SvedbergOpen
DISSEMINATIONOF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

Assessing the Current Status of Information Security Risk Management at Vietnamese Enterprises

Vu Hoang Dat[1], Le Quang Minh[2], Ha Thi Hao[3]

[1] VNU Information Technology Institute, Vietnam National University, Hanoi. E-mail: 26218001@vnu.edu.vn, ORCID: 0000-0003-2389-4564
[2] VNU Information Technology Institute, Vietnam National University, Hanoi. E-mail: quangminh@vnu.edu.vn,
[3] VNU Information Technology Institute, Vietnam National University, Hanoi. E-mail: 26218002@vnu.edu.vn, ORCID: 0009-0002-6578-1357

Abstract
With the growing pace of digital transformation in Vietnam, enterprises are subjected to more and more complex cybersecurity threats that should be managed via the ISRM discipline. Although the internationally accepted norms and standard frameworks such as ISO/IEC 27001:2022, as well as the NIST Cybersecurity Framework (CSF) 2.0 are available, there is no empirical study investigating the status of the ISRM execution of Vietnamese enterprises. This study uses a mixed-method design, mainly based on a structured survey of 120 enterprises from six industry sectors, complemented by semi-structured interviews and an expert Delphi validation procedure. 65.8% of the enterprises are positioned at ISRM Maturity Level 1 or 2 and the overall mean maturity index is 2.51 on a scale from 0 to 5 (SD = 0.86). The Banking & Finance industry has the best maturity level (M = 3.19), whereas Retail (M = 1.56) and Manufacturing (M = 2.14) industries are grouped into the Initial and Developing phases. The lack of qualified staff (M = 4.43, 100% of the respondents rated it High/Very High) and limited resources of budget (M = 4.48) are the most important barriers of adoption, followed by the low awareness of the management (M = 4.24). An ISRM four-phase maturation (Foundation, Structuring, Maturing and Optimizing phases) based ISRM improvement roadmap is developed and validated by experts review. The results offer practical guidance for enterprise security managers, policy makers, and researchers interested in improving cybersecurity governance in Vietnam and similar developing nations.

Keywords: Information Security Risk Management ISO/IEC 27001 Cybersecurity Transformation Enterprise Security Maturity

1. Introduction

The speedy growth of digital transformation in Vietnam has greatly changed the way all kinds of enterprises operate. Given that the National Digital Transformation Program (Decision 749/QD-TTg, 2020) envisions a minimum of 50% of economic activities transferring to digital platforms by 2025, enterprises are weaving cloud computing, IoT ecosystems, and digital payment infrastructures into their core business [1]. While this migration creates huge economic prospects, it also dramatically expands the cyber threat landscape, making organizations targets of more advanced and targeted cyber attacks [2].

Vietnam faced 13,900 cyberattacks on information systems in 2023 according to the National Cyber Security Technology Corporation (NCS), with about 83,000 computers and servers infected by ransomware, a 8.4% increase compared to 2022 [3]. Brazen breaches of banks, healthcare, and e-commerce giants have highlighted systemic weaknesses in enterprise security infrastructure. These are signs of significant concern and call for strong, institutionalized Information Security risk Management (ISrM) across the Vietnamese enterprise ecosystem.

ISRM encompasses the systematic identification, assessment, treatment, and ongoing monitoring of information security risks within an organization [4]. Internationally, two frameworks dominate ISRM implementation: ISO/IEC 27001:2022, which specifies requirements for an Information Security Management System (ISMS), and the NIST Cybersecurity Framework (CSF) 2.0, which provides a flexible, maturity-tiered approach structured around six core functions: Govern, Identify, Protect, Detect, Respond, and Recover [5, 6]. Despite the broad availability and demonstrated effectiveness of these frameworks, their adoption in developing economies such as Vietnam remains constrained by contextual barriers including limited financial resources, shortage of skilled professionals, and organizational culture [7, 8].

Vietnam's regulatory environment for cybersecurity has evolved considerably in recent years. The Law on Cybersecurity (2018), Decree 13/2023/ND-CP on Personal Data Protection, and Circular 09/2020/TT-NHNN on information security in the banking sector collectively establish minimum compliance standards. Nevertheless, a significant gap persists between regulatory mandates and actual organizational practice, particularly among SMEs, which represent over 97% of businesses in Vietnam [9]. Empirical studies examining this gap at the enterprise level are scarce, limiting the ability of policymakers and security practitioners to design evidence-based interventions [10].

This paper explores three interrelated research objectives:(i) to evaluate the current ISRM practice and maturity level in Vietnamese companies from different industry sectors; (ii) to analyze the key obstacles for adopting ISO/IEC 27001 and NIST CSF within Vietnamese companies; (iii) to present and verify a systematic ISRM enhancement road map that is tailored to the unique context of Vietnam. Employing a mixed-methods approach integrating a structured survey (n = 120), semi-structured interviews, and Delphi expert validation, the outcomes of this study are both statistically and theoretically grounded as well as practically meaningful.

There are three main contributions in this work. In terms of theory, it adapts and contextualises a multi-domain ISRM maturity measurement tool based on ISO/IEC 27001 and NIST CSF 2.0 using the Cyber Resilience Review (CRR) approach for application to the context of Vietnamese enterprises. In addition, it results in a holistic cross-sector ISRM maturity assessment for Vietnamese enterprises with quantitative profiling by sector, enterprise size, and certification status. From a practical point of view, it presents a context-sensitive, multi-phased ISRM improvement road map validated by expert review and thus contributes actionable guidance for enterprise security managers, regulators, and international development partners.

