International Journal of Safety and Security Engineering
Vol. 16, No. 4, April, 2026, pp. 889-897
Journal homepage: http://iieta.org/journals/ijsse

Cybersecurity Maturity Profile of the Insurance Sector in Indonesia with the Critical Cybersecurity Maturity Index Framework

Slamet Aji Pamungkas[1*], Widowati[2], Aris Sugiharto[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] Department of Informatics, Faculty of Sciences and Mathematics, Diponegoro University, Semarang 50275, Indonesia

Corresponding Author Email: mamung0618@gmail.com

https://doi.org/10.18280/ijsse.160416

Received: 9 March 2026
Revised: 20 April 2026
Accepted: 27 April 2026
Available online: 30 April 2026

Keywords:
digital transformation, cybersecurity maturity, insurance sector, critical cybersecurity maturity index

ABSTRACT

The digitalization of the insurance industry in Indonesia is undergoing rapid transformation, marked by the adoption of Insurtech (Insurance Technology), artificial intelligence (AI), and Internet of Things (IoT) to improve operational efficiency and customer service. In 2025–2026, this industry is expected to continue positive growth with increasingly massive digital transformation, driven by the need for faster, more transparent, and more accessible online insurance services. As this digital transformation accelerates, the risk of cyber disruption increases, and the more digital the system, the greater the disruption. To measure the readiness of insurance industry players to implement digital transformation and utilize electronic systems, it is necessary to profile the level of cybersecurity maturity of insurance industry players in their digital transformation towards a digital economy. The Critical Cybersecurity Maturity Index (CCMI) is a framework and instrument developed to measure cybersecurity maturity levels and also provides recommendations for insurance industry players in Indonesia to improve their cyber readiness to support the digital transformation process in insurance companies. This paper discusses the development, use, and analysis of the CCMI to profile the level of cybersecurity maturity in the Indonesian insurance industry. Based on the profiling results, recommendations can be provided to improve cybersecurity maturity for insurance industry players in the use of electronic systems towards a safer digital economy.

1. INTRODUCTION

The core of digital transformation lies the electronic system, a comprehensive framework of devices and protocols designed to manage the full lifecycle of electronic information. The use of electronic systems includes the use of network-based information technology to process, store, and disseminate information securely and efficiently. The use of electronic systems aims to improve efficiency, transparency, and public service [1]. In Indonesia, the use of electronic systems is growing rapidly in line with policies accelerating digital transformation in all sectors.

Meanwhile, Digital Transformation exists as a major and fundamental change in the way businesses or organizations operate and interact with their customers through the use of digital technology. This transformation is essentially carried out to achieve strategic goals and improve performance [2, 3].

The development of digital transformation in Indonesia like other developing neighboring countries, driven by the high internet penetration. The ongoing digitalization of the financial sectors has introduced an escalating spectrum of cyber that pose a multi-level challenge for state regulators, commercial entities, and the public. Digital transformation has become a major topic in various business development discussions and also hot research issue due to its significant benefits in achieving competitive advantage in the digital era. The various benefits of digital transformation for a business include increased efficiency, productivity, and innovation, enhanced customer service, increased employee engagement and satisfaction, and the creation of new business opportunities [3].

Amidst the rise of digital transformation towards a digital economy, there is the potential for cyber threats that can disrupt and cause significant losses for industry players utilizing the digital economy. Cybersecurity is a threat to most industry players in Indonesia that utilize the digital economy in their businesses. Enhanced security is needed so that industry players can utilize all digital economy services without fear of hacking or data theft. The combination of digital economic expansion, the rise in AI-based fraud, and Indonesia's position on the global attack map shows that cyber risk has transformed into an economic and geopolitical risk.

Cyberattacks not only cause losses in terms of the cost of restoring affected infrastructure and systems, but also involve

ransom payments, which can be financially burdensome. Furthermore, the impact on company revenue is a primary focus of analysis, given that cyberattacks can cause significant operational disruptions and harm productivity. Therefore, a thorough understanding of various aspects of cyberattacks, including human resource awareness, reputational and operational impacts, recovery costs, and revenue losses, will be key to designing effective security strategies and mitigating the risks that can arise from cyberattacks.

