International Journal of Safety and Security Engineering
Vol. 15, No. 12, December, 2025, pp. 2603-2611
Journal homepage: http://iieta.org/journals/ijsse

Cyber Security Risk Management in the Indonesian Capital Market

Slamet Aji Pamungkas[1*], Widowati[2], Aris Sugiharto[2], Muhammad Hilmi Amanullah[3]

[1] Doctoral Program of Sciences and Mathematics, Faculty of Sciences and Mathematics, Diponegoro University, Semarang 50275, Indonesia
[2] Department of Mathematics, Faculty of Sciences and Mathematics, Diponegoro University, Semarang 50275, Indonesia
[3] Bureau of Law and Public Communication, National Cyber and Crypto Agency, Depok 16516, Indonesia

Corresponding Author Email: mamung0618@gmail.com

https://doi.org/10.18280/ijsse.151216

Received: 15 October 2025
Revised: 15 December 2025
Accepted: 23 December 2025
Available online: 31 December 2025

Keywords:
digital transformation, Indonesian capital market, cyber risk management, financial sector, critical information infrastructure

ABSTRACT

The digital transformation of the Indonesian capital market is transforming a rigid system into an inclusive, data-driven ecosystem, increasing efficiency, transparency, and accessibility through online platforms, smartphone applications, and crowdfunding. Digital capital markets offer ease of investment, but they also open up significant opportunities for cyber risks such as data theft, phishing, and ransomware, which target the weakest vulnerabilities in customers and securities company systems. While businesses have significant financial incentives to accept digital transactions, it is important to understand the key security risks associated with them and implement appropriate protocols to mitigate them. This can facilitate the utilization of digital capital market instruments while ensuring the continuity of secure long-term relationships. This research aims to develop an Integrated Risk Management Framework for the Indonesian Capital Market (IRMCM) as a tool for identifying and prioritizing top cyber risks in the IRMCM. The IRMCM framework combines two key components of risk analysis: likelihood and impact. By combining this two-dimensional approach, the IRMCM provides a clear and focused representation of cyber risk priorities at the sectoral level. The resulting risk priorities can help stakeholders gain a comprehensive understanding of the cyber risk landscape, enabling them to make more informed and effective decisions. More broadly, cyber risk identification will produce a list of top cybersecurity risks and their recommendations at the financial sector level, specifically in the case study of the IRMCM sector. Thus, this research is expected to provide strategic contributions, both for the government and for the IRMCM ecosystem, to improve cyber resilience and enhance the stability of the digital economy in Indonesia. The research results are the IRMCM as an Instrument for Measuring Cybersecurity Risk in the Financial Sector, and the results of its implementation in the IRMCM ecosystem.

1. INTRODUCTION

Digitization in the Indonesian capital market supports the government's goal of a stronger digital economy. Bank Indonesia regulates to ensure fintech innovations are secure, efficient, and inclusive. Rapid digitalization has made capital markets more convenient, offering faster, safer, and more efficient transactions. Cyber threats in the financial sector, including the capital market, are evolving quickly and becoming more sophisticated. While digitalization brings increased investor access, efficiency, transparency, and new products, it also creates new vulnerabilities. Investors can now transact from anywhere using mobile apps, speeding up transactions and compliance. However, alongside these benefits, digitalization also introduces new and increasingly sophisticated cyber threats that pose significant risks to the financial sector, including the capital market.

Despite the accelerated adoption of digital technologies in the Indonesian capital market, cyber risk management practices remain fragmented and insufficiently integrated at the sectoral level. Existing approaches tend to address cyber risks in isolation or at the organizational level, without providing a structured mechanism to identify, prioritize, and respond to the most critical cyber risks across the capital market ecosystem. This limitation reduces the ability of regulators and market participants to develop coordinated, risk-based strategies that effectively enhance cyber resilience.

Furthermore, most existing cyber risk management frameworks are adapted from global financial markets and are not specifically designed to reflect the regulatory environment, institutional structure, and digital maturity of the Indonesian capital market. These frameworks generally (1) lack a sector-level perspective for consolidating and prioritizing cyber risks, (2) do not provide practical instruments for translating risk identification into implementation, monitoring, and reporting, and (3) offer limited guidance on aligning cyber risk priorities with Indonesia's national digital economy objectives. This creates a clear gap between theoretical cyber risk frameworks

and their practical applicability in the Indonesian capital market context.

The Integrated Risk Management Framework for the Indonesian Capital Market (IRMCM) was developed to identify the top cyber risk profiles at the sectoral level, such as the financial sector. Using the IRMCM sector as a case study, this paper can serve as a guideline for prioritizing the top cyber risks within a sector, providing guidance on developing instruments to facilitate their implementation, and providing guidance on compiling reports and recommendations for preventing and addressing identified cyber risks. Through this series of approaches, the IRMCM framework can be used as a strategic tool through the description of top cyber risks and the resulting recommendations. Stakeholders, such as the government and businesses, can increase their attention to cyber risks in their sectors, thereby enhancing cyber resilience and the stability of Indonesia's digital economy.

This research aims to develop the IRMCM framework as a tool for identifying and prioritizing top cyber risks within the IRMCM ecosystem. The IRMCM framework combines two key components of risk analysis: likelihood and impact. By combining this two-dimensional approach, the IRMCM provides a clear and focused representation of cyber risk priorities at the sectoral level. The resulting risk priorities can help stakeholders gain a comprehensive understanding of the cyber risk landscape, enabling them to make more informed and effective decisions.

