Volume 4, No. 7 July 2026
p-ISSN3032-3037| e-ISSN 3031-5786

ADVANCES IN SOCIAL HUMANITIES RESEARCH

Designing User-Centered Risk Management Framework to Enhance Security Posture and Security Control Model in SME

Jahja Mayudin Kurniawan* , M. Amin Soetomo, Charles Lim
Swiss German University, Indonesia
Email: jahja.kurniawan@student.sgu.ac.id* , mohammad.soetomo@sgu.ac.id, charles.lim@sgu.ac.id

Keywords:
Risk Management; ISO/IEC 27001; ISO/IEC 27005; SME; Security Control

Abstract

Small and Medium Enterprises (SMEs) face increasing cybersecurity risks while often having limited resources and low readiness to implement ISO/IEC 27001. This research aims to design a user-centered risk management framework to improve security posture and enhance the effectiveness of security control implementation. The study employs the Design Science Research Methodology (DSRM) by integrating ISO/IEC 27005 as an operational risk management standard and ISO 31000 as strategic guidance, supported by a Multi-Criteria Decision Analysis (MCDA) approach for security control prioritization. The framework was demonstrated through a case study at PT Pulsabayar and evaluated using Focus Group Discussions (FGDs) and expert validation. Risk analysis identified 20 cybersecurity risks, consisting of 9 medium risks and 11 low risks, with the three highest-priority risks being application account takeover, phishing attacks, and malware infections. Security control prioritization generated priority scores ranging from 0.36 to 0.64, enabling systematic resource allocation for risk mitigation. The framework received positive evaluations from internal stakeholders and external experts, confirming its clarity, usability, and alignment with organizational needs. This research concludes that a user-centered and standards-aligned framework can strengthen cybersecurity governance and support SMEs in achieving incremental compliance and sustainable security improvements.

INTRODUCTION

Small and Medium Enterprises (SMEs) constitute a critical pillar of the national economy; however, they face increasingly complex challenges related to information security and cyber risks. The growing dependence on information technology has made SMEs more vulnerable to security incidents, while their available resources, both financial and human expertise, remain relatively limited (Chidukwani et al. 2022; Kezron 2024). Existing risk assessment approaches are often generic and insufficiently consider user contexts, while available audit instruments are frequently difficult for SME practitioners to understand, hindering the effective implementation of risk-based approaches (AL-Dosari et al. 2023; Crovini et al. 2021; Meersman 2019; Moschella et al. 2023). This condition creates a significant gap between the practical needs of SMEs and the compliance requirements established by the ISO/IEC 27001 standard.

ISO/IEC 27001 is an internationally recognized standard for establishing and maintaining an Information Security Management System (ISMS). However, its adoption

among SMEs remains limited, primarily due to the complexity of risk assessment processes, extensive documentation requirements, and audit approaches that are often designed for larger organizations. Compliance with ISO/IEC 27001 is increasingly recognized as an indicator of organizational credibility, providing SMEs with competitive advantages, enhancing stakeholder confidence, and ensuring alignment with information security best practices (Folorunso et al. 2024; Olagbemide 2024; Ramli et al. 2025).

The identified challenges at PT Pulsabayar, the SME selected as the case study, were categorized into four domains: People, Process, Method, and Governance. This research focused specifically on the Process domain, which involved the absence of clearly defined risk assessment and maturity evaluation mechanisms, and the People domain, which involved limited internal understanding of ISO/IEC 27001 concepts. Table 1 presents a summary of the problem analysis across the four identified domains.

Table 1. Problem Analysis of Cybersecurity Challenges in SME (derived from Fishbone Analysis)

Category	Identified Challenges
People	Limited internal understanding of ISO/IEC 27001 concepts; lack of security awareness; insufficient expertise in practical risk assessment execution.
Process	Absence of clearly defined risk assessment process; no maturity evaluation model; security controls not implemented effectively; no systematic security risk prioritization.
Method	Generic and complex risk assessment approaches not tailored to SME context; limited practical risk evaluation tools.
Governance	No single coherent risk management framework to assess risk across all domains; unclear risk prioritization leading to incomplete organizational risk profiles.