Legally mandated under a Presidential Regulation (Perpres), the governance of Critical Information Infrastructure (IIC) necessitates the implementation of rigorous defensive measures by industry stakeholders to ensure the continuity of electronic systems deemed vital to national and public stability [4]. Generally, the nature of the impact on strategic services extends from the company level to the national level. For example, the potential impact is felt when a disruption occurs to electricity distribution infrastructure. The interruption of electricity distribution services not only results in losses for electricity providers but also disrupts services in other sectors such as finance, health, transportation, and government administration. If such incidents are not addressed quickly, they have the potential to escalate into a national crisis. The Critical Cybersecurity Maturity Index (CCMI) is an instrument used to assess cybersecurity maturity, with the aim of assisting the insurance industry in assessing the extent to which cybersecurity maturity has been implemented in their companies. The CCMI is a guide to fulfilling cybersecurity maturity controls used as a reference for insurance industry players to understand the state of security implementation to improve their cybersecurity maturity. This guide also provides examples of mapping electronic system protection framework controls against several general standards such as SNI ISO/IEC 27001:2022, NIST SP 800-53 revision 5, NIST CSF 1.1, and NIST CSF 2.0. The conceptualization of the CCMI instrument is fundamentally anchored in the NIST Cybersecurity Framework (CSF) 2.0.

This framework provides a comprehensive taxonomy through six pivotal functions Govern, Identify, Protect, Detect, Respond, and Recover which serve as the structural pillars for evaluating organizational resilience. By aligning the CCMI with these standardized functions, the instrument facilitates a granular analysis of cybersecurity maturity. This alignment is critical for establishing a robust management protocol for the socio-technical risks inherent in digital ecosystems, ensuring that security measures evolve in tandem with emerging threats [5, 6].

2. REVIEW OF LITERATURE

2.1 Cybersecurity landscape in Indonesia

According to the 2025 National Cyber and Cyber Security Agency (BSSN) report, the total anomalous traffic in Indonesia during 2024 was 330,527,636 anomalies, with the highest type of anomalous traffic being the Mirai Botnet, with a total of 81,286,596 activities. In 2024, there were 2,487,041 Advanced Persistent Threat (APT) activities, 514,508 Ransomware activities, and 26,771,610 phishing activities. BSSN sent 1,367 incident notification alerts to stakeholders, with the most common notification type being Data Breach. A search of the darknet revealed 56,128,160 data exposures impacting 461 stakeholders in Indonesia. In the case of web defacement, 5,780 cases were found targeting multiple domains, and 4,071 web defacements related to online gambling targeted government websites [7].

Based on reports received from stakeholders on the cyber complaint service, 1,814 complaints were received in 2024. BSSN has published 51 security alerts. One of the Top CVEs globally based on the Common Vulnerability Scoring System (CVSS) score with a Critical impact level is CVE-2024-3400 which allows threat actors to steal information, install malware, or disrupt critical operations on the system. Meanwhile, one of the Top CVEs nationally based on the highest number of hits in Indonesia is CVE-2024-23897 which causes sensitive information disclosure, Server-Side Request Forgery (SSRF), and local script execution to control the server or increase access rights on the system. Based on the results of the IT Security Assessment (ITSA) test, 1,931 vulnerabilities were found consisting of 256 critical vulnerabilities, 405 high vulnerabilities, 350 medium vulnerabilities, 621 low vulnerabilities, and 299 info vulnerabilities in 462 applications targeted by ITSA, including web, mobile, and infrastructure applications [7].

2.2 Cybersecurity maturity level

Cybersecurity maturity is a condition that describes an organization's capability and progress in implementing, improving, and implementing cybersecurity effectively and efficiently. A cybersecurity maturity level is an evaluation framework for measuring the effectiveness of information security policies, processes, and technologies within an organization, using a specific scale [8, 9]. This helps map the current position, identify weaknesses, and plan security improvements in a structured and progressive manner [10].

The cybersecurity maturity level for an electronic system is formulated with reference to the following:

(1) Improving industry players' understanding of the importance of cybersecurity.

This aims to provide stakeholders with a clear picture of the state of cybersecurity implementation and to enhance industry players' understanding of the importance of assessing maturity in implementing the electronic system protection framework they use [9, 10].

(2) Referencing information security standards (national and international).