The remainder of this paper is structured as follows. Section 2 reviews the relevant literature. Section 3 describes the research methodology. Section 4 presents empirical findings derived from the survey dataset. Section 5 discusses implications and proposes the improvement roadmap. Section 6 concludes with directions for future research.

2. Literature review

2.1 Theoretical foundations of ISRM

Information security risk management is broadly defined as the process of identifying organizational assets, evaluating threats and vulnerabilities, and selecting appropriate treatments to reduce risk to an acceptable level [4, 11]. ISO/IEC 27005:2022 provides a structured process model consisting of risk identification, analysis, evaluation, treatment, and monitoring, while NIST SP 800-37 Rev. 2 frames risk management as a continuous, lifecycle-driven activity aligned with organizational mission and system objectives [12, 13]. Three theoretical perspectives inform ISRM adoption behavior: Institutional Theory, which explains adoption driven by regulatory (coercive), professional (normative), or imitative (mimetic) pressures [14]; the Resource-Based View (RBV), which frames ISRM capabilities as strategic assets generating competitive resilience [15]; and the Technology Acceptance Model (TAM), which addresses individual and organizational readiness for security tools [16]. In the Vietnamese context, coercive institutional pressure, particularly banking sector regulation, appears to play an important role in driving ISRM adoption, while internal capability development remains relatively underdeveloped [10].

2.2 ISRM maturity models

Maturity models provide a structured continuum for evaluating organizational security capabilities. The five-level maturity hierarchy, consisting of Initial (ad hoc), Developing (basic but inconsistent), Defined (standardized and documented), Managed (quantitatively controlled), and Optimizing (continuous improvement embedded), is consistent across major models including CMMI, SSE-CMM, and the CISA Cyber Resilience Review [17]. Empirical studies conducted in developing economies suggest that many organizations remain at the Initial or Developing stages of cybersecurity maturity, while higher maturity levels are more commonly observed among larger and more resource-rich enterprises [18, 19]. Vietnam's digital transformation trajectory, regulatory environment, and enterprise composition suggest a similar profile. Our instrument adapts the maturity taxonomy across five ISRM domains: Governance & Policy; Risk Assessment Process; Technical Controls; Incident Response; and Human Awareness & Training. Recent maturity-assessment work continues to refine this taxonomy for resource-constrained settings: dual-survey approaches that weight expert and organizational input against NIST CSF functions [20], metrics-driven ISO/IEC 27001:2022 compliance models for technology-sector SMEs [21], and NIST CSF 2.0-based maturity models validated on micro and small enterprises in emerging economies [22] all reinforce the relevance of a multi-domain, context-adapted maturity instrument such as the one applied in this study.

2.3 Cybersecurity challenges in Vietnam

Multiple studies identify a consistent set of ISRM challenges in Vietnam's enterprise context. Javaheri et al. [23] categorize cybersecurity threats in digital finance into technical vulnerabilities (malware, ransomware, APTs, supply chain) and organizational failures (insider threats, weak authentication). Nguyen et al. [10] specifically identify Malware Infections and Supply Chain Vulnerabilities as the highest-impact risks in Vietnam's banking sector. At the organizational level, Thanh et al. [7] document low cybersecurity awareness among enterprise managers, absence of dedicated ISRM functions in most organizations, and heavy reliance on reactive, ad hoc technical measures. Budget constraints and human capital deficits are pervasive: Vietnam's National Cyber Security Association estimated a deficit of over 700,000 cybersecurity professionals by 2025 [24]. Regulatory compliance pressures, while increasing through laws such as Decree 13/2023/ND-CP, remain inconsistently enforced across sectors, creating uneven adoption patterns [9, 25].

2.4 Research gaps

Three principal gaps motivate this research. First, no comprehensive cross-sector empirical dataset on ISRM maturity in Vietnamese enterprises currently exists; sector-specific studies concentrate primarily on banking, leaving manufacturing, retail, and healthcare under-examined. Second, existing studies document cybersecurity challenges but rarely apply a multi-domain maturity assessment instrument with validated reliability. Third, practical ISRM improvement roadmaps tailored to Vietnam's resource constraints, regulatory requirements, and digital transformation trajectory are absent from the literature. This study directly addresses all three gaps.

3. Research methodology

3.1 Research design and sampling

This study adopts a sequential mixed-methods design. Phase 1 comprises a structured literature review aimed at identifying relevant theoretical constructs and informing survey instrument development. Phase 2 involves a structured survey administered to 120 enterprises and 20 semi-structured interviews with security managers and CISOs. Phase 3 applies descriptive and inferential statistical analysis using SPSS v.26 on the validated survey dataset. Phase 4 validates the proposed ISRM roadmap through a single-round expert validation review with 15 cybersecurity experts.

The target population comprised enterprises operating in Vietnam across six sectors: Banking & Finance, Information Technology, Manufacturing, Retail & E-Commerce, Healthcare, and Government/Public Sector. A purposive stratified sampling strategy was employed to ensure sector and size representation. Sample size (n = 120) exceeds the recommended minimum for exploratory cross-sectional studies involving multivariate statistical analysis, consistent with Hair et al. [26]. The survey was distributed through professional cybersecurity networks and direct organizational contacts between October and December 2025. Respondents held roles as CISO, IT Manager, Risk/Compliance Officer, or C-Suite, ensuring strategic-level insight into organizational ISRM practices.