Source: Adapted from fishbone analysis conducted during the problem identification phase of DSRM

This research addressed these challenges through three primary objectives: (1) designing a user-centered risk management framework to improve organizational understanding of the risk management process (Grobler et al., 2021; Mirza, 2024); (2) enhancing the effectiveness of security control implementation based on identified risks (Moreira et al., 2025; Taborda Blandon et al., 2026); and (3) establishing a systematic security gap analysis approach to identify, assess, and prioritize gaps between existing practices and applicable security control requirements (Marican et al., 2023; Sukumar et al., 2023). The research was conducted as a single case study at PT Pulsabayar, focusing on framework development rather than full-scale technical security audit implementation.

This research addressed gaps in the risk management literature regarding the application of ISO/IEC 27005 and ISO 31000 within SMEs (Al-Dosari & Fetais, 2023) by advancing theoretical understanding of security control prioritization in resource-constrained environments through the integration of Multi-Criteria Decision Analysis (MCDA) and user-centered design principles (Papathanasiou et al., 2025). Practically, the findings provide actionable insights for SME managers in developing accessible and

standards-aligned risk management processes (Benz & Chatterjee, 2020; Van Haastrecht et al., 2021), while the proposed framework offers structured approaches for risk identification, analysis, and treatment that are adaptable to organizations with limited cybersecurity expertise (Alahmari & Duncan, 2020; Aoudi & Al-Aqrabi, 2025). The prioritization model supports effective resource allocation by focusing on critical risks and security controls, while policymakers can benefit from evidence-based recommendations for developing SME-specific cybersecurity guidance (Chaudhary et al., 2023). Finally, this study provides a foundation for future research by identifying implementation challenges and encouraging longitudinal validation of the framework's impact on security outcomes.

METHOD

Research Design

This research employed the Design Science Research Methodology (DSRM) (Osvaldo & Sordi, 2021), combining qualitative and quantitative methods within a descriptive-evaluative approach. The DSRM process consisted of six phases: (1) problem identification, which analyzed cybersecurity risk management challenges in SMEs; (2) definition of solution objectives, which translated identified problems into framework requirements; (3) design and development, which involved constructing the proposed framework; (4) demonstration, which applied the framework at PT Pulsabayar; (5) evaluation, which assessed framework quality through Focus Group Discussions (FGDs) with internal stakeholders and structured interviews with external cybersecurity experts; and (6) communication, which disseminated the research outcomes.

Primary data were collected through documentation reviews of risk registers, organizational procedures, and asset inventories, supplemented by semi-structured interviews. The FGD was conducted on January 9, 2026, involving the Operational Manager (6 years of experience), an IT representative (5 years of experience), and a General Affairs representative (4 years of experience). External validation involved three certified experts from PT TUV SUD Indonesia, PT Mitra Berdaya Optima, and PT Krakatau Steel, each holding CEH and/or ISO/IEC 27001 certifications and possessing 5–7 years of relevant professional experience.

Proposed Risk Management Framework

The proposed framework adapts ISO/IEC 27005 as the operational backbone for information security risk management, complemented by ISO 31000 for strategic governance, and augmented with MCDA for security control prioritization. The framework comprises six phases: Context Establishment, Risk Identification, Risk Analysis, Risk Evaluation, Risk Treatment, and Evaluation and Validation.

Context Establishment

This phase defines organizational, technical, and environmental parameters for systematic risk assessment. It involves determining the scope (defined as "Biller Aggregator" operations), risk evaluation criteria aligned with organizational values, and relevant internal and external contextual factors. Data is collected through document

reviews and stakeholder interviews to ensure the framework reflects real-world organizational conditions.

