history always downloaded and backed up monthly • Access to alarm system application limited to physical security team only	• Sensitivity/accuracy of devices (sensors) has weakened for detection • Several sensors (shock detector & motion sensor) are old • Alarm panel system uses outdated technology • Alarm system manager application has complex configuration • Login password for alarm system manager application is weak • Alarm Log (history) cannot record activities more than 500 histories • Alarm log (history) sometimes not recorded by system • No formal SOP for data backup and system maintenance
7	Surveillance System (CCTV)	• Device problems • Configuration errors • Vandalism • Full storage media • Power access interrupted • Incomplete/corrupted system log history	• Has night mode recording feature (infrared) • Recording done only when there is movement (motion) so it does not record continuously • Recording history always checked periodically (monthly) • Time synchronization for time stamp checked regularly	• CCTV monitoring application not updated • Some IP Cameras have exceeded service life • Inaccurate recording time stamp • Real-time video sometimes does not appear on security monitoring screen • No formal SOP for data backup and system maintenance • NVR storage can only store recording data for about the last 3 months
8	UPS	• Device problems • Electrical network configuration errors • Limited power storage capacity • Long-term power outage	No control	• Already old • UPS for CCTV can only cover for 15 minutes if power outage occurs • UPS for Alarm System combined with CCTV UPS

		• Vandalism		
9	Backup Battery - Access Control	• Device problems • Device theft • Limited power storage capacity	Functional check at least once a year	Can only cover for 2 hours if main power outage occurs
10	Electricity	• Power access interrupted • Electrical short circuit • Limited generator fuel capacity	• Generator from main building • UPS backup	Power exceeds load
11	Security Network	• Access privilege abuse • Configuration errors	Network check once a month	Unauthorized access to security LAN network (special network not connected to internet)
12	Personnel (IT & Security Team)	• Access privilege abuse • Procedure abuse • Vandalism • Inaccurate incident data • Data and device theft	Security training conducted annually	• Abuse of access to IT Workshop room • Unauthorized access system • Incident reports not escalated • System configuration records scattered • Computer access abuse

4.1.2 Risk Evaluation

Risk assessment for applications at Company ABC refers to calculation criteria from ISO 27005:2008, where if a risk meets several different impact level categories, the highest impact level will be used as reference. Vandalism risk that has low financial impact but medium impact on reputation will be classified as risk with medium impact level.

Table 2. Impact Criteria

Impact Level	Impact Criteria
	Actual Loss (Financial)
Low	0% < unconsolidated monthly revenue ≤ 0.25%
Medium	0.25% < unconsolidated monthly revenue ≤ 2.5%
High	unconsolidated monthly revenue ≥ 2.5%

(Source: ISO 27005, 2008)

Calculation criteria according to ISO 27005:2008 connect the likelihood of threat occurrence with the effectiveness of existing controls to produce the likelihood value of incident scenario [19].

Table 3. Likelihood Criteria

Likelihood	Occurrence Probability	Frequency
Low	Chance of occurrence < 2 times in 1 year	Very Rarely Occurs
Medium	Chance of occurrence 3-5 times in 1 year	Sometimes Occurs
High	Chance of occurrence > 6 times in 1 year	Often Occurs

(Source: ISO 27005, 2008)

Based on results conducted at Company ABC, the following is the evaluation of existing risks with their coding.

Table 4. Risk Evaluation

Asset (Code)	Threat (Code)	Impact Level	Likelihood Level
A1. Physical Security Team – Laptop	T1. Device problems	Medium	Low
	T2. Access privilege abuse	High	Low
	T3. Device theft	High	Low
	T4. Data theft	High	Low
	T5. Vandalism	Medium	Low
A2. Physical Security Team - PC	T6. Access control server configuration errors	Medium	Low