The structured literature review was conducted to map existing theoretical frameworks and empirical findings relevant to ISRM maturity, adoption barriers, and cybersecurity governance in developing economies. Searches were performed across four electronic databases Scopus, Web of Science, IEEE Xplore, and Google Scholar covering publications from January 2015 to December 2023. An initial search yielded 312 records. After deduplication (n = 224), records were screened by title and abstract; 87 papers proceeded to full-text review, of which 42 met the inclusion criteria: peer-reviewed articles published in English or Vietnamese, with an empirical or conceptual focus on ISRM or cybersecurity governance at the organizational level. The review was not conducted as a formal systematic review and does not claim the comprehensiveness of a PRISMA-compliant process; its primary purpose was to derive a theoretically grounded construct pool for survey item generation and to situate the present study within the existing literature.

3.2 Instrument development and reliability

The 25-item survey instrument was developed through a three-stage process: (1) item generation from ISO/IEC 27001:2022 Annex A, NIST CSF 2.0 Informative References, and CISA CRR domains [27]; (2) content validity assessment by five cybersecurity practitioners via cognitive interviewing and item refinement; (3) pilot testing with 15 enterprises before main administration. Items were rated on a five-point Likert scale (1 = No process in place; 5 = Optimized and continuously improving), corresponding to the five ISRM maturity levels. ISRM domain scores were computed as the simple mean of their constituent items. Reliability was assessed

using Cronbach's alpha coefficient (α), with α ≥ 0.70 as the acceptability threshold [26]. All five domains and the overall scale met this criterion, with most domains exceeding α = 0.90 (Table 4). The survey instrument used in this study consisted of 25 maturity assessment items, 10 barrier assessment items, and a demographic profile section.

3.3 Semi-structured interviews and expert validation

Twenty semi-structured interviews were conducted between November and December 2025 to complement the quantitative survey data. Participants were selected using purposive criterion sampling: eligibility required a minimum of five years of professional experience in information security, IT management, or compliance, and direct organizational responsibility for ISRM-related decisions. Participants included CISOs (n = 8), IT Directors (n = 6), Risk and Compliance Officers (n = 4), and C-suite executives with a security oversight portfolio (n = 2), drawn from eight enterprises across the Banking & Finance, IT, Manufacturing, and Healthcare sectors. Each interview lasted between 45 and 75 minutes and was conducted via video conference or in person, with the participant's consent to audio recording.

An interview guide was developed based on the five ISRM domains assessed in the survey. Interviews were transcribed verbatim and coded in NVivo 12 following Braun and Clarke's [28] six-phase thematic analysis framework. Two researchers coded independently, with intercoder agreement assessed using Cohen's kappa (κ = 0.81), indicating strong agreement.

The expert validation panel comprised 15 cybersecurity professionals with a minimum of seven years of relevant experience, including ISO 27001 lead auditors, NIST CSF practitioners, CISA-certified analysts, and senior academics in information security. Panelists reviewed the proposed four-phase ISRM improvement roadmap and rated each phase and its component initiatives on two criteria: (i) technical feasibility for Vietnamese enterprises (1 = Not feasible to 5 = Highly feasible), and (ii) strategic priority for maturity advancement (1 = Low priority to 5 = High priority). The consensus threshold was set at 80% agreement (i.e., at least 12 of 15 panelists rating an item ≥ 4 on each criterion). All 14 roadmap initiatives met the consensus threshold; phases achieving unanimous agreement (100%) and those reaching the 80% threshold are detailed in Table 8.

3.4 Data analysis

Descriptive statistics (mean, standard deviation, frequency distributions) were computed for all survey items and domain scores directly from the SPSS dataset. Chi-square tests with Cramér's V effect size were conducted to examine associations between categorical variables (enterprise size, sector, ISO certification status) and ISRM maturity levels. One-way ANOVA was used to compare barrier ratings across enterprise size categories. Thematic analysis of interview transcripts employed NVivo 12, following Braun and Clarke's [28] six-phase framework. All quantitative analyses were conducted in SPSS v.26.

4. Results

4.1 Sample characteristics

Table 1 presents the profile of the 120 participating enterprises. Small enterprises (< 50 employees) constitute the largest group (41.7%), reflecting the SME-dominated composition of Vietnam's economy. The Banking & Finance (21.7%) and IT (20.0%) sectors are the largest individual segments. The most common respondent roles are IT Manager/Director (33.3%) and CISO/Security Manager (28.3%). Only 18.3% of enterprises hold full ISO 27001 certification, and over half (55.8%) are not pursuing certification. Critically, 50.8% of enterprises allocate less than 5% of their IT budget to cybersecurity, indicating a relatively low level of investment in security-related activities.