Risk Analysis Parameters

Risk analysis employs a quantitative likelihood-impact matrix. Likelihood is assessed on a 5-point scale (Table 4) based on expected event frequency. Impact is assessed on a 5-point scale across four dimensions (Table 5): Financial, Reputation, Legal, and Operational. Risk level is calculated as: Risk Score = Likelihood × Impact. Results are mapped to the risk matrix (Table 6) to classify risks as Low (1–3), Medium (4–12), or High (13–25).

Table 2. Likelihood Scale

Likelihood	Value	Description
Almost Certain (>99.9%)	5	Almost certain to happen in all conditions; has occurred more than 5 times in the past year.
Very Likely (50%)	4	Very possible under current conditions; has occurred 1–5 times in the past year.
Possible (10%)	3	Potential to occur under current conditions; has occurred once in the past 5 years.
Unlikely (1%)	2	Unlikely to occur even without controls; has occurred once in the past 10 years.
Very Unlikely (<0.1%)	1	Only occurs under extraordinary circumstances such as prolonged recession, epidemic, or force majeure; completely unheard of in the past.

Source: Adapted from ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management (ISO, 2018) and NIST SP 800-37 Risk Management Framework (US Department of Commerce, 2018).

Table 3. Impact Scale

Risk Factor	Severe (5)	Significant (4)	Moderate (3)	Minor (2)	Negligible (1)
Financial	Losses/fines > IDR 50 billion	Losses IDR 10–50 billion	Losses IDR 1–10 billion	Losses IDR 50 million–1 billion	Impact < IDR 50 million
Reputation	Company brand no longer trusted by the public	Brand issues requiring legal and PR handling	Issues requiring management clarification	Issues handled by field team	No reputation issue
Legal	Legal problems so severe the company faces bankruptcy	Prolonged legal problems difficult to win	Legal issues resolvable with legal advisor; good winning chance	Issues resolvable through mediation	No potential for lawsuits
Operational	Service disruption > 1 day	Disruption 1–24 hours	Disruption 15 minutes–1 hour	Disruption 1–15 minutes	Disruption < 1 minute

Source: Adapted from ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management (ISO, 2018), NIST SP 800-37 (US Department of Commerce, 2018), and multi-criteria risk assessment frameworks

Table 4. Risk Level Matrix (Likelihood × Impact)

Likelihood \ Impact	5	4	3	2	1
5 (Almost Certain)	25 [H]	20 [H]	15 [H]	10 [M]	5 [M]
4 (Very Likely)	20 [H]	16 [H]	12 [M]	8 [M]	4 [M]
3 (Possible)	15 [H]	12 [M]	9 [M]	6 [M]	3 [L]
2 (Unlikely)	10 [M]	8 [M]	6 [M]	4 [M]	2 [L]
1 (Very Unlikely)	5 [M]	4 [M]	3 [L]	2 [L]	1 [L]

[H] = High Risk (13–25) | [M] = Medium Risk (4–12) | [L] = Low Risk (1–3)

Source: Adapted from ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management (ISO, 2018) and NIST SP 800-37 Risk Management Framework (US Department of Commerce, 2018)

Table 5. Risk Treatment Approach by Risk Level

Risk Level	Risk Treatment
High (13–25)	Mitigation — immediate priority; must be addressed within 3 months; existing systems may continue operating while controls are urgently implemented.
Medium (4–12)	Mitigation — medium priority; security controls to be developed and implemented within 6 months.
Low (1–3)	Accepted — monitored with minimal intervention; no immediate action required.

Source: Adapted from ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management (ISO, 2018), ISO 31000:2018 Risk management — Guidelines (The British Standard Institution, 2018), and multi-criteria risk treatment frameworks (Ganin et al., 2020).

Security Control Prioritization (MCDA)

Security controls are prioritized using MCDA, aggregating four criteria into a single priority score through weighted summation. Based on FGD consensus, the criteria weights are: Employee (42%), Security (31%), Strategic (19%), and Dependency (8%). Each criterion is scored 1–5. The MCDA score formula is: Score = (Employee × 0.42) + (Security × 0.31) + (Strategic × 0.19) + (Dependency × 0.08). Both Risk Score and MCDA Score are normalized using min-max normalization before computing the final Priority Score as their average.