More broadly, the cyber risk identification will produce a list of top cybersecurity risks and their recommendations at the financial sector level, specifically in the case study of the IRMCM sector. Therefore, this research is expected to make strategic contributions to both the government and the IRMCM ecosystem, thereby enhancing cyber resilience and stability in the country's digital economy. The research results include the Integrated Risk Management Development Framework for the IRMCM as a Cybersecurity Risk Measurement Instrument for the Financial Sector, and its implementation within the IRMCM ecosystem.

This study makes the following contributions:

• Sector-level cyber risk integration: Proposes an integrated framework to identify and prioritize cyber risks at the capital market sector level, moving beyond organization-centric approaches.

• Actionable instrument: Develops a practical tool that connects cyber risk identification with implementation, monitoring, and reporting for regulatory and industry use.

• Contextual relevance: Aligns cyber risk management with Indonesia’s regulatory environment, institutional structure, and digital maturity to support national digital economy objectives.

2. REVIEW OF LITERATURE

2.1 Risk management

Risk management, as a step to mitigate incidents and provide alternative solutions, is crucial for increasing efficiency and effectiveness in performance, as well as improving public services [1]. Therefore, our study of risk management aims to mitigate potential incidents that could lead to losses, as well as the steps that must be taken to address these issues. Risk management is all processes undertaken solely to minimize or even prevent company risks. It encompasses identification, planning, strategy, action, monitoring, and evaluation of potential negative outcomes. Risk management requires careful consideration of both internal and external factors [2]. Risk management is a theory that must be applied in building a business. Without proper management, entrepreneurs cannot detect potential adverse events. Ironically, companies can experience decline or collapse without knowing the cause. Beyond its theoretical foundation, risk management functions as a systematic mechanism for anticipating uncertainty and preventing organizational decline caused by unidentified or unmanaged risks.

Risk management has specific components that distinguish it from other business management systems. These instruments must be present within management to ensure optimal implementation. The effectiveness of risk management depends on the presence of clearly defined components, governance structures, and decision-making instruments that enable consistent implementation across organizational units.

ISO 31000 provides a universal framework for risk management applicable across industries, including financial services [3]. It emphasizes a principles-based approach, focusing on risk identification, assessment, treatment, and monitoring within an organization's context. Unlike NIST, ISO 31000 is not prescriptive, allowing flexibility in implementation. This adaptability makes it suitable for diverse organizational structures and risk environments, including the heterogeneous landscape of Indonesian financial systems, which range from large banks to fintech startups. For the IRMCM, ISO 31000's flexibility is a key advantage, enabling organizations to tailor risk management processes to local regulatory requirements and cultural nuances. Its emphasis on stakeholder involvement aligns well with Indonesia's collaborative regulatory approach, where coordination between Bank Indonesia, OJK, and private entities is critical. However, ISO 31000's lack of specific cybersecurity guidance may require supplementation with other standards, such as ISO 27001, to address the growing threat of cyber-attacks in digital financial systems.

The IRMCM operates in a dynamic environment characterized by rapid digital adoption, diverse market players, and unique regulatory requirements. Both NIST and ISO frameworks offer valuable insights but require customization to address Indonesia-specific challenges, such as limited cybersecurity infrastructure in rural areas, varying levels of financial literacy, and compliance with local regulations. ISO 31000 offers critical flexibility as integration of both frameworks can enhance risk management effectiveness, ensure resilience, and compliance in Indonesia's rapidly evolving financial sector. This condition underscores the importance of an integrated risk management approach that combines general risk management principles with cybersecurity frameworks to enhance resilience, effectiveness, and regulatory compliance in Indonesia’s rapidly evolving capital market.

2.2 Indonesian capital market

According to the Indonesia Stock Exchange (IDX), the capital market is a market for various long-term, tradable financial instruments, including debt securities (bonds), equities (shares), mutual funds, derivative instruments, and other instruments. The capital market serves as a funding

source for companies and other institutions (e.g., the government) and serves as a platform for investment activities [4]. Thus, the capital market facilitates various means and infrastructure for buying and selling, and other related activities. The Indonesian capital market plays a crucial role in the national economy. By offering investment instruments such as stocks, bonds, and mutual funds, it enables investors to support company and infrastructure development while granting companies access to essential expansion capital.

The President Director of the IDX, Iman Rachman, acknowledged that the performance of the Indonesian capital market has improved with the implementation of digital technology innovations. This progress is expected to further enhance the transparency of investor fund management by listed companies. Digitization also increases transparency and the availability of information for investor decision-making. Furthermore, digitalization increases the efficiency and speed of transactions and provides broader access to investment information and education. This helps attract more investors, especially the younger generation, and ultimately supports corporate funding and national economic growth. However, there are challenges to overcome, including digital transaction data security issues, the rapid pace of technological development that demands regulatory adaptation, the need for improved public literacy, limited access to technology in some regions, and competition with conventional capital markets. These challenges indicate that the digital transformation of the Indonesian capital market introduces not only operational efficiencies but also increased exposure to systemic and cyber-related risks. As digital platforms become integral to capital market operations, effective risk management becomes a critical requirement to maintain market integrity, investor confidence, and operational continuity.

2.3 Cyber security regulations in Indonesia

According to Presidential Regulation of the Republic of Indonesia No. 82 of 2022 on the Protection of Critical Information Infrastructure (CII PR), cybersecurity is defined as an adaptive and innovative effort to protect all layers of cyberspace—including the information assets contained therein—from cyber threats and attacks, both technical and social in nature [5]. The regulatory framework that supports the implementation of cybersecurity in Indonesia, as part of the government's efforts to enhance cybersecurity across various sectors, includes the following: Electronic Information and Transactions (EIT) Law and its amendments, Law No. 11 of 2008, Law No. 19 of 2016, and Law No. 1 of 2024; Law No. 27 of 2022 on Personal Data Protection (PDP Law); Government Regulation No. 71 of 2019 on the Operation of Electronic Systems and Transactions; Government Regulation No. 80 of 2019 on Electronic-Based Trading; Presidential Regulation No. 82 of 2022 on the Protection of Critical Information Infrastructure; Presidential Regulation No. 47 of 2023 on the National Cybersecurity Strategy and Cyber Crisis Management; BSSN Regulation No. 8 of 2020 on Security Systems for Electronic System Operators (PSE); and BSSN Regulation No. 1 of 2024 on Cyber Incident Management. Collectively, these regulations form Indonesia's national cybersecurity governance framework, defining obligations for data protection, electronic system security, critical infrastructure protection, and incident response across sectors, including the financial and capital markets.