Table 1. Respondent Profile

Characteristic	Category	n	%
Enterprise Size	Large (>300 employees)	28	23.3%
	Medium (51–300 employees)	42	35.0%
	Small (10–50 employees)	50	41.7%
Industry Sector	Banking & Finance	26	21.7%
	Information Technology	24	20.0%

	Manufacturing	22	18.3%
	Retail & E-Commerce	20	16.7%
	Healthcare	16	13.3%
	Government / Public Sector	12	10.0%
Respondent Role	CISO / Security Manager	34	28.3%
	IT Manager / IT Director	40	33.3%
	Risk / Compliance Officer	28	23.3%
	C-Suite / Senior Management	18	15.0%
ISO 27001 Certified	Yes – Fully Certified	22	18.3%
	In Progress / Partial	31	25.8%
	No – Not Pursuing	67	55.8%
IT Security Budget	< 5% of IT budget	61	50.8%
	5–15% of IT budget	38	31.7%
	> 15% of IT budget	21	17.5%

4.2 ISRM maturity assessment results

Table 2 shows the average ISRM maturity scores by domain and sector. The average ISRM Maturity Index is 2.51 (with a SD of 0.86) over 5.0, in terms of total scores. This suggests that on average a Vietnamese enterprise lies in-between Level 2 (Developing) and Level 3 (Defined). Technical Controls (D3), with a domain mean of (M=2.84), shows a tendency for enterprises to prioritize technical rather than governance and process dimensions, while Human Awareness & Training (D5) has the lowest mean (M=2.32), corroborating the critical human capital shortage found in literature [7, 24]. The Banking & Finance industry outperforms all others in every domain (overall M=3.19), spurred by SBV Circular 09/2020 [29] regulatory compliance urgency, with Government/Public Sector (M=2.65) and Healthcare (M=2.59) but a close second. Unsurprisingly Retail & E-Commerce reports by far the lowest maturity (overall M = 1.56), again reflecting lack of regulatory oversight and severe budget constraints; the disparity between Retail and all other sectors is one of the most striking features of the data, is the largest contrast in the data. One-way ANOVAs Reveals a significant difference in Maturity by Sector within Each of the Five Domains as well as the Composite (all $p < .001$; See ANOVA detail below Table 2).

Table 2. ISRM Maturity Scores by Domain and Sector

ISRM Domain	Banking	IT	Mfg.	Retail	Health	Govt.	Overall
D1. Governance & Policy	3.22	2.84	2.08	1.57	2.71	2.80	2.55
D2. Risk Assessment Process	3.22	2.77	2.13	1.47	2.63	2.58	2.50
D3. Technical Controls	3.56	3.13	2.44	1.86	2.95	2.92	2.84
D4. Incident Response	2.94	2.61	2.05	1.53	2.41	2.46	2.36
D5. Human Awareness & Training	3.03	2.64	1.98	1.38	2.25	2.47	2.32
Overall ISRM Maturity Index	3.19	2.80	2.14	1.56	2.59	2.65	2.51
Maturity Level (mean-based)	Level 3	Level 3*	Level 2	Level 2*	Level 3*	Level 3*	Level 2/3*

*Boundary cases: sector means within 0.1–0.15 points of the Level 2/3 cutoff (2.50) are flagged with an asterisk and should be interpreted with caution given within-sector dispersion (SD ≈ 0.5–0.9). One-way ANOVA on the

composite index by sector: $F(5,114) = 15.26$, $p < .001$, $\eta^2 = 0.40$ a large effect, confirming sector is strongly associated with maturity.

Table 3 details the maturity level distribution across the full sample. The cumulative proportion of enterprises at Level 1 or Level 2 is 65.8% (38 + 41 of 120), underscoring that the majority of Vietnamese enterprises lack standardized, consistently applied ISRM processes. Only 11.7% of enterprises have reached Level 4 or above. Cross-tabulating maturity level against ISO 27001 status confirms that certification status is a strong maturity correlate: 0% of Level 1 enterprises hold full certification, rising to 37.0% at Level 3, 81.8% at Level 4, and 100% at Level 5.

Table 3. ISRM Maturity Level Distribution

Maturity Level	Description	n	%	Predominant Sector(s)	ISO 27001 Certified (%)
Level 1 – Initial	Ad hoc, undocumented, reactive only	38	31.7%	Retail (18), Mfg. (10)	0%
Level 2 – Developing	Basic practices exist; inconsistent across units	41	34.2%	IT (12), Mfg. (11)	0%
Level 3 – Defined	Standardized processes documented; regularly applied	27	22.5%	Banking (8), Healthcare (6)	37.0%
Level 4 – Managed	Quantitative metrics in use; performance tracked	11	9.2%	Banking (6), IT (3)	81.8%
Level 5 – Optimizing	Continuous improvement; threat-driven adaptation	3	2.5%	Banking (2), IT (1)	100%
Total		120	100%	-	-

4.3 Measurement reliability

Table 4 presents Cronbach's alpha reliability statistics for the five ISRM domain scales and the composite 25-item scale, computed directly via SPSS RELIABILITY. All domains substantially exceed the $\alpha = 0.70$ threshold, ranging from 0.856 (Human Awareness & Training, 3 items) to 0.940 (Technical Controls, 7 items). The overall 25-item ISRM scale achieves $\alpha = 0.980$, indicating excellent internal consistency indicating excellent internal consistency and supporting the reliability of the composite maturity index.