Evaluation and Validation

Framework evaluation was conducted through an internal FGD with PT Pulsabayar stakeholders using a structured questionnaire assessing four criteria: Clarity and

Usability, Comprehensiveness and Relevance, Feasibility and Applicability, and Alignment and Acceptance. External validation involved three certified cybersecurity experts using structured interviews covering the same four criteria, ensuring the framework is methodologically sound and aligned with industry standards.

RESULTS AND DISCUSSION

Context Establishment

PT Pulsabayar operates a Biller Aggregator application with four defined IT security objectives: 100% protection against ransomware, zero personal data breach cases in the application, full compliance with applicable information security regulations, and biannual employee security awareness training. Contextual analysis identified two primary governance challenges: (1) the lack of a clearly defined risk management model, resulting in an incomplete organizational risk profile; and (2) unclear risk prioritization without a unified systematic process, making it difficult to consistently focus limited resources on the most significant cybersecurity risks.

Risk Identification

Asset identification covered 29 physical and logical assets across IT systems, documented in the organizational asset register and presented in Table 8. Risk identification employed a structured three-dimensional methodology: threat identification (natural threats such as power failure, human threats such as malware and unauthorized access, and environmental threats); vulnerability identification across organizational, procedural, personnel, and technical areas; and consequence identification based on CIA (Confidentiality, Integrity, Availability) impacts.

Table 6. Organizational Asset Inventory

Asset Name	Asset No.	Status
Monitor Lenovo	INV.PB.003	Good
Keyboard Logitech	INV.PB.005	Good
CPU Intel	INV.PB.011	Good
CPU I7 RAM 16GB VGA RX550 4GB	INV.PB.012	Good
CPU I7 RAM 16GB VGA RX550 4GB	INV.PB.010	Good
Mouse Logitech	INV.PB.019	Good
CPU Intel	INV.PB.044	Good
CPU Dell	INV.PB.045	Good
CPU Dell	INV.PB.052	Good
CPU I7 RAM 16GB VGA RX550 4GB	INV.PB.071	Good
UPS	INV.PB.058	Good
UPS	INV.PB.059	Good
UPS	INV.PB.060	Good
DVR Hikvision	INV.PB.032	Good
DVR Hikvision	INV.PB.040	Good

Mikrotik 1	INV.PB.063	Good
Mikrotik 2	INV.PB.062	Good
Switch Hub	INV.PB.048	Good
Modem Indihome	INV.PB.049	Good
Modem Backup/GSM	INV.PB.050	Good
MacBook Air 13	INV.PB.083	Good
Monitor TV LG CCTV	INV.PB.034	Good
CPU TV LG	INV.PB.035	Good
Printer Epson	INV.PB.057	Good
Modem	INV.PB.068	Good
CCTV Kvision	INV.PB.025	Good
CCTV Kvision	INV.PB.026	Good
CCTV Kvision	INV.PB.027	Good
Generator Set	INV.PB.046	Good

Source: Compiled from PT Pulsabayar organizational asset register during the Context Establishment phase of the risk management framework

Risk Analysis

Risk analysis was conducted through a structured FGD with the Director and Information Security Coordinator. Each of the 20 identified risks was collaboratively assessed for likelihood and impact using the defined scales. Risk scores were calculated as the product of likelihood and impact values. The complete risk level analysis is presented in Table 7.