One of the key references for the before mentioned cybersecurity regulations is the NIST Cybersecurity Framework 2.0. NIST identifies six core functions to enhance cybersecurity implementation: Govern, Identify, Protect, Detect, Respond, and Recover [6]. These functions establish a structured, lifecycle-based approach to cybersecurity, emphasizing governance, risk management, and informed decision-making rather than focusing solely on technical controls. Furthermore, in the context of cyber risk management, the regulatory framework frequently refers to various international standards such as ISO 31000:2018 – Risk Management Guidelines; ISO/IEC 27005 on Information Security Risk Management, Cybersecurity, and Privacy Protection; NIST SP800-30 Guide for Conducting Risk Assessments; CRAMM (The Central Risk Analysis and Management Method); and other frameworks such as OCTAVE, COSO, and COBIT 5 for Risk. These standards collectively reflect a multi-layered approach to cybersecurity risk management, combining enterprise risk management principles, technical risk assessment methodologies, and governance-oriented control frameworks. However, the coexistence of multiple frameworks and standards may lead to fragmented implementation, as organizations often adopt them selectively without a unified integration model tailored to sector-specific characteristics. In the context of the Indonesian capital market, where regulatory compliance, digital infrastructure, and cybersecurity risks intersect, this regulatory landscape underscores the need for an integrated approach that aligns national regulations with international standards while supporting consistent and effective cyber risk management practices.

2.4 Cyber security risk in the capital market

Research findings have emphasized the need to enhance cybersecurity measures to mitigate cyber threat risks in the financial sector [7, 8]. The correlation between post-cyber threat costs and the net profit of financial institutions illustrates the urgency of protecting this sector. Using descriptive analysis tools, the study summarizes variables such as post-cybercrime costs, net profit of the banking industry, and financial sector performance (as a percentage of GDP). Correlation analysis establishes the relationship and significance between post-attack costs and industry performance. Data was collected from secondary sources, including Statista and the U.S. Bureau of Economic Analysis, covering the period from 2007 to 2022. A negative correlation was found between rising annual costs due to cyberattacks and declining financial sector performance, highlighting the potentially detrimental effects of cybercrime. This highlights the necessity for robust cybersecurity measures in the financial sector. While this stream of research effectively captures the macro-level financial impacts of cybersecurity incidents, it remains largely outcome-oriented and offers limited insight into structured risk management frameworks for proactive prevention and mitigation.

A literature review [3] on topics such as cybersecurity risks and safeguards in the banking sector presents best practices in implementing cybersecurity risk management. It explores methodologies tailored for the banking industry, including quantitative risk assessments, threat modelling, and scenario analysis. Best practices emphasize the proactive integration of threat intelligence, continuous monitoring, and incident response planning. Advanced technologies, such as artificial intelligence and machine learning, are noted for improving the

efficiency of risk assessment. Human factors also play a crucial role in cybersecurity, underscoring the importance of training and awareness programs in mitigating risks associated with human error and social engineering attacks. Although this body of work effectively addresses technical and operational controls at the organizational level, it remains largely domain-specific and provides limited integration with broader governance structures and sector-wide risk management perspectives.

A study on the risk management of the Indonesian Ministry of Finance's application system, known as Agency Level Financial Application System (SAKTI) [9, 10], revealed that the system lacked mechanisms to ensure service availability. The risk management framework developed for SAKTI identified 25 risk scenarios and designated responsible parties for mitigation. The process involved establishing context, assessing risk using ISO 27005 and NIST standards, treating risk, and accepting risk. The resulting framework serves as a mitigation guide in case of disruptions, ensuring data availability for operational continuity. While this study demonstrates the practical application of international standards within a specific organizational setting, its scope is confined to a single system and does not address sector-level integration or comparative cyber risk profiling across financial market participants.

Rahman et al. [11] identified attributes of cybercrime in Bangladesh's banking sector and examined the role of board oversight in cybersecurity. The empirical analysis was based on a comprehensive survey involving board members of ten commercial banks. Researchers identified probable cyber risks and sources, applied Enterprise Risk Management tools, and assessed the impact and likelihood of cybercrime over time. The study found that active board involvement is essential in reducing cybersecurity risks. However, most banks lack dedicated IT committees, and few board members possess IT expertise, which hinders the effective implementation of cybersecurity plans. These results underscore the importance of governance structures and organizational maturity in cybersecurity risk management. Nonetheless, governance-focused studies often remain disconnected from operational and technical risk assessment processes and lack standardized measurement frameworks for integrated cyber risk evaluation.

Cybersecurity risk management in the financial sector extends beyond banking. It also applies to the capital market, insurance, and other financial components. The previous studies [12-19] suggested that cyber threats can significantly harm electronic system operators, necessitating risk profiles tailored for financial systems to minimize such impacts. Technological advancement presents challenges for system operators in maintaining business continuity. Therefore, developing risk-based frameworks such as the integrated risk management model is crucial in addressing and mitigating cybersecurity risks. Overall, prior studies demonstrate that cybersecurity risks in the financial sector are multifaceted, encompassing economic impact, technical vulnerabilities, governance challenges, and compliance requirements. However, these dimensions are frequently addressed in isolation rather than through an integrated risk management perspective.