Table 4. Reliability Statistics by ISRM Domain

Domain	No. of Items	Cronbach's α	Mean Score	Std. Dev.
D1. Governance & Policy	5	0.919	2.55	0.93
D2. Risk Assessment Process	6	0.928	2.50	0.93
D3. Technical Controls	7	0.940	2.84	0.92
D4. Incident Response	4	0.922	2.36	0.94
D5. Human Awareness & Training	3	0.856	2.32	0.89
Overall ISRM Scale (25 items)	25	0.980	2.51	0.86

4.4 ISRM adoption barriers

Table 5 presents the ten ISRM adoption barriers ranked by mean importance rating, recomputed from SPSS DESCRIPTIVES and FREQUENCIES. Personnel shortage is rated essentially universally critical 100% of respondents rated it High or Very High ($M = 4.43$, $SD = 0.50$) making it, jointly with budget insufficiency ($M = 4.48$, $SD = 0.59$, 95.0% High/Very High), the most pressing constraint on ISRM adoption. Low management awareness ($M = 4.24$) and complexity of international standards ($M = 4.12$, rated High/Very High by 94.2% of

respondents) round out the top four. Resistance to organizational change is the least critical of the ten barriers tested (M = 3.50), and is the only barrier rated High/Very High by just half of respondents (50.0%).

Table 5. ISRM Adoption Barriers, Ranked by Mean (n = 120; Scale 1–5)

Rank	Barrier	Mean	SD	% High/Very High	Sector with highest mean
1	Shortage of qualified cybersecurity personnel	4.43	0.50	100.0%	IT (4.54)
1	Insufficient cybersecurity budget	4.48	0.59	95.0%	Manufacturing (4.64)
3	Low management awareness and commitment	4.24	0.73	84.2%	Manufacturing (4.41)
4	Complexity of international standards (ISO/NIST)	4.12	0.47	94.2%	Manufacturing (4.27)
5	Rapid evolution of cyber threat landscape	4.04	0.56	86.7%	Manufacturing (4.36)
6	Lack of a dedicated ISRM function/team	4.02	0.74	75.0%	Manufacturing (4.23)
7	Absence of national ISRM implementation guidance	3.81	0.57	72.5%	Healthcare (3.88)
8	Inadequate ISRM tools and technology	3.79	0.53	73.3%	Healthcare (3.88)
9	Weak enforcement of cybersecurity regulations	3.66	0.61	63.3%	Manufacturing (3.91)
10	Resistance to organizational change	3.50	0.57	50.0%	Banking/Govt. (3.58)

Note: Rows 1–2 are tied to two decimal places by overall mean across the full sample (4.475 vs. 4.433); insufficient budget is marginally higher and is listed first by convention. "Sector with highest mean" reflects the sector recording the largest mean rating for that specific barrier item, not the sector most affected overall.

Table 6 presents ANOVA results comparing barrier ratings by enterprise size. Statistically significant differences are observed for five of the six barriers tested. The absence of a dedicated ISRM team yields by far the largest F-statistic ($F = 215.40$, $p < .001$), indicating an extremely strong association between organizational structure and ISRM capability considerably stronger than for any other barrier. Low management awareness also shows a very large effect ($F = 102.02$, $p < .001$), with small enterprises reporting it as far more critical ($M = 4.82$) than large enterprises ($M = 3.32$). Budget insufficiency remains highly significant ($F = 53.32$, $p < .001$; small $M = 4.84$ vs. large $M = 3.79$). Complexity of standards shows only a modest, marginally significant difference ($F = 3.59$, $p = .031$).

Table 6. ISRM Barriers by Enterprise Size - ANOVA

Barrier	Large (n=28)	Medium (n=42)	Small (n=50)	F	Sig.
Budget insufficiency	3.79	4.50	4.84	53.32	<.001***
Personnel shortage	4.00	4.38	4.72	27.76	<.001***
Low mgmt. awareness	3.32	4.17	4.82	102.02	<.001***
Standard complexity	3.93	4.12	4.22	3.59	.031*
No dedicated ISRM team	2.96	3.95	4.66	215.40	<.001***
Lack of national guidance	3.54	3.86	3.92	4.58	.012*

Note: *** $p < .001$; * $p < .05$. Scale 1–5 (1 = Not a barrier; 5 = Critical barrier).

4.5 Statistical association tests

Table 7 presents chi-square test results examining associations between key categorical variables and ISRM maturity outcomes. The statistical tests reveal several important patterns in the relationships among the key variables: the strongest associations are now ISO 27001 status × maturity grouping (Cramér's V = 0.575, strong) and budget level × Technical Controls score (V = 0.529, strong), followed by enterprise size × budget allocation (V = 0.522, strong). By contrast, the association between management awareness and the Governance domain score, while still statistically significant (p = .019), is only weak-to-moderate (V = 0.221) far weaker than previously claimed and the association between having a dedicated ISRM team and Incident Response maturity is similarly weak (V = 0.206, p = .038). These results indicate that management awareness is important, but its direct association with the Governance score is only weak to moderate.

Table 7. Chi-Square Association Tests: Key ISRM Predictors × Maturity Outcomes

Variable Pair	χ^2	df	p-value	Cramér's V	Interpretation
ISO 27001 Status × Maturity (Low/Mid/High)	79.25	4	<.001***	0.575	Strong
Budget Level × Technical Controls (tertile)	67.12	4	<.001***	0.529	Strong
Enterprise Size × Budget Allocation	65.29	4	<.001***	0.522	Strong
Industry Sector × ISRM Maturity Level	67.28	20	<.001***	0.374	Moderate
Enterprise Size × ISRM Maturity Level	27.69	8	<.001***	0.340	Moderate
Management Awareness × Governance Score (tertile)	11.75	4	.019*	0.221	Weak–moderate
Dedicated ISRM Team × Incident Response (tertile)	10.16	4	.038*	0.206	Weak

Note: *** p < .001; * p < .05. Cramér's V: < 0.3 = weak; 0.3–0.5 = moderate; > 0.5 = strong association.