Table 7. Risk Level Analysis Results

Risk No.	System Characterization	Threat	Vulnerability	Risk	Impact	Likelihood	Score	Risk Level
1	Software license expired	Cyber attack	System exploitation vulnerability	System down	1	3	3	Low
2	Phishing attack	Cyber attack	Firewall vulnerability; BYOD use; email filter inactive; human error	System down, data loss/damaged	4	2	8	Medium
3	Wrong network configuration	Configuration failure	Network vulnerability	Data exposure	3	2	6	Medium
4	Data inconsistency	Human error; data	Manual data input; no	Data integrity risk;	3	1	3	Low

	: master vs operational	governance gaps	system validation	compliance issues				
5	Malware infection on computer	External attacker; phishing; infected removable media	Outdated OS; antivirus not updated; no USB port control; human error	System downtime; data corrupted; ransomware	3	2	6	Medium
6	IT device stolen	User carelessness; unauthorized intruder	Lack of security awareness	Data breach	3	1	3	Low
7	Data missing during server migration	Data loss; data corruption	No trial run; no rollback plan; tools failure; no data backup	Application downtime; business disruption	3	1	3	Low
8	Data leakages on firewall	External attacker exploiting misconfiguration; APT	Misconfigured firewall rules; lack of encryption in transit	Data breach	4	1	4	Medium
9	Network cable error	Weak configuration control; cable damage	Poor cable management; no redundancy	Network downtime; data transmission failure	3	1	3	Low
10	CCTV error	Recording failure; unauthorized entry	Lack of maintenance; power failure; poor monitoring	Investigation failure; physical security breach	2	2	4	Medium

11	UPS failure	Power interruption; electrical instability	Lack of maintenance; expired UPS batteries	System downtime; data corrupted; business continuity disrupted	3	1	3	Low
12	DVR CCTV cannot save recording	Unauthorized intruder; infrastructure sabotage	Over storage capacity; hardware failure on DVR; poor physical security	Data loss of surveillance; security breach	3	1	3	Low
13	Electricity shutdown	Utility maintenance; power grid outage	No backup power; single power source dependency	System downtime; data loss	3	1	3	Low
14	Unauthorized access to application	Infiltration; unlocked /unprotected devices	No access right review; weak access control	Data breach; application down	3	1	3	Low
15	Takeover of user account on application	Malware; brute force attack; keylogger	Weak password policy; no account lockout; insecure session management	Data breach; application disruption on services	4	3	12	Medium
16	Application bugs	SQL injection; session hijacking	Hacker exploitation; APT; secure coding errors	Data leakage; application down	2	2	4	Medium
17	Network/internet infrastructure error	ISP failure; DDoS attack;	ISP dependency; single point of failure	Operational business	2	1	2	Low

		misconfiguration		downtime				
18	Phishing email	Business email compromise; account takeover	Weak email filtering; no MFA; poor email security policy	Data breach; ransomware	4	1	4	Medium
19	Software Otomax infected by malicious code	Malware attack; insider threat	Endpoint security not updated; no patch management; no network segmentation	Data breach; system downtime	3	1	2	Low
20	Hardware failures (PC, laptop, printer)	Security weakness exploitation	Human error; physical device obsolescence	Data leakages; system downtime	2	2	4	Medium

Source: Compiled from risk assessment conducted through Focus Group Discussion with PT Pulsabayar stakeholders (Director and Information Security Coordinator) during the Risk Analysis phase (PT Pulsabayar FGD, January 2026; ISO/IEC 27005, 2018)

Risk analysis identified 20 risks: 9 classified as Medium Risk and 11 as Low Risk; no High Risk items were found during the assessment period. The highest-scoring risk is account takeover on the application (Risk #15, score: 12), followed by phishing attacks (Risk #2, score: 8), malware infection and wrong network configuration (Risks #5 and #3, score: 6 each).

Risk Evaluation and Prioritization

Risk evaluation prioritized all 20 identified risks based on likelihood-impact scores. PT Pulsabayar adopted two treatment approaches: mitigation for Medium risks and acceptance for Low risks. Medium risks require security controls within a defined timeframe—high-priority items within 3 months, others within 6 months. The top 10 prioritized risks are presented in Table 8.