3. METHODOLOGY

3.1 Development of the Integrated Risk Management Framework for the Indonesian Capital Market assessment instrument

The methodology used in this study includes the development of an Integrated Risk Management for the IRMCM model. The IRMCM model was developed jointly by the National Cyber and Crypto Agency (BSSN), Bank of Indonesia, the Indonesian Payment System Association, and Cyber Security Experts. The research methodology framework is illustrated in Figure 1.

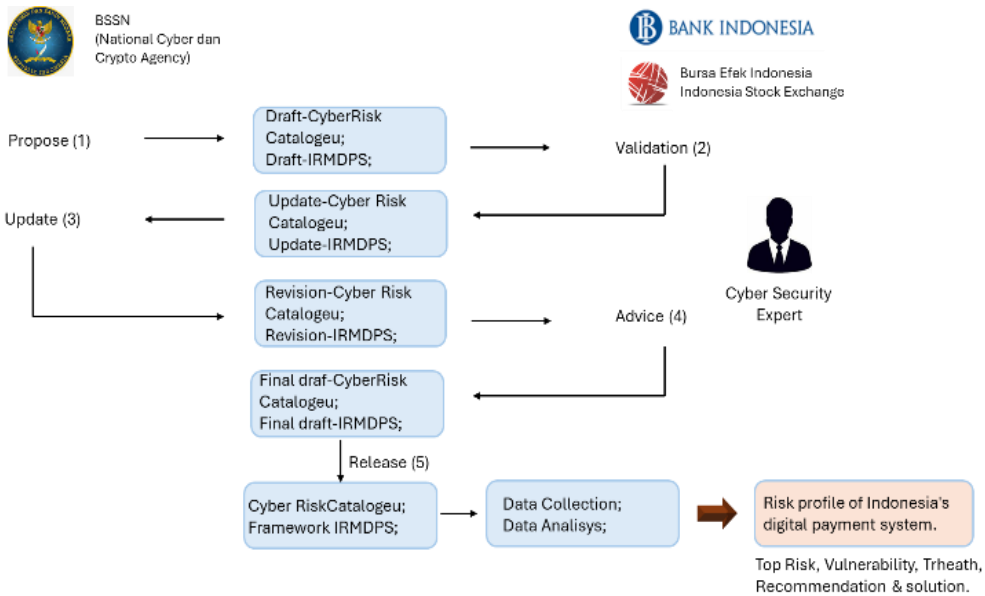

Figure 1. Research methodology for cyber risk profiling in the Indonesian capital market (pasar modal)

The first phase of this research procedure involves the design of an instrument to assess cyber risks in the IRMCM. This instrument is based on the development of the IRMCM framework, which is tailored to identify, measure, and evaluate cyber risks within Indonesia's financial industry. This study uses the IRMCM as a quantitative framework to assess cybersecurity risks, particularly within the IRMCM. The framework integrates international standards such as NIST and

ISO to assess sectoral-level cyber risks. The core components of the framework include Cyber Risk Identification, Cyber Risk Measurement, Cyber Risk Analysis, and Recommendation Development. The steps for constructing the cyber risk assessment instrument for the IRMCM include:

1. The National Cyber and Information Systems Agency (BSSN) will draft a risk catalogue and IRMCM framework based on references, including NIST, ISO, and other existing methods/frameworks.
2. The draft risk catalogue and IRMCM framework will then be validated by Bank Indonesia and the IDX for suggestions and improvements.
3. The BSSN will revise the draft risk catalogue and IRMCM framework, in accordance with recommendations from Bank Indonesia and the IDX.
4. The BSSN, Bank Indonesia, and the IDX will invite a Cyber Security Expert to provide suggestions, recommendations, and improvements to the final risk catalogue and IRMCM framework.
5. The BSSN, Bank Indonesia, and the IDX. will draft the final version of the risk catalogue and IRMCM framework based on the suggestions and recommendations of the Cyber Security Expert.
6. Validity and Reliability Testing of the IRMCM framework will then be conducted.

3.2 Survey and data analysis

The survey targets participants from the IRMCM industry, including banks, non-bank financial institutions, and electronic capital market service providers. A survey approach was selected to gather empirical data from a broad sample of respondents and facilitate statistical analysis. Data collection will be conducted via a structured questionnaire completed by representatives of entities operating in the IRMCM industry.

3.3 Dissemination of research results

One of the crucial stages of research activities is disseminating the research results. Dissemination here is part of the effort to disseminate research results for widespread knowledge and utilization. The dissemination of this research result is conducted only for a limited audience, namely Bank Indonesia, the IDX, and IDX members, as the risk profiling of digital capital market systems in Indonesia is limited to this audience.

4. RESEARCH DISCUSSION

4.1 Development of an integrated risk management capital market

The assessment criteria for each risk refer to National Cyber and Crypto Agency Regulation Number 7 of 2023 concerning the Identification of Vital Information Infrastructure (IIV). This model defines nine criteria: Probability, Operational Impact, Impact on Data/Information, Financial Impact, General Impact, Interdependence Impact, Reputation Impact, Legal Impact, and Other Impacts/Aspects. This risk assessment model will also undergo a validation process by the IDX and cybersecurity experts, ensuring that the criteria and impact scale align with the Indonesian Digital Payment System ecosystem. The model used in developing this assessment instrument will be referred to as IRMCM.