Ensuring that in implementing the electronic system protection framework, industry players have referred to information security standards and other relevant standards to strengthen the protection of the electronic systems they use [8, 9].

(3) Mapping controls against cybersecurity standards.

Provides examples of mapping controls within an electronic system protection framework to commonly used international standards, such as SNI ISO/IEC 27001:2022, NIST SP 800-53 revision 5, NIST CSF 1.1, and NIST CSF 2.0, as a reference in implementing effective and appropriate controls [8, 9].

2.3 Insurance industry in Indonesia

The insurance industry plays a crucial role in the Indonesian economy. In today's era, insurance plays a crucial role in protecting against unforeseen events, both risks impacting businesses and individuals [11]. In other words, insurance helps businesses and individuals mitigate the risks inherent in every activity. When linked to the business sector, insurance

can play a role across all sectors, such as commodities, retail, transportation, infrastructure, and others. For individuals, insurance can be present in all aspects requiring protection, including health, life, and property protection [11]. This demonstrates the vital role of the insurance industry in driving the Indonesian economy.

Digital transformation in the Indonesian insurance industry is rapidly developing through the adoption of Insurtech (Insurance Technology) and mobile applications [12]. This technological integration aligns with the strategic framework established in the study [13], which positions digital transformation as a fundamental pillar for reinforcing industrial structures and restoring public trust through governance reform. Furthermore, these initiatives aim to cultivate a more inclusive and efficient insurance ecosystem, thereby enhancing the sector's capacity to mitigate systemic risks and achieve heightened levels of cybersecurity maturity within the digital economy.

To support operational activities aimed at serving policyholders, the utilization of information technology is necessary. By effectively utilizing information technology, insurance companies can drive efficiency and effectiveness in their business processes while increasing their competitiveness [13, 14]. Digital transformation in the insurance industry is not just about adopting new technology, it also changes the way companies operate and interact with customers, as well as improving service quality. In the insurance industry, digital transformation is not only about adopting new technologies, but also about changing the way companies operate and interact with customers, as well as improving service quality. Insurance companies are leveraging digital technology to create more relevant products for customers, provide better services, and improve operational efficiency. This includes strengthening their information technology infrastructure, increasing human resource capacity in the technology sector, and expanding collaboration with digital ecosystems. These efforts continue to accelerate due to the rapid pace of change in the digital economy, requiring the insurance industry to adapt accordingly [12, 14].

2.4 Cyber risks in the insurance sector in Indonesia

While the digital paradigm facilitates unprecedented growth and operational agility within the insurance sector, it concurrently expands the surface for cyber risk exposure. The transition toward data centric business models introduces critical vulnerabilities, including the unauthorized exfiltration of sensitive policyholder information and the potential for prolonged interruption of core business operations. These threats scale proportionally with the intensity of technological integration, underscoring the necessity for a structured, maturity based approach to risk management. Consequently, to safeguard institutional resilience, industry stakeholders must transition toward a holistic, security posture that evolves in tandem with the advancing digital landscape [12-18].

Cyberattacks in the Indonesian insurance sector increased dramatically in line with digital transformation policies, targeting customer and operational data through ransomware and data breaches [14]. Some examples of cyberattacks that have occurred in the insurance sector in Indonesia include:

(1) The Bank Rakyat Indonesia Life (BRI Life) data breach in 2021. Hackers allegedly stole approximately 2 million customer data and 460,000 important documents, including scanned ID cards and account details, which were then sold on the dark web.

(2) Ransomware attacks on the Social Security Administration (BPJS) in 2020-2021. The BPJS Kesehatan data leak and ransomware attacks on several Indonesian hospitals hampered access to patient data, impacting the health insurance claims process. This cyber-attack on BPJS also resulted in the leakage of hundreds of millions of participant data, potentially causing material losses of up to IDR 600 trillion (approximately US$40 billion), and a high risk of data misuse.

These cyberattacks resulted in data leaks that could result in losses for both companies and customers, including facilitating phishing, wallet account takeovers, the creation of fake ID cards for online loans, and other threats [19-22].