Table 8. Top 10 Prioritized Risks

No.	Risk No.	System Characterization	Risk	Impact	Likelihood	Risk Score
1	#15	Takeover account user on application	Data breach; application disruption services	4	3	12
2	#2	Phishing attack	System down; data loss/damaged	4	2	8
3	#5	Malware infection on computer	System downtime; data corrupted; ransomware	3	2	6
4	#3	Wrong configuration network	Data exposure	3	2	6
5	#20	Hardware failures (PC, laptop, printer)	Data leakages; system downtime	2	2	4
6	#16	Application bugs	Data leakage; application down	2	2	4
7	#10	CCTV error	Investigation failure; physical security breach	2	2	4
8	#18	Phishing email	Data breach; ransomware	4	1	4
9	#8	Data leakages on firewall	Data breach	4	1	4
10	#1	Software license expired	System down	1	3	3

Source: Compiled from risk evaluation and prioritization results during the Risk Evaluation phase (PT Pulsabayar FGD, January 2026; ISO/IEC 27005, 2018

Risk Treatment and Control Prioritization

Security controls were mapped to ISO/IEC 27001 Annex A controls and prioritized using MCDA across four dimensions: Employee (42%), Security (31%), Strategic (19%), and Dependency (8%). Priority scores represent the normalized weighted combination of risk severity and MCDA scores. The top 10 prioritized security controls are presented in Table 9.

Table 9. Security Control Prioritization

No.	Risk No.	System Characterization	Risk	Treatment	Risk Control (People/Process/Technology)	ISO/IEC 27001 Annex A	Priority Score
1	15	Takeover account user	Data breach; application disruption	Mitigation	People: Password management & security awareness training. Process: IAM policy; user access review. Technology: Encryption, MFA, WAF.	A.6.3, A.5.15, A.5.16, A.8.24	0.64
2	2	Phishing attack	System down; data loss	Mitigation	People: Awareness training & phishing simulation. Process: BYOD procedure; email filtering. Technology: Firewall, IDS/IPS.	A.6.3, A.8.7, A.8.21	0.58
3	5	Malware infection on computer	System downtime; ransomware	Mitigation	People: Security awareness training. Process: SOP patch management; incident response. Technology: Firewall, IDS/IPS.	A.6.3, A.8.7, A.8.21	0.53
4	20	Hardware failures	Data leakages; system downtime	Mitigation	People: Training on correct device use. Process: SOP device maintenance. Technology: Asset management system.	A.6.3, A.7.13, A.5.9	0.55
5	16	Application bugs	Data leakage; application down	Mitigation	People: Secure coding training; role segregation. Process: SDLC; testing & QA. Technology: Testing tools; monitoring & logging.	A.6.3, A.5.3, A.8.25, A.8.29, A.8.15	0.50
6	10	CCTV error	Investigation failure; physical security breach	Mitigation	People: Operator training. Process: Maintenance & recovery procedure. Technology: Backup power; automatic monitoring.	A.7.4, A.7.13, A.8.13	0.48
7	18	Phishing email	Data breach; ransomware	Mitigation	People: Security awareness training. Process: Email security policy; access control review. Technology: MFA, EDR, endpoint protection.	A.6.3, A.5.15, A.8.1, A.8.7	0.48
8	3	Wrong network configuration	Data exposure	Mitigation	People: Staff training. Process: SOP change management. Technology: Automatic configuration validation.	A.6.3, A.8.9, A.8.32	0.43
9	8	Data leakages on firewall	Data breach	Mitigation	People: Role-Based Access; Segregation of Duties. Process: Firewall security policy; change management.	A.5.18, A.5.3, A.8.20, A.8.24	0.36

					Technology: Encryption, MFA, firewall hardening.		
10	1	Software license expired	System down	Accept	People: Security awareness; define roles & responsibility. Process: Periodic software audit. Technology: Asset management tool & license alerts.	A.8.7, A.8.21, A.8.16, A.8.32	0.49

Source: Compiled from security control prioritization using MCDA approach during the Risk Treatment phase (PT Pulsabayar FGD, January 2026; ISO/IEC 27001:2022, ISO/IEC 27005:2018; Ganin et al., 2020)

Evaluation and Validation Results

Internal evaluation through FGD confirmed the framework's effectiveness. All three stakeholder representatives (Operations, IT, and General Affairs) approved formal adoption, with scores consistently ranging 4–5 out of 5 across all criteria. Clarity and Usability ratings confirmed that the framework's processes, terminology, and diagrams are clear and practicable. Comprehensiveness and Relevance scores confirmed that the framework identifies and prioritizes significant operational risks. Feasibility and Applicability received consistent scores of 4, indicating achievability within existing resources and budget. Alignment and Acceptance received 4–5, with all stakeholders approving formal adoption, subject to periodic review and future investment planning for security control tools.