5. Discussion and ISRM improvement roadmap

5.1 Interpreting the maturity landscape

The overall ISRM Maturity Index of 2.51 (sitting at the Level 2/Level 3 boundary) situates Vietnamese enterprises below the Level 3 threshold that international benchmarks consider a minimum for effective risk management governance [17]. This result is broadly consistent with studies conducted in developing ASEAN economies, which have reported that many organizations remain at early or intermediate stages of cybersecurity maturity, particularly outside highly regulated sectors [18, 19]. The higher maturity observed in technical controls (D3, M = 2.84) relative to governance (D1, M = 2.55) and human capital dimensions (D5, M = 2.32) reflects a common pattern in technology-oriented security approaches, where organizations tend to prioritize visible and technology-based solutions such as firewalls, endpoint protection, and encryption over governance, process, and people-related aspects of ISRM [11, 23].

The pronounced maturity gap between the Banking & Finance sector (M = 3.19) and the Retail & E-Commerce sector (M = 1.56), a difference of 1.63 points, is attributable to sector-specific regulatory pressure under SBV Circular 09/2020/TT-NHNN [29], which mandates minimum information security controls and annual risk assessments, against the near-absence of equivalent obligations in retail. This finding is consistent with Institutional Theory, which suggests that coercive pressures such as sector-specific regulations can play a significant role in encouraging ISRM adoption [14]. However, even Banking's relatively modest maturity in the Human Awareness domain (M = 3.03) suggests that even regulated sectors have not fully addressed the people dimension of cyber risk.

Although the IT sector achieved a comparatively high maturity score (M = 2.80), it remained below the Banking & Finance sector and, on the strict mean-based threshold used here, sits only marginally inside Level 3. Interview findings suggest that many IT firms prioritize technology deployment and business growth objectives, while governance formalization, risk documentation, and compliance-oriented security management practices are less developed than those observed in highly regulated industries. This finding indicates that technological expertise alone does not necessarily translate into higher ISRM maturity.

The co-leading position of personnel shortage (M = 4.43, rated High/Very High by 100% of respondents) alongside budget insufficiency (M = 4.48) is particularly notable: every single respondent in the sample rated

the shortage of qualified cybersecurity personnel as at least a moderately high barrier, making it, in practical terms, the most universally acknowledged constraint in the dataset even though its mean is fractionally below the budget barrier. This is consistent with the documented national shortfall of qualified cybersecurity professionals [24] and reinforces qualitative interview findings that budget constraints are compounded by difficulties in demonstrating cybersecurity ROI to senior management, and that limited investment and low ISRM maturity are mutually reinforcing challenges.

The recalculated chi-square results in Table 7 also refine the interpretation of organizational drivers of maturity. ISO 27001 certification status shows the strongest categorical association with overall maturity grouping (V = 0.575), confirming that formal certification (or active pursuit of it) remains the single most reliable correlate of advanced ISRM maturity in this sample, ahead of enterprise size or sector membership taken individually. By contrast, management awareness and the presence of a dedicated ISRM team while clearly important on the barrier-rating scales in Tables 5 and 6 show only weak-to-moderate categorical associations with specific domain scores (Governance and Incident Response, respectively), suggesting that the relationship between these organizational factors and maturity outcomes is more diffuse across multiple domains than a single cross-tabulation can capture.

5.2 Proposed ISRM improvement roadmap

Based on the empirical findings and validated through the expert panel review, this study proposes a four-phase ISRM improvement roadmap structured around the maturity transition pathways identified in the survey data. The roadmap is designed to be modular and scalable, accommodating the diverse resource environments of enterprises from SMEs to large organizations. Expert panel review (n = 15; consensus threshold ≥ 80%) confirmed the feasibility and strategic priority of all four phases and their component initiatives. Unanimous agreement (100%) was recorded for Phase 1 (Foundation) as the prerequisite phase; 86.7% consensus was reached on the sequencing of Phases 2–4. All 14 roadmap initiatives met or exceeded the consensus threshold on both feasibility and priority criteria.

Table 8. Four-Phase ISRM Improvement Roadmap for Vietnamese Enterprises

Phase	Timeline	Key Actions	Target Level
Phase 1: Foundation	Year 1 (0–12 mo.)	Appoint ISRM champion; ISO 27001 gap analysis; launch all-staff security awareness program; implement MFA and endpoint protection	Level 2
Phase 2: Structuring	Year 2 (12–24 mo.)	Adopt NIST CSF as primary framework; document risk assessment methodology and risk register; establish Security Operations function; conduct tabletop exercises	Level 3
Phase 3: Maturing	Year 3 (24–36 mo.)	Implement SIEM/SOC capabilities; pursue ISO 27001 certification; integrate third-party risk assessments; develop KRIs and security dashboards	Level 3–4
Phase 4: Optimizing	Year 4 (36+ mo.)	Deploy AI-assisted threat detection; participate in national threat-intelligence sharing; conduct red-team exercises; review ISMS annually	Level 4–5