	T7. Full repository	Medium	Medium
A3. IT Team - Laptop	T1. Device problems	Medium	Low
	T2. Access privilege abuse	High	Low
	T3. Device theft	High	Low
	T4. Data theft	High	Low
	T5. Vandalism	Medium	Low
A4. IT Team - PC	T1. Device problems	High	Low
	T2. Access privilege abuse	High	Low
	T5. Vandalism	Medium	Low
	T8. Invalid asset data	Medium	Medium
	T9. CCTV not operating	High	Medium
A5. Access Control	T1. Device problems	High	High
	T2. Access privilege abuse	High	High
	T5. Vandalism	High	Low
	T10. Configuration errors	High	Medium
	T12. Full storage media	Medium	High
	T13. Power access interrupted	High	Medium
	T14. Backup battery capacity depleted	High	Medium
	T20. Incomplete/corrupted system log history	Medium	Medium
A6. Alarm System	T1. Device problems	High	High
	T10. Configuration errors	High	Medium
	T11. Procedure abuse	High	Low
	T12. Full storage media	High	High
	T13. Power access interrupted	High	Medium
	T5. Vandalism	High	Low
	T20. Incomplete/corrupted system log history	Medium	High
A7. Surveillance System (CCTV)	T1. Device problems	High	High
	T10. Configuration errors	High	Medium
	T5. Vandalism	High	Low
	T12. Full storage media	High	Medium
	T13. Power access interrupted	High	Medium
	T20. Incomplete/corrupted system log history	Medium	High
A8. UPS	T1. Device problems	High	Low
	T15. Electrical network configuration errors	High	Low
	T16. Limited power storage capacity	High	Low
	T17. Long-term power outage	High	Low
	T5. Vandalism	High	Low
A9. Backup Battery - Access Control	T1. Device problems	High	Medium
	T3. Device theft	Medium	Low
	T16. Limited power storage capacity	High	Medium
A10. Electricity	T13. Power access interrupted	High	Low
	T18. Electrical short circuit	High	Low
	T19. Limited generator fuel capacity	High	Low
A11. Security Network	T2. Access privilege abuse	High	Low
	T10. Configuration errors	Medium	Low
A12. Personnel (IT & Security Team)	T2. Access privilege abuse	High	High
	T11. Procedure abuse	High	Medium
	T5. Vandalism	Medium	Low
	T8. Inaccurate incident data	High	Medium
	T21. Data and device theft	High	Low

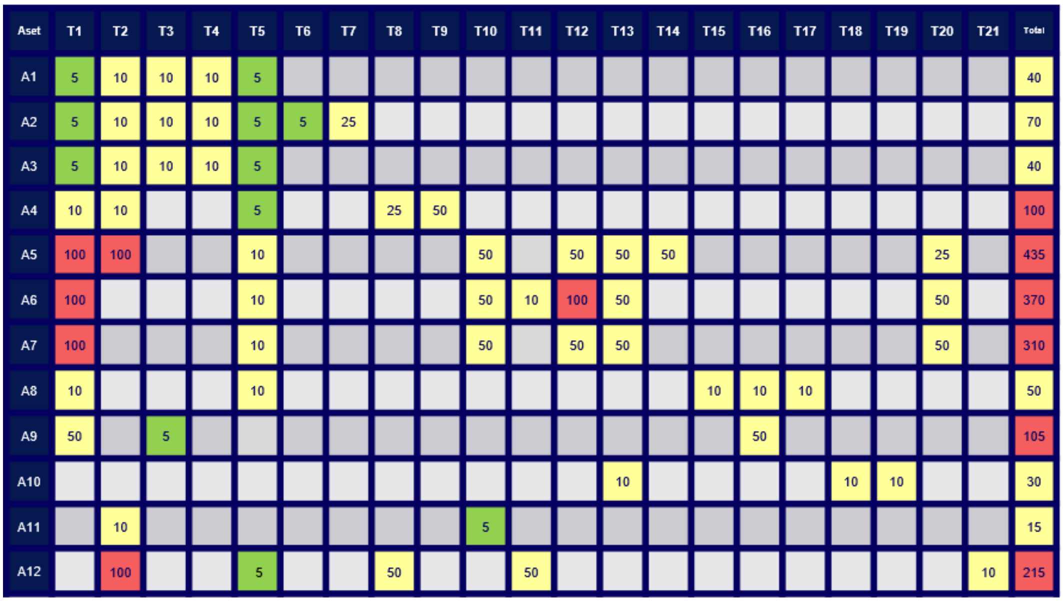
4.1.3 Control Evaluation

The risk evaluation stage is conducted with the aim of compiling a risk priority list, established based on evaluation criteria relevant to risk scenarios that contribute to the occurrence of such risks [20]. Evaluation of risk values is first performed by researchers referring to risk analysis results compiled in the previous stage. After the initial evaluation process is complete, researchers then discuss the results in depth with case study owners to obtain input, clarification, and validation of calculations performed.