The assessment is conducted to measure each risk based on the established criteria. The results of this assessment are then used to determine the impact scale, from probability to impact, for each risk. The ten highest-scoring risks will be processed into the Indonesian Capital Market Cyber Risk Profile Book. Respondents to the cyber risk assessment instrument are companies involved in the Indonesian payment system. The preparation of the Indonesian Capital Market Cyber Risk Assessment Instrument is part of a series of activities to prepare the Indonesian Capital Market Cyber Risk Profile, which was carried out for 3 months, with the following stages (Figure 2).

The proposed cyber risk catalogue refers to the primary reference, the cybersecurity & data privacy risk management model (C|P-RMM) 2025 [20]. The proposed draft cyber risk catalogue contains 33 (thirty-three) cyber risks divided into seven risk groups: Access Control, Asset Management, Business Continuity, Exposure, Governance, Incident Response, and Situational Awareness.

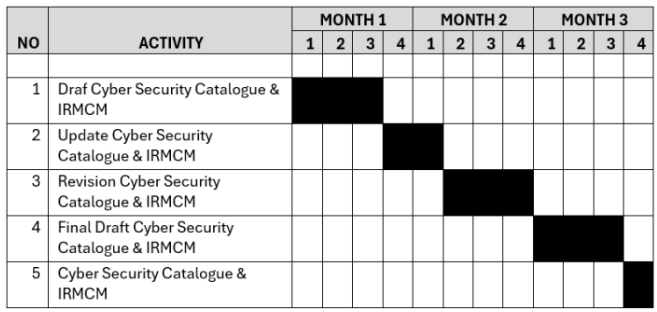

Figure 2. Schedule of Integrated Risk Management Framework for the Indonesian Capital Market (IRMCM) development

The risk criteria in the IRMCM model utilize five impact scales and nine assessment criteria. This IRMCM risk assessment model will undergo a validation process by Bank Indonesia, the IDX, and Cyber Security Experts to ensure that the criteria and impact scales align with the Indonesian Digital Payment System ecosystem.

To align with the integrated cyber risk assessment pillars that capture the unique nature of digital threats [21], this methodology utilizes a multi-dimensional approach to evaluate risk. Several criteria are employed to assess each risk, including Probability, Operational Impact, Data/Information Impact, Financial Impact, General Impact, Interconnectivity Impact, Legal Impact, and Reputational Impact. Each risk criterion utilizes a five-level impact scale, where each level is tailored to relevant cyber risk scenarios by considering likelihood, consequences, and other contributing factors. These levels are categorized as: Low (L), Low to Moderate (LTM), Moderate (M), Moderate to High (MTH), and High (H). The tiered hierarchical structure of each point facilitates the quantification of subjective nuances, providing the necessary data granularity for empirical statistical testing [22].

Figure 3 shows the complete assessment method that will be used to obtain a value for each cyber risk.

Figure 4 is an example of mapping one of the risks on the cyber risk list, namely "Improper assignment of privileged functions or improper granting of privileges by administrators." This risk is mapped to the criteria and impact scale as follows.

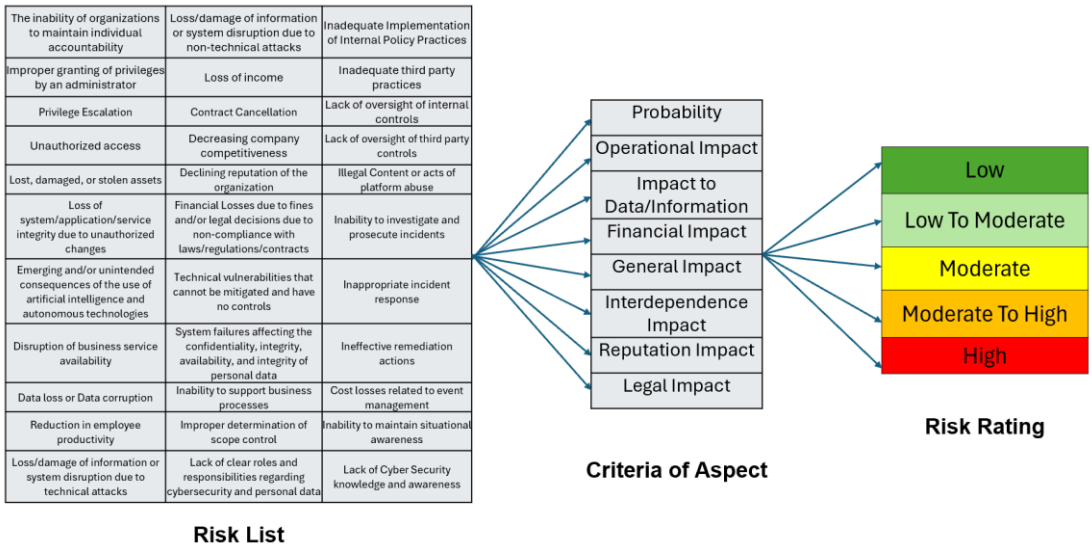

Figure 3. Complete assessment method that will be used to obtain a value for each cyber risk