3. METHODOLOGY

3.1 Development of Critical Cybersecurity Maturity Index (CCMI) maturity level measurement instrument

Figure 1 shows how the development of the CCMI instrument process is carried out through the following stages:

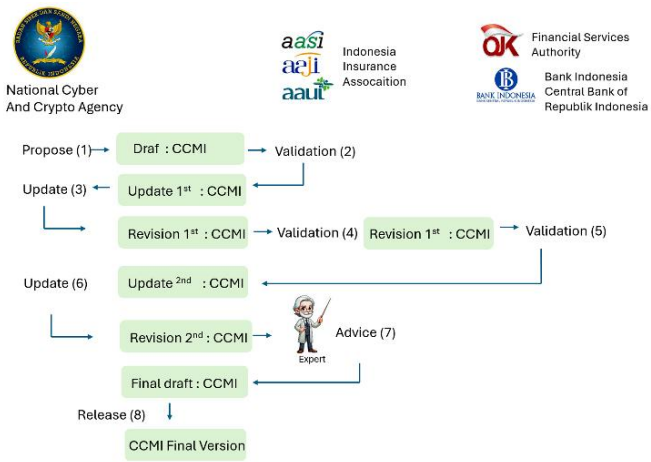

Figure 1. Critical Cybersecurity Maturity Index (CCMI) development mindmap

(1) The National Cyber and Crypto Agency (BSSN) team conducted a literature review of existing models, instruments, and standards to develop the CCMI instrument. Some of the references used in developing the CCMI instrument include: SNI ISO/IEC 27001:2022, NIST SP 800-53 revision 5, NIST CSF 1.1, and NIST CSF 2.0, and BSSN Regulation Number 10 of 2023 concerning cybersecurity maturity assessment.

(2) To ensure the instrument's content and face validity, the CCMI framework underwent a structured qualitative validation process through iterative Focus Group Discussions (FGDs). The expert panel consisted of representatives from BSSN, the Indonesian General Insurance Association (AAUI), Life Insurance Association (AAJI), and Sharia Insurance Association (AASI), specifically selecting individuals with over 10 years of experience in cybersecurity policy and financial sector regulations. These experts evaluated each control item for clarity, practical relevance, and alignment with OJK (Financial Services Authority)

regulatory requirements, leading to several refinements in the control descriptions before the field survey was initiated.

(3) The BSSN team revised and revised the CCMI draft based on recommendations from the insurance associations in Indonesia. The first revision was then sent to the Indonesian insurance association, Bank Indonesia (BI), and the Financial Services Authority (OJK) for review and recommendations.

(4) After receiving the review and recommendations, the BSSN team made improvements and produced the second revision of the CCMI. A final discussion with cybersecurity experts was then held to produce the final version of the CCMI.

Figure 2 shows CCMI development timeline, with a time span of approximately 3 months.

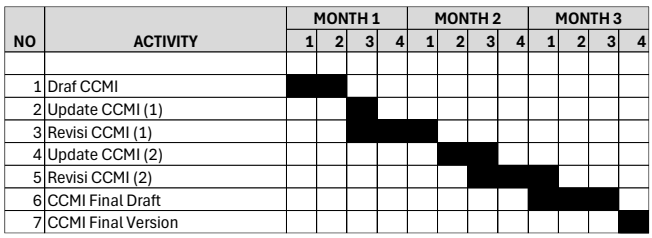

Figure 2. Critical Cybersecurity Maturity Index (CCMI) development timeline

3.2 Survey and data analysis

After the CCMI instrument was developed, the next step was to conduct a survey of the insurance industry. To obtain accurate and valid data, the survey sample was determined by the Indonesian Insurance Association, Bank Indonesia (BI), and the Financial Services Authority (OJK). The questionnaire was completed online, using a web-based application for the CCMI instrument. Respondents were assisted by the BSSN team during the data collection process. After the data collection, analysis was conducted to obtain a profile of the cyber maturity of the insurance industry in Indonesia and provide recommendations for improvements to enhance its cybersecurity maturity. The sampling strategy was conducted in close coordination with the Indonesian General Insurance Association (AAUI) and the Life Insurance Association (AAJI) to ensure the representativeness of the data. The selected participants encompass a majority of the market leaders and key industry players, providing a comprehensive cross-section of the insurance sector in Indonesia. This collaborative approach allowed for a balanced inclusion of both systemic large-scale insurers and medium-sized enterprises, ensuring that the maturity profile reflects the diverse operational scales within the ecosystem. Furthermore, the involvement of these associations served as a preliminary validation layer to ensure that the participating entities possess the necessary digital infrastructure to be assessed by the CCMI framework.