Table 5. Evaluation Value Calculation

Business Impact	Threat Probability		
	Low (0.1)	Medium (0.5)	High (1)
Low (10)	Low (10 x 0.1) = 1	Low (10 x 0.5) = 5	Low (10 x 1) = 10
Medium (50)	Low (50 x 0.1) = 5	Medium (50 x 0.5) = 25	Medium (50 x 1) = 50
High (100)	Medium (100 x 0.1) = 10	Medium (100 x 0.5) = 50	High (100 x 1) = 100

This evaluation aims to ensure that obtained risk values reflect actual field conditions and are appropriate to the context and characteristics of the company being studied. The risk value filling process is performed using the risk evaluation formula, namely multiplying the impact level with the threat occurrence likelihood level, to obtain a risk score representing the magnitude of potential risk to the assessed asset. The results obtained are mapped in Figure 2.



Aset	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	T16	T17	T18	T19	T20	T21	Total
A1	5	10	10	10	5																	40
A2	5	10	10	10	5	5	25															70
A3	5	10	10	10	5																	40
A4	10	10			5			25	50													100
A5	100	100			10					50		50	50	50						25		435
A6	100				10					50	10	100	50							50		370
A7	100				10					50		50	50							50		310
A8	10				10										10	10	10					50
A9	50		5													50						105
A10													10					10	10			30
A11		10								5												15
A12		100			5			50			50										10	215

Figure 3. Control Evaluation

4.1.4 Control Selection

The control selection stage is conducted based on total values and average risks calculated previously, to determine the most effective control action priorities in mitigating risks to assessed assets.

Table 6. Control Selection

Priority	Asset & Scenario	Total Risk Value	Average Risk Level
1	A5. Access Control (T1, T2, T5, T10, T12, T13, T14, T20)	435	54
2	A6. Alarm System (T1, T5, T10, T11, T12, T13, T20)	370	53
3	A7. Surveillance System (T1, T5, T10, T12, T13, T20)	310	52
4	A12. Personnel (T2, T5, T8, T11, T21)	215	43
5	A9. Backup Battery (T1, T3, T16)	130	33
6	A4. IT Team - PC (T1, T2, T5, T8, T9)	100	20
7	A2. Physical Security Team - PC (T1, T2, T3, T4, T5, T6, T7)	70	10
8	A8. UPS (T1, T5, T15, T16, T17)	50	10
9	A10. Electricity (T13, T18, T19)	30	10
10	A11. Security Network (T2, T10)	20	8
11	A3. IT Team - Laptop (T1, T2, T3, T4, T5)	40	8
12	A1. Physical Security Team - Laptop (T1, T2, T3, T4, T5)	40	8

4.1.5 Control Selection

The risk management assessment conducted has produced several recommendations that can be accepted by PT. XYZ management because they can resolve several problems including:

1) Management becomes aware of the importance of building an Asset Management System to serve as a reliable information source for asset traceability.
2) Strengthening User Access Control Policy can minimize access privilege abuse and password sharing habits.
3) Management becomes aware of the importance of developing SOPs related to operational security, as proper documentation can be an efficient knowledge transfer method.
4) Management becomes aware of the importance of building a centralized repository for security systems (configuration, documentation, backup, and others) because currently repositories are still stored locally and individually.
5) Management agrees to provide strict sanctions to security violators to create a deterrent effect. Staff must also attend security training (annual refreshment) to ensure all staff have awareness of information security.