CYBER RISK PARAMETER							
Risk Number	Risk Name	Aspect Criteria	Low	Low to Moderate	Moderate	Moderate to High	High
			1	2	3	4	5
2	***Improper assignment of privileged functions***	Probability	Occurs < 1.5% of the total number of activities per period	Occurs 1.5% ≤ X < 2.5% of the total number of activities per period	Occurs 2.5% ≤ X < 5% of the total number of activities per period	Occurs 5% ≤ X < 7% of the total number of activities per period	Occurs 7.5% ≥ of the total number of activities per period
		Operational Impact	Zero Incidents (or No Incidents)	Incidents occurred, but user SLA is still met with a permanent solution in place	Incidents occurred, and user SLA is still met with a temporary solution (workaround) in place	Incidents occurred leading to failure to meet user SLA	Incidents occurred resulting in system failure and failure to meet user SLA
		Data / Information Impact	Zero Leakage (or No Data Leakage)	Level I Leakage (The released information has no impact on any related parties).	Level II Leakage (The released information only provides benefit to the receiver/provider of the information).	Level III Leakage (The released information has the potential to harm BEI/IDX as the information owner, and/or other stakeholders and/or shareholders).	Level IV Leakage (Information released from BEI/IDX has the potential to harm the industry).
		Financial Impact	Loss ≤ 2,5%	Loss 2,5% < X ≤ 5%	Loss 5% < X ≤ 7,5%	Loss 7,,5% < X ≤ 10%	Loss > 10%
		Reputation Impact	No negative information / news or Customer Complaints via contact center media, corporate social media, or other company-designated media.	Verbal negative information / news or Customer Complaints delivered directly to company staff	Negative information / news published in various national/international media, resulting in a regulator warning/reprimand or customer complaints submitted via letter or directly to the Head of Unit / Head of Division	Negative information / news published in various national/international media, resulting in a warning/reprimand from a Minister and the regulator, or customer complaints submitted via letter or directly to the Board of Directors (BOD) / Executive Board	Negative information / news published in various national/international media, resulting in a reprimand from the Head of State; OR Notification/letter/warning received from OJK (Financial Services Authority) regarding customer complaints submitted to OJK.
		Legal Impact	No reprimands / warnings / fines	Informal / Verbal appeal / suggestion	Informal / Verbal Reprimand/Warning (e.g., via email)	Written Reprimand / Warning without fine or sanction	Written Warning accompanied by a fine or sanction

Figure 4. Example of risk mapping

	Impact				
Probability	1	2	3	4	5
1	L	L	LTM	M	MTH
2	L	LTM	M	M	MTH
3	LTM	M	M	MTH	H
4	M	M	MTH	H	H
5	MTH	MTH	H	H	H

Figure 5. Probability and impact matrix of risk

The measurement essentially uses the Probability and Impact Matrix concept to assess and prioritize risks based on two main factors: the probability of the risk occurring and the impact it will have if it occurs. The matrix provides a visual representation in tabular form, with one column showing the probability scale and the other showing the impact scale. Each cell in the matrix represents a combination of probability and impact and provides a corresponding risk value. The aforementioned criteria are used to classify cyber risk levels based on two primary parameters: the Probability Scale (P) and the Impact Scale (D). Specifically, there is one criterion for probability and five distinct criteria for impact. In this study, each respondent provides values for P and D corresponding to the risk-related questions presented. To determine the overall impact value from the five criteria for each respondent, an average score is calculated. Once the probability and impact values are obtained, each risk is mapped onto the scale—(L), (LTM), (M), (MTH), (H)—to determine its final risk classification. The matrix used for risk value measurement is shown in Figure 5.

Upon identifying the risk scale for each respondent, the data is grouped to determine the total frequency of each scale (L,

LTM, M, MTH, and H). Subsequently, the final weight is calculated by multiplying the frequency of each scale by its respective predetermined coefficient. The IRMCM Model will generate a list of identified Criteria Aspects and Impact Scales, which will then be assessed using the Assessment Instrument and risk measurement. The results of these measurements will indicate a list of the top cyber risks based on their risk weighting.

4.2 Data collection and assessment

Data collection was conducted through a structured survey method using a questionnaire developed based on the IRMCM framework. This questionnaire was designed as an instrument to assess inherent cyber risks at the sector level. The survey approach was chosen to reach a broad sample of respondents and collect empirical data that could be statistically analysed. The population of this study included all entities in the Digital Payment System industry in Indonesia, consisting of banks, non-bank financial institutions, and electronic payment service providers. The research sample consisted of PSE of Payment Systems specifically selected by the IDX. The IDX's involvement as a Self-Regulatory Organization (SRO) in the IRMCM industry ensures that the selected sample represents the overall landscape of the payment system industry in Indonesia. This provides strong validity to the research findings, as the sample assessed includes key entities that collectively reflect the dynamics and diversity of the sector. Each respondent assessed 33 cyber risks, grouped into seven main categories: Access Control, Asset Management, Business Continuity, Exposure, Governance, Incident Response, and Situational Awareness. The assessment was conducted by assigning a score to each risk based on the probability and impact criteria established in the questionnaire. Respondents assigned a score to each criterion using a five-point rating scale tailored to the relevant cyber conditions in their organization.

4.3 Data analysis

The data analysis flow is carried out sequentially and in detail, as explained below:

1. Calculation of probability value and impact of cyber risk

Based on questionnaires completed by various payment system companies, probability and impact scores were obtained for each cyber risk. The probability (P) score for each cyber risk was calculated based on a scale of 1-5 (L, LTM, M, MTH, and H) provided by all respondents. The impact (D) score for each risk was calculated based on the average score from the five impact criteria assessed by the respondents. Selecting the highest impact score ensures that even if the probability of a cyber risk occurring is low, it has a high impact. Therefore, it can be considered a priority risk for optimal management.

2. Risk value calculation

The risk value is then calculated as a function of probability (P) and impact (D). These values are mapped using a probability and impact matrix. The matrix in Figure 5 serves as a visual representation that identifies the appropriate risk value for each combination of probability and impact.