Phase 1 (Foundation, Year 1) targets enterprises at Level 1–2 the 65.8% majority identified in Table 3 and prioritizes regulatory compliance baseline establishment, appointment of an ISRM champion, and launch of an enterprise-wide security awareness program, directly addressing the two highest-rated barriers (personnel shortage and budget insufficiency) by lowering the resourcing bar for a first concrete step. Phase 2 (Structuring, Year 2) targets the transition from Level 2 to Level 3 through adoption of the NIST CSF as the primary risk management framework, reflecting expert panel consensus that the CSF's non-prescriptive, maturity-tiered structure is more accessible for enterprises without prior ISRM experience than an immediate ISO 27001 push, while serving as an effective bridge to eventual certification a pathway supported by the strong empirical association between certification status and maturity (Table 7, V = 0.575). Phase 3 (Maturing, Year 3) introduces continuous monitoring capabilities and the pursuit of ISO 27001 certification. Phase 4 (Optimizing, Year 4) targets Level 4–5 enterprises, the 11.7% of the sample already at the leading edge, and focuses on advanced threat detection and national threat-intelligence participation.

5.3 Implications for policy and practice

For enterprise security managers, the maturity assessment results emphasize the need to balance investments in technical controls with corresponding investments in governance structures, risk assessment processes, and security awareness programs, as these are the domains where the largest maturity gaps were observed. For policymakers, the strong association between ISO 27001 status and maturity, together with the much wider-than-expected Banking–Retail gap, suggests that extending sector-specific information security obligations beyond banking to retail, manufacturing, and healthcare could meaningfully accelerate national ISRM maturity. The proposed roadmap provides a practical template that regulatory bodies can incorporate into sector-specific ISRM guidance documents, reducing the complexity barrier (M = 4.12, 94.2% rating it High/Very High) that currently deters SME adoption.

For international standards bodies and development partners, the study highlights that direct transplantation of ISO 27001 or NIST CSF requirements without contextual adaptation to Vietnam's resource environment, regulatory context, and organizational culture is unlikely to succeed at scale. Localized implementation guidance, translated resources, and subsidized certification pathways merit consideration by Vietnamese authorities and international partners.

6. Conclusion

This study provides a cross-sector empirical assessment of ISRM maturity at Vietnamese enterprises, examining 120 organizations across six industry sectors through a validated mixed-methods research design, with all quantitative figures were obtained directly from the SPSS survey output. The principal findings are: (i) the majority of Vietnamese enterprises (65.8%) operate at ISRM Maturity Level 1 or 2, indicating predominantly reactive, unstandardized security risk management practices; (ii) the Banking & Finance sector demonstrates substantially higher maturity (M = 3.19) than Retail & E-Commerce (M = 1.56) and Manufacturing (M = 2.14), a gap considerably wider than earlier estimated, driven by sector-specific regulatory requirements; (iii) personnel shortage (rated High/Very High by 100% of respondents) and budget insufficiency are the two most critical adoption barriers, with management awareness and standards complexity close behind, and pronounced disparities by enterprise size; (iv) ISO 27001 certification status is the strongest categorical correlate of overall maturity (Cramér's V = 0.575), more so than enterprise size or sector; and (v) the proposed four-phase ISRM improvement roadmap provides a validated, context-sensitive framework for enterprise maturity advancement.

The theoretical contributions of this study include a validated multi-domain ISRM maturity instrument adapted for developing-economy contexts, and an empirically grounded application of Institutional Theory and the Resource-Based View to explain ISRM adoption patterns in Vietnam. Practically, the study offers enterprise security managers a sector-benchmarked maturity baseline and a phased improvement roadmap validated by domain experts.

Several limitations should be acknowledged. The sample (n = 120) is drawn primarily from enterprises with some degree of IT security awareness, potentially overstating maturity levels relative to the broader enterprise population. The cross-sectional design precludes causal inference; longitudinal studies tracking maturity progression over time would strengthen future findings. The comparative analysis was limited to descriptive cross-tabulations and ANOVA; future research should apply structural equation modeling to test theorized relationships among contextual factors, adoption determinants, and maturity outcomes. Additionally, extending the survey to a larger and more geographically diverse sample of Vietnamese enterprises, spanning additional provinces and economic regions beyond the six sectors examined here, would enhance the generalizability of the findings and support the development of a nationally representative ISRM maturity benchmark for Vietnam.

References

[1] Vietnamese Government, National Digital Transformation Program to 2025, with Orientations to 2030, Decision No. 749/QD-TTg, Hanoi, 2020.

[2] U. Tariq, I. Ahmed, A.K. Bashir, K. Shaukat, A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review, Sensors 23 (2023).

[3] VTV, "13,900 cyberattacks targeting information systems in Vietnam in 2023, VTV.vn, Dec. 12, 2023. https://vtv.vn/cong-nghe/13900-vu-tan-cong-an-ninh-mang-nham-vao-cac-he-thong-tai-viet-nam-trong-nam-2023-2023121218065446.htm.

[4] ISO/IEC, Information Security Risk Management, ISO/IEC 27005:2022, International Organization for Standardization, Geneva, 2022.