4.2 Discussion

Based on the research results conducted, the implementation of ISO/IEC 27005:2018 in managing information security risks within Company XYZ's IT Workshop environment shows significant findings and provides valuable understanding about the current information security conditions. The results of problem identification and asset determination show that Company XYZ faces complex information security challenges, particularly related to asset management and access control. From the 12 asset categories analyzed, it was found that most assets do not have adequate controls, with only several assets such as Access Control and Alarm System having basic control mechanisms. The findings align with research by Ningrum *et al.* (2024) which emphasizes that physical design weaknesses can contribute to security breaches and potential data compromise [9]. The condition is clearly visible in critical assets such as Physical Security Team PC and IT Team devices that have no controls whatsoever, creating significant security gaps. The password sharing problems found in several assets reflect the lack of information security awareness at the operational level. The situation is consistent with findings by Handri *et al.* (2023) stating that human factors are often the most crucial yet most challenging aspect in security system management [17].

Risk evaluation results show that Access Control System occupies the highest priority with a total risk value of 435 and an average risk level of 54. The finding indicates that the system which should serve as the frontline of physical security actually has the highest vulnerabilities. The discovery is very critical considering that Access Control System functions as the main gateway for facility security. Alarm System and Surveillance System (CCTV) occupy the second and third priorities with relatively high risk values. The condition shows that the company's physical security infrastructure experiences significant degradation, especially related to outdated technology usage and lack of systematic maintenance. Personnel (IT & Security Team) occupies the fourth priority with a risk value of 215, confirming that human factors constitute a substantial risk component. The finding aligns with research by Agustino (2018) which identifies that physical component weaknesses and operational procedure gaps in institutional environments can create entry points that can be exploited for unauthorized access [4].

Vulnerability analysis reveals several systemic issues requiring immediate attention across multiple dimensions. Technology vulnerabilities manifest through the use of outdated technology in Alarm Panel System and several IP Cameras that have exceeded their service life, creating high operational risks. The condition is worsened by unupdated monitoring applications and complex system configurations without adequate documentation. Process vulnerabilities emerge through the absence of formal SOPs for data backup and system maintenance in almost all critical systems, showing fundamental weaknesses in operational governance. The situation is consistent with findings by Fahrurozi *et al.* (2020) which emphasize the importance of risk-based approaches in providing thorough perspectives on information security threats [11]. Human vulnerabilities surface through password sharing practices, weak password usage, and lack of information security awareness, reflecting the need for strengthening security awareness programs. The findings support recommendations by Fahrudin *et al.* (2022) about the importance of employee data risk assessment using structured frameworks [5].

The implementation of ISO/IEC 27005:2018 methodology proves effective in systematically identifying and categorizing risks. The structured approach enables organizations to understand risk landscapes thoroughly and prioritize mitigation actions based on impact and likelihood. The research results support findings by Sinaga and Taan (2024) which show that ISO/IEC 27001:2022 implementation helps organizations in addressing information system security management challenges [10]. The systematic approach used in the research successfully reveals previously unidentified vulnerabilities, aligning with research by Isnaini *et al.* (2023) [7]. The methodology effectiveness demonstrates how structured frameworks can provide organizations with clear pathways for risk identification and management, enabling more informed decision-making processes regarding security investments and resource allocation.

The research findings have significant strategic implications for Company XYZ management across several critical areas. Infrastructure investment becomes essential, requiring substantial investment for physical security system modernization, especially replacement of obsolete devices and backup power system capacity enhancement. Policy development emerges as another priority, with strengthening User Access Control Policy and developing operational SOPs becoming top priorities to reduce human error risks and access abuse. Building a centralized repository for security systems will improve management efficiency and facilitate audit and compliance processes, while implementation of continuous security training programs is needed to increase awareness and change employee behavior regarding information security. These strategic directions require coordinated efforts across multiple organizational levels to ensure effective implementation and sustainable security improvements. The research provides significant value to the body of knowledge in several innovative aspects. Methodology integration demonstrates the effectiveness of combining ISO/IEC 27005:2018 with fishbone diagram analysis for root cause analysis in physical security settings, which has not been extensively explored in previous literature. The specific focus on IT Workshop environments in multinational technology companies provides new perspectives on information security challenges in settings that have not been widely studied. The holistic approach successfully integrates people, technology, and process dimensions in a thorough risk assessment framework, offering a more realistic understanding of how different security factors interact and influence overall organizational security posture.