External expert validation by three certified cybersecurity professionals confirmed the methodological soundness of the ISO/IEC 27005 and ISO 31000 integration. The risk matrix was validated as a practical and reliable instrument for assessing the PT Pulsabayar risk register, and risk control prioritization was rated as accurate. Key improvement recommendations included incorporating financial cost data to justify mitigation investments and ensuring a complete compliance audit trail from risk identification through control selection.

CONCLUSION

This research successfully designed, demonstrated, and validated a user-centered risk management framework for PT Pulsabayar, an SME operating as a Biller Aggregator in Indonesia, using the Design Science Research Methodology (DSRM). The framework integrated ISO/IEC 27005 for operational risk management and ISO 31000 for strategic risk governance, complemented by a Multi-Criteria Decision Analysis (MCDA) approach for security control prioritization. A total of 20 cybersecurity risks were identified within the organization’s applications and business operations, consisting of 9 medium risks and 11 low risks. The three highest-priority risks were application account takeover (priority score: 0.64), phishing attacks (0.58), and malware infections on computers (0.53). These risks were mapped to relevant ISO/IEC 27001 Annex A controls and addressed through structured People, Process, and Technology countermeasures. Internal stakeholder evaluations confirmed the framework’s clarity, usability, relevance, feasibility, and

alignment with organizational IT objectives. External expert validation further supported the methodological robustness of integrating ISO/IEC 27005 and ISO 31000, with recommendations to incorporate financial cost modeling to strengthen the objectivity of mitigation prioritization.

It is recommended that PT Pulsabayar formally adopt the proposed framework as part of its Information Security Management System (ISMS), prioritize the implementation of critical controls—including security awareness training, periodic user access reviews, multi-factor authentication, and data encryption—and utilize the risk register as a foundation for resource allocation and cybersecurity investment decisions. Future research should conduct longitudinal studies involving full-scale implementation to measure actual reductions in security incidents, apply quantitative Analytic Hierarchy Process (AHP) weighting with external expert input to improve control prioritization objectivity, and extend the framework's application to other SME service sectors to validate its scalability and generalizability across diverse organizational contexts.

REFERENCES

Al-Dosari, K., & Fetais, N. (2023). Risk-management framework and information-security systems for small and medium enterprises (SMEs): A meta-analysis approach. *Electronics, 12*(17), 3629. https://doi.org/10.3390/electronics12173629

Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 1–5. https://doi.org/10.1109/CyberSA49311.2020.9139638

Aoudi, S., & Al-Aqrabi, H. (2025). Integrating IoT security practices into a risk-based framework for small and medium enterprises (SMEs). *Computer Standards & Interfaces*, Article 104099. https://doi.org/10.1016/j.csi.2025.104099

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons, 63*(4), 531–540. https://doi.org/10.1016/j.bushor.2020.03.010

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2023). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. *Computer Science Review, 50*, Article 100592. https://doi.org/10.1016/j.cosrev.2023.100592

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations. *IEEE Access, 10*, 85701–85719.

Crovini, C., Santoro, G., & Ossola, G. (2021). Rethinking risk management in entrepreneurial SMEs: Towards the integration with the decision-making process. *Management Decision, 59*(5), 1085–1113.

Folorunso, A., Mohammed, V., Wada, I., & Samuel, B. (2024). The impact of ISO security standards on enhancing cybersecurity posture in organizations. *World Journal of Advanced Research and Reviews, 24*(1), 2582–2595.