3. Rate values calculation for cyber risk ranking development

Once the cyber risk scores are obtained, a cyber risk ranking is performed based on the weighted value of each cyber risk. This weighting value serves as a quantitative metric that aggregates the collective assessment of each risk from all respondents. The final risk score for the ranking is calculated using a quantitative approach:

$$R=f(P,D)=(1*L)+(2*LTM)+(3*M)+(4*MTH)+(5*H)$$

Total Respondent Rating							Weight Value
No	Risk	Low	Low to Moderate	Moderate	Moderate to High	High	
1	Talent Scarcity in Cybersecurity	15	2	9	1	2	60
2	Critical Information Infrastructure Vulnerability	14	2	8	2	3	65
3	Missue of Personal Data Information	12	5	6	1	5	69
4	Social Engineering	13	4	6	1	5	68
5	Risk of Mobile Phone Number Misuse	14	1	8	1	5	69
6	Weak Identity Proofing	16	2	7	0	4	61
7	Third Party Operational Risk	17	4	5	1	2	54
8	Software Party Operational Risk	12	1	11	1	4	71
9	End of Support/ End of Life Device Risk	13	1	9	1	5	71
10	Malware and Randsomeware as a Service	12	5	8	1	3	65

Figure 6. Risk ranking based on weight value

The numbers 1, 2, 3, 4, and 5 above are numerical coefficients that assign different weights to each scale level, so that higher rankings proportionally contribute more to the final weighted score. As shown in Figure 6, the final score is generated based on the multiplication of each coefficient for each scale. Next, the final risk scores for each risk are ranked from highest to lowest. This ranking produces a list of the top 10 cyber risks that are the highest priority for the digital payment system sector in Indonesia.

4.4 Preparation of risk profiles and alternative solutions

Through a process of analysing and ranking cyber risks, this study has identified the top 10 cyber risks out of a total of 33 assessed. This list represents the most significant cyber risks and is a priority for management by the IRMCM industry. The following is a list of the top 10 cyber risks, along with a summary of strategic recommendations for each risk (Table 1).

The emergence of these ten primary risks manifests a dynamic interaction between accelerated digital transformation and limited defensive capabilities, which can be interpreted across three key domains. Within the Technical Domain, risks such as Software Vulnerabilities and End-of-Life (EoL) Device Risk are driven by technological factors—particularly legacy systems—that broaden the exposure

criteria and weaken asset management. In the Organizational Domain, Talent Scarcity and Weak Identity Proofing arise from deficiencies in governance and access control criteria, where regulatory drivers often misalign with internal budget availability and human resource competencies. Meanwhile, in the Operational Domain, phenomena such as Ransomware as a Service (RaaS) and Third-Party Risk reflect a shift toward a more organized cybercrime ecosystem, directly challenging an organization's incident management, business continuity, and situational awareness in the face of complex external threats.

Table 1. Summary of top 10 cyber risks

No.	Cyber Risk	Recommendation
1	Talent Scarcity in Cybersecurity	• Implement a well-thought-out cyber-HR plan to fill the quality and quantity gaps. • Conduct regular education, training, and certification programs for HR.
2	Critical Information Infrastructure Vulnerability	• Implement cybersecurity risk management effectively and regularly. • Conduct regular cybersecurity testing.
3	Misuse of Personal Data Information	• Develop and implement internal policies that align with the Personal Data Protection Law (UU PDP). • Ensure that collaborating third parties implement personal data protection provisions.
4	Social Engineering	• Establish and enhance a security awareness program for all employees and users. • Strengthen authentication methods in payment systems, such as the use of Multi-Factor Authentication (MFA).
5	Risk of Mobile Phone Number Misuse	• Increase security awareness within the organization. • Strengthen security controls by implementing more secure MFA mechanisms.
6	Weak Identity Proofing	• Conduct periodic security awareness improvements for all parties. • Use more advanced verification technology, such as biometrics, as MFA.
7	Third Party Operational Risk	• Implement third party management in accordance with Information Security principles. • Implement strict third-party management policies and procedures, including regular compliance monitoring.
8	Software Vulnerabilities	• Implement a Secure Software Development Life Cycle (SSDLC). • Perform regular update management (patching) for all software and operating systems.
9	End of Support/End of Life Device Risk	• Limit the use of access rights on applications to minimize potential damage if a security compromise occurs. • Implement a phased migration of devices and systems that have reached EoS/EoL.
10	Malware and Ransomware as a Service	•Always perform data backups regularly and periodically. • Implement network security solutions such as Intrusion Prevention System (IPS) and firewalls to block malicious activity.

The survey was conducted on 50 Indonesian capital market (PSE) companies selected by the IDX. The IDX selected a sample of PSEs to represent the payment system in Indonesia. Data collection was conducted through an inherent cyber risk mapping survey using the IRMCM (Intrinsic Risk Management) as an instrument to assess cyber risk at the sector level, including the Capital Market. Each respondent assessed 28 inherent cyber risks based on a validated cyber risk catalogue. From the 28 assessed risks, a ranking data analysis was performed to determine priority cyber risks, resulting in the top 10 cyber risks:

1. Talent Scarcity in Cybersecurity.
2. Critical Information Infrastructure Vulnerability.
3. Misuse of Personal Data Information.
4. Social Engineering.
5. Risk of Mobile Phone Number Misuse.
6. Weak Identity Proofing.
7. Third-Party Operational Risk.
8. Software Vulnerabilities.
9. End-of-Support/End-of-Life Device Risk.
10. Malware and Ransomware as a Service.

5. CONCLUSIONS

This study developed the IRMCM framework as a specialized instrument to identify and prioritize cybersecurity risks based on likelihood and impact at the sectoral level. Implementation within the IRMCM ecosystem successfully identified the top priority risks, such as talent scarcity in cybersecurity, critical information infrastructure vulnerabilities, misuse of personal data, and social engineering. This framework provides a structured risk profile that serves as a practical tool for regulators and industry stakeholders in standardizing risk reporting, formulating evidence-based policies, and coordinating sectoral mitigation strategies.