The research has several limitations that need acknowledgment to properly frame the findings and their applicability. Focus on one company limits the generalizability of findings to other organizational settings and industry sectors. The relatively short observation period may not capture risk variations over time or seasonal patterns that could influence security risk profiles. Dependence on self-reported data from respondents can introduce subjective bias that may affect the accuracy and completeness of risk assessments. For future research, it is recommended to conduct comparative studies on various types of technology companies to enhance generalizability, develop predictive models for information security risk anticipation, and explore the integration of emerging technologies such as AI and IoT in information security risk management frameworks. The research results provide a solid foundation for developing more robust and adaptive information security strategies against the dynamics of security threats in the digital era, offering practical guidance for organizations seeking to enhance their security risk management capabilities while advancing broader understanding of security management in contemporary organizational environments.

5. Conclusion

Based on the comprehensive assessment conducted throughout this study, several significant conclusions emerged regarding the risk landscape affecting the company's critical assets. The evaluation process commenced with a thorough risk identification procedure encompassing 12 primary organizational assets, incorporating the recognition of potential threat vectors, existing control mechanisms currently deployed, inherent vulnerabilities within each asset category, and recommended treatment strategies designed to mitigate or effectively manage identified risks. Following this initial phase, a detailed analysis and systematic evaluation of risk severity levels was undertaken, yielding a structured classification framework: three assets—specifically A5, A6, and A7—demonstrated characteristics consistent with high-risk categorization; an additional three assets, including A4, A9, and A12, exhibited risk profiles aligned with moderate-level classifications; whereas the remaining six assets, encompassing A1, A2, A3, A8, A10, and A11, presented risk characteristics falling within acceptable low-risk parameters. Drawing from these comprehensive evaluation findings, researchers developed a tailored series of strategic recommendations and risk management protocols, each specifically calibrated to address the unique characteristics and corresponding risk thresholds of individual assets, ultimately seeking to enhance the overall protective framework and security posture of the organization's asset portfolio.

References

[1] Naibaho Sulaiman, R. (2017). Peranan dan perencanaan teknologi informasi dalam perusahaan. *Warta Edisi 52*, April, 45. https://doi.org/10.46576/wdw.v0i52.253

[2] Lionel, E., Leonard, L., Fernando, N., Ong, T., & Septama, V. (2023). Analisis manajemen risiko pada malaya cafe. *CEMERLANG: Jurnal Manajemen dan Ekonomi Bisnis*, 3(1), 251–266. https://doi.org/10.55606/cemerlang.v3i1.716

[3] Hikam, M. L. B., Dewi, F., & Praditya, D. (2024). Analisis manajemen risiko informasi menggunakan ISO/IEC 27005:2018 (studi kasus: PT.XYZ). *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, 9(2), 728–734. https://doi.org/10.29100/jipi.v9i2.4709

[4] Agustino, D. (2018). Information security management system analysis menggunakan iso/iec 27001 (studi kasus: stmik stikom bali). *Eksplora Informatika*, 8(1), 1. https://doi.org/10.30864/eksplora.v8i1.130

[5] Fahrudin, N., S, A., & Putra, K. (2022). Penilaian risiko keamanan data karyawan pada sistem informasi dengan menggunakan framework nist sp 800-30 pada pt. abc. *Jurnal Ilmiah Teknologi Infomasi Terapan*, 8(3). https://doi.org/10.33197/jitter.vol8.iss3.2022.900

[6] Handayani, N., Wibowo, H., Sari, D., Satria, Y., & Gifari, A. (2019). Risk assessment of information system of faculty of engineering university diponegoro using failure mode effect and analysis method based on framework iso 27001. *Teknik*, 39(2), 78. https://doi.org/10.14710/teknik.v39i2.15918