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis, 40*(1), 183–199.

https://doi.org/10.1111/risa.12891
Grobler, M., Gaire, R., & Nepal, S. (2021). User, usage and usability: Redefining human centric cyber security. *Frontiers in Big Data, 4*, Article 583723. https://doi.org/10.3389/fdata.2021.583723
International Organization for Standardization. (2018). *Information technology—Security techniques—Information security risk management* (ISO 27005:2018).
International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection—Information security management systems—Requirements* (ISO/IEC 27001:2022).
Kezron, I. E. (2024). Enhancing cybersecurity capacity in small and medium enterprises: A framework for workforce development. *Iconic Research and Engineering Journals, 7*(10), 421–428.
Marican, M. N. Y., Razak, S. A., Selamat, A., & Othman, S. H. (2023). Cyber security maturity assessment framework for technology startups: A systematic literature review. *IEEE Access, 11*, 5442–5452. https://doi.org/10.1109/ACCESS.2022.3229766
Meersman, M. W. (2019). *Developing a cloud computing risk assessment instrument for small to medium sized enterprises: A qualitative case study using a Delphi technique* [Doctoral dissertation, Northcentral University].
Mirza, Z. A. (2024). *Protecting small and medium enterprises: A specialized cybersecurity risk assessment framework and tool* [Bachelor's thesis, University of Twente]. Preprints.org. https://doi.org/10.20944/preprints202408.1691.v1
Moreira, F. R., Canedo, E. D., Nunes, R. R., Serrano, A. L. M., Abbas, C. J. B., Pereira Júnior, M. L., & Lopes de Mendonça, F. L. (2025). Cybersecurity risk assessment through analytic hierarchy process: Integrating multicriteria and sensitivity analysis. *Proceedings of the 27th International Conference on Enterprise Information Systems*. SciTePress.
Moschella, J., Boulianne, E., & Magnan, M. (2023). Risk management in small- and medium-sized businesses and how accountants contribute. *Contemporary Accounting Research, 40*(1), 668–703.
Olagbemide, V. A. (2024). *Developing an effective framework for information security compliance management in small and medium-sized enterprises (SMEs)* [Doctoral dissertation, University of Derby].
Osvaldo, J., & Sordi, D. (2021). *Design science research methodology: Theory development from artifacts.*
Papathanasiou, A., Liontos, G., Katsouras, A., Liagkou, V., & Glavas, E. (2025). Cybersecurity guide for SMEs: Protecting small and medium-sized enterprises in the digital era. *Journal of Information Security, 16*(1). https://doi.org/10.4236/jis.2025.161001
Ramli, A., et al. (2025). Strengthening trust and security through ISO 27001 compliance: A conceptual framework for information management. In *2025 IEEE International Conference on Artificial Intelligence in Engineering and Technology (IICAIET)* (pp. 31–36). IEEE.
Sukumar, A., Hannan, A. M., & Vahid, J. (2023). Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors. *Risk Analysis*, 1–17.
Taborda Blandon, G. E., Hurtado Rivera, J. F., Durán Vásquez, J. M., Monsalve Ruiz, M. J., Silva Castillo, M. T., & Vargas Montoya, H. F. (2026). Selecting a

cybersecurity risk analysis methodology for MSMEs using a multi-criteria method (AHP). *Technologies, 14*(4), Article 227. https://doi.org/10.3390/technologies14040227

The British Standards Institution. (2018). *ISO 31000:2018 Risk management—Guidelines*. BSI.

U.S. Department of Commerce. (2018). *NIST Special Publication 800-37 Revision 2: Risk management framework for information systems and organizations*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-37r2

Van Haastrecht, M., Sarhan, I., Shojaifar, A., Baumgartner, L., Mallouli, W., & Spruit, M. (2021). A threat-based cybersecurity risk assessment approach addressing SME needs. *Proceedings of the 16th International Conference on Availability, Reliability and Security*, 1–12. https://doi.org/10.1145/3465481.3469199