ACKNOWLEDGMENT

This activity is supported by the Research Cluster for Mathematical Modeling and Optimization, Diponegoro University, Semarang, Indonesia. My appreciation also goes to the Indonesian National Cyber and Crypto Agency (BSSN), which supported me in completing my research. I warmly welcome any constructive criticism and suggestions regarding this research, as they are invaluable to my growth and improvement.

REFERENCES

[1] Cains, M.G., Flora, L., Taber, D., King, Z., Henshel, D.S. (2022). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. Risk Analysis, 42(8): 1643-1669. https://doi.org/10.1111/risa.13687

[2] Nguyen, P.H., Nguyen, L.A.T., Pham, H.A.T., Nguyen, T.H.T., Vu, T.G. (2024). 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(19): e37893. https://doi.org/10.1016/j.heliyon.2024.e37893

[3] Dawodu, S.O., Omotosho, A., Akindote, O.J., Adegbite, A.O., Ewuga, S.K. (2023). Cybersecurity risk assessment in banking: Methodologies and best practices. Computer Science & IT Research Journal, 4(3): 220-243. https://doi.org/10.51594/csitrj.v4i3.659
[4] Financial Services Authority (OJK). Law No.8 of 1995 on Capital Market. https://ojk.go.id/en/kanal/pasar-modal/regulasi/undang-undang/Pages/law-no-8-of-1995-on-capital-market.aspx.
[5] President of the Republic of Indonesia. (2022). Presidential Regulation (Perpres) No. 82 of 2022 on the protection of vital information infrastructure. https://peraturan.bpk.go.id/Details/211029/perpres-no-82-tahun-2022.
[6] National Institute of Standards and Technology (NIST). (2024). The NIST Cybersecurity Framework (CSF) 2.0. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.
[7] Asakpa, S.T. (2023). From risk to resilience: Strengthening cyber security in financial institutions. International Journal of Advance Research, Ideas and Innovations in Technology, 9(6): 137-145.
[8] Mpofu, Q. (2025). Digital transformation in the accounting profession in Sub-Saharan Africa: Challenges, opportunities, and strategic pathways. Journal of Accounting, Finance and Auditing Studies, 11(4): 222-230. https://doi.org/10.56578/jafas110403
[9] Thach, N.N., Hanh, H.T., Huy, D.T.N., Nga, L.T.V., Huong, L.T.T., Vu, Q.N. (2021). Technology quality management of the industry 4.0 and cybersecurity risk management on current banking activities in emerging markets-the case in Vietnam. International Journal for Quality Research, 15(3): 845-856. https://doi.org/10.24874/IJQR15.03-10
[10] Supristiowadi, E., Sucahyo, Y.G. (2018). Information security risk management in the agency-level financial application system (SAKTI) of the ministry of finance. Indonesian Treasury Review: Journal of Treasury, State Finance and Public Policy, 3(1): 23-33. https://doi.org/10.33105/itrev.v3i1.20
[11] Rahman, M.B., Karim, T., Chowdhury, I.U. (2021). Role of boards in cybersecurity risk profiling: The case of Bangladeshi commercial banks. Global Journal of Management and Business Research, 21(A3): 49-58. https://doi.org/10.34257/GJMBRAVOL21IS3PG49
[12] Bouveret, A. (2018). Cyber risk for the financial sector: A framework for quantitative assessment. International Monetary Fund. https://doi.org/10.5089/9781484360750.001
[13] Cele, N.N., Kwenda, S. (2025). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. Journal of Financial Crime, 32(1): 31-48. https://doi.org/10.1108/JFC-10-2023-0263
[14] Jalilvand, A., Moorthy, S. (2023). Triangulating risk profile and risk assessment: A case study of implementing enterprise risk management system. Journal of Risk and Financial Management, 16(11): 473. https://doi.org/10.3390/jrfm16110473
[15] Lattanzio, G., Ma, Y. (2023). Cybersecurity risk and corporate innovation. Journal of Corporate Finance, 82: 102445. https://doi.org/10.1016/j.jcorpfin.2023.102445
[16] Putra, I.W.N.M., Wasesa, M. (2024). Managing inherent IT business risk against cyber threats: A decision analysis case study of an oil and gas company. International Journal of Advances in Data and Information Systems, 5(1): 85-100. https://doi.org/10.59395/ijadis.v5i1.1315
[17] Quinn, S., Quinn, S., Ivy, N., Barrett, M., Witte, G., Gardner, R.K. (2024). Staging cybersecurity risks for enterprise risk management and governance oversight. US Department of Commerce, National Institute of Standards and Technology.
[18] Uddin, M.H., Ali, M.H., Hassan, M.K. (2020). Cybersecurity hazards and financial system vulnerability. Risk Management, 22(4): 239-309. https://doi.org/10.1057/s41283-020-00063-2
[19] Ugwuja, V.C., Ekunwe, P.A., Henri-Ukoha, A. (2020). Cyber risks in electronic banking: Exposures and cybersecurity preparedness of women agro-entrepreneurs in South-South Region of Nigeria. Journal of Business Diversity, 20(3): 51-60. https://doi.org/10.33423/jbd.v20i3.3087
[20] Compliance Forge. (2025). Cybersecurity & data privacy risk management model (C|P-RMM) overview. https://securecontrolsframework.com/content/SCF-Risk-Management-Model.pdf.
[21] Chong, W.F., Feng, R., Hu, H., Zhang, L. (2025). Cyber risk assessment for capital management. Journal of Risk and Insurance, 92(2): 424-471. https://doi.org/10.1111/jori.12504
[22] Koo, M., Yang, S.W. (2025). Likert-type scale. Encyclopedia, 5(1): 18. https://doi.org/10.3390/encyclopedia5010018

NOMENCLATURE

P	Probability
D	Impact
L	Low
LTM	Low to Moderate
M	Moderate
MTH	Moderate to High
H	High