[7] Isnaini, K., Sari, G., & Kuncoro, A. (2023). Analisis risiko keamanan informasi menggunakan iso 27005:2019 pada aplikasi sistem pelayanan desa. *Eksplora Informatika*, 13(1), 37-45. https://doi.org/10.30864/eksplora.v13i1.696

[8] Mahardika, K., Wijaya, A., & Cahyono, A. (2019). Manajemen risiko teknologi informasi menggunakan iso 31000: 2018 (studi kasus: cv. xy). *Sebatik*, 23(1), 277-284. https://doi.org/10.46984/sebatik.v23i1.572

[9] Ningrum, F., Riwanto, Y., Pratiwi, I., & Fikri, M. (2024). Analisis keamanan sistem informasi perguruan tinggi berbasis indeks kami. *Jurnal Informatika Polinema*, 10(3). https://doi.org/10.33795/jip.v10i3.5154

[10] Sinaga, R., & Taan, F. (2024). Penerapan iso/iec 27001:2022 dalam tata kelola keamanan sistem informasi: evaluasi proses dan kendala. *Nuansa Informatika*, 18(2), 46-54. https://doi.org/10.25134/ilkom.v18i2.205

[11] Fahrurozi, M., Tarigan, S. A., Tanjung, M. A., & Mutijarsa, K. (2020, October). The use of ISO/IEC 27005: 2018 for strengthening information security management (a case study at data and information center of ministry of defence). In *2020 12th International Conference on Information Technology and Electrical Engineering (ICITEE)* (pp. 86-91). IEEE. https://doi.org/10.1109/ICITEE49829.2020.9271748

[12] Agrawal, V. (2017, June). A framework for the information classification in ISO 27005 standard. In *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)* (pp. 264-269). IEEE. https://doi.org/10.1109/CSCloud.2017.13

[13] Ariyani, S., & Sudarma, M. (2016). Implementation of the ISO/IEC 27005 in risk security analysis of management information system. *Journal of Engineering Research and Applications*, 6(8), 1-6.

[14] Agrawal, V. (2016). Towards the ontology of ISO/IEC 27005: 2011 risk management standard. In *HAISA* (pp. 101-111).

[15] Patiño, S., Solís, E. F., Yoo, S. G., & Arroyo, R. (2018, April). ICT risk management methodology proposal for governmental entities based on ISO/IEC 27005. In *2018 International Conference on eDemocracy & eGovernment (ICEDEG)* (pp. 75-82). IEEE. https://doi.org/10.1109/ICEDEG.2018.8372361

[16] Ariyani, S., & Sudarma, M. (2016). Implementation of the ISO/IEC 27005 in risk security analysis of management information system. *Journal of Engineering Research and Applications*, 6(8), 1-6.

[17] Handri, E. Y., Putro, P. A. W., & Sensuse, D. I. (2023, August). Evaluating the people, process, and technology priorities for NIST cybersecurity framework implementation in e-government. In *2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)* (pp. 82-87). IEEE. https://doi.org/10.1109/ICoCICs58778.2023.10277024

[18] Utami, G. C., Supramaji, A. B., & Isnaini, K. N. (2023). Penilaian risiko keamanan informasi pada website dengan metode DREAD dan ISO 27005:2018. *JUSTINDO (Jurnal Sistem dan Teknologi Informasi Indonesia)*, 8(1), 47–56. https://doi.org/10.32528/justindo.v8i1.219

[19] Syahid, P. P., Saedudin, R. R., & Rahmad, B. (2018). Implementasi dan penilaian risk assessment atas infrastruktur teknologi informasi di pt. xyz menggunakan framework cobit 5. *e-Proceeding of Engineering*, 5(1), 1400–1410. https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/6238

[20] Putri, M. K., & Hakim, A. R. (2021). Perancangan manajemen risiko keamanan informasi layanan jaringan MKP berdasarkan kerangka kerja ISO/IEC 27005:2018 dan NIST SP 800-30 revisi 1. *Info Kripto*, 15(3), 134–141. https://doi.org/10.56706/ik.v15i3.34