[5] ISO/IEC, Information Security Requirements, ISO/IEC 27001:2022, International Organization for Standardization, Geneva, 2022.
[6] NIST, The NIST Cybersecurity Framework 2.0, National Institute of Standards and Technology, Gaithersburg, MD, 2024.
[7] N.T.P. Thanh, T.H. Le, H. Van Thuc, D.T.N. Huy, Cyber Attacks and Security System Design Solutions in Emerging Markets and Vietnam, Lecture Notes in Networks and Systems 356 (2022) 521–528.
[8] General Statistics Office of Vietnam (GSO), Results of the 2021 Enterprise Census, Statistical Publishing House, Hanoi, 2022.
[9] N.N. Thach, H.T. Hanh, D.T.N. Huy, Technology Quality Management of Industry 4.0 and Cybersecurity Risk Management on Current Banking Activities in Emerging Markets: The Case of Vietnam, International Journal for Quality Research 15 (2021) 845–856.
[10] P.-H. Nguyen, T.-V. Pham, L.-A.T. Nguyen, H.-A.T. Pham, T.-H.T. Nguyen, T.-G. Vu, Assessing Cybersecurity Risks and Prioritizing Top Strategies in Vietnam's Finance and Banking System Using Strategic Decision-Making Models-Based Neutrosophic Sets and Z Number, Heliyon 10 (2024) e37893.
[11] W.S. Admass, Y.Y. Munaye, A.A. Diro, Cyber Security: State of the Art, Challenges and Future Directions, Cyber Security and Applications 2 (2024) 100031.
[12] NIST, Risk Management Framework for Information Systems and Organizations, NIST SP 800-37 Rev. 2, NIST, Gaithersburg, MD, 2018.
[13] A. Zadeh, B. Lavine, H. Zolbanin, D. Hopkins, A Cybersecurity Risk Quantification and Classification Framework for Informed Risk Mitigation Decisions, Decision Analytics Journal 9 (2023).
[14] P.J. DiMaggio, W.W. Powell, The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields, American Sociological Review 48 (1983) 147–160.
[15] J. Barney, Firm Resources and Sustained Competitive Advantage, Journal of Management 17 (1991) 99–120.
[16] F.D. Davis, Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology, MIS Quarterly 13 (1989) 319–340.
[17] Cyber Sierra, "NIST CSF Maturity Levels Explained (Model, Stages, Importance)," Cybersierra.co, Oct. 25, 2024. https://cybersierra.co/blog/nist-csf-maturity-levels-everything-you-need-to-know/.
[18] I. Ahmed, N.U.I. Hossain, S.A. Fazio, M. Lezzi, A Decision Support Model for Assessing and Prioritization of Industry 5.0 Cybersecurity Challenges, Sustainable Manufacturing and Service Economics 3 (2024) 100018.
[19] O. Shulha, I. Yanenkova, M. Kuzub, I. Muda, V. Nazarenko, Banking Information Resource Cybersecurity System Modeling, Journal of Open Innovation: Technology, Market, and Complexity 8 (2022).
[20] L. Bernardo, S. Malta, J. Magalhães, An Evaluation Framework for Cybersecurity Maturity Aligned with the NIST CSF, Electronics 14 (2025) Art. no. 1364.
[21] G. Quispe-Kobashikawa, C. Zuloaga-Estrada, P. Castaneda, J. Mansilla-Lopez, A.D. Garcia-Nunez, Enhancing Information Security in Technology Small and Medium-Sized Enterprises: A Metrics-Driven Model Based on ISO/IEC 27001:2022, Engineering, Technology & Applied Science Research 16 (2026) 34316-34326.
[22] L. Biggi, J. Rioja, P. Castaneda, J. Mansilla-Lopez, A.D. Garcia-Nunez, Development and Validation of a Cybersecurity Model for Ransomware Mitigation Based on NIST CSF 2.0: The Case Study of a Peruvian Micro-Small Enterprise, Engineering, Technology & Applied Science Research 15 (2025) 30015-30025.
[23] D. Javaheri, M. Fahmideh, H. Chizari, P. Lalbakhsh, J. Hur, Cybersecurity Threats in FinTech: A Systematic Review, Expert Systems with Applications 241 (2024) 122697.
[24] Dan Tri, "Solving the shortage of over 700,000 cybersecurity personnel in Vietnam, Dantri.com.vn, Apr. 11, 2025. https://dantri.com.vn/cong-nghe/giai-bai-toan-thieu-hut-700000-nhan-luc-an-ninh-mang-viet-nam-20250411133821985.htm.
[25] C.T. Phan, T.H. Phan, N.Q.A. Huynh, Cyber Security Risks in Digital Banking Activities: Vietnam Case, Information and Communications Publishing House, Hanoi, 2021.
[26] J.F. Hair, W.C. Black, B.J. Babin, R.E. Anderson, Multivariate Data Analysis, 8th ed., Cengage, 2019.
[27] CISA, Cyber Resilience Review (CRR) Method Description and Self-Assessment User Guide, Cybersecurity and Infrastructure Security Agency, 2020.
[28] V. Braun, V. Clarke, Using Thematic Analysis in Psychology, Qualitative Research in Psychology 3(2) (2006) 77–101.
[29] State Bank of Vietnam, Circular No. 09/2020/TT-NHNN on Information Security Regulation in Banking Operations, Hanoi, 2020.