3.3 Dissemination of research results

The next step is to disseminate the insurance sector's cybersecurity maturity profile and recommendations for improvement, so that the Indonesian Insurance Association can immediately take steps in accordance with the recommendations. These cybersecurity maturity profiles and recommendations are expected to form the basis for the Indonesian Insurance Association's work program, aimed at improving maturity and preparedness in the face of increasingly prevalent cyber threats.

4. RESEARCH DISCUSSION

4.1 Development the Critical Cybersecurity Maturity Index instrument

The CCMI is designed to measure the extent to which an electronic system has implemented an electronic system protection framework by an electronic system organizer (ESO). In implementing this framework, the ESO is expected to refer to various relevant cybersecurity standards. In this paper, the ESO referred to is an insurance company that uses electronic systems for office operations, customer services, and other purposes. The CCMI also provides examples of mapping electronic system protection framework controls to several general standards, such as SNI ISO/IEC 27001:2022, NIST SP 800-53 revision 5, NIST CSF 1.1, and NIST CSF 2.0.

Distinct from the broad-spectrum approach of international standards like these standards above, the CCMI is tailored to the unique constraints of the Indonesian insurance landscape. The framework transcends basic control mapping by embedding context-specific indicators mandated by national regulators, such as OJK and BSSN. A pivotal innovation in the CCMI scoring logic is the inclusion of an 'Inherent Risk' multiplier, which evaluates the specific classifications of processed data—a specialized metric typically absent in global cybersecurity maturity models.

The CCMI has four domains: Identification, Protection, Detection, and Mitigation and Recovery. When using the CCMI to determine the cybersecurity maturity level of an ESO, weighting is required for each domain, taking into account various factors, including organizational size, infrastructure complexity, and risk profile. The weighting for each domain is as follows:

(1) Identification Domain (25%)

Includes asset inventory, risk assessment, and threat analysis. This is the initial stage in identifying what needs to be protected and understanding potential risks. This weight is assigned because asset identification is the foundational risk management step. In a sector where digital footprints are expanding through third-party Insurtech, knowing the boundaries of the digital ecosystem is a high-priority strategic requirement.

(2) Protection Domain (30%)

Focuses on implementing controls to protect systems and data from threats, including access control, encryption, and security policies. As the domain with the highest weight, this reflects the 'Prevention-First' principle. The analytical justification lies in the mandatory compliance with the Indonesian Personal Data Protection (PDP) Law, where the cost of data exfiltration far exceeds the cost of preventive controls for sensitive policyholder data.

(3) Detection Domain (25%)

This component measures an organization's ability to quickly and accurately identify suspicious activity or cybersecurity incidents. This includes network monitoring, threat detection, and security analysis. This domain is weighted equally with 'Identify' to address the critical gap in real-time monitoring within the industry. Analytically, effective detection serves as the primary failsafe to minimize

the 'dwell time' of an attacker, which is vital for maintaining the integrity of financial transactions.

(4) Mitigation and Recovery Domain (20%)

This covers incident response, impact mitigation, and necessary actions, including isolation of affected systems, remediation, and recovery. This domain includes ensuring business continuity, even in the event of a cyberattack. While slightly lower in weight, these domains represent the resilience phase. The logic here is that while resilience is essential, the framework's current strategic goal for the Indonesian insurance sector is to first mature the capabilities of prevention and early detection to reduce the frequency of full-scale incidents.

The weighting of these CCMI domains is based on the following considerations:

(1) Balance between Prevention and Response: It is important to strike a balance between preventing attacks and being able to respond when they occur. Strong protection reduces the likelihood of an attack, while detection and response ensure that unavoidable threats can be effectively managed.

(2) Organizational Needs: Different organizations have different needs. For example, organizations with highly sensitive data may require a larger allocation for protection, mitigation, and recovery.

(3) Industry Regulations and Standards: Certain standards and regulations may influence allocation, as set out in frameworks like the NIST Cybersecurity Framework, which recommends a risk-based approach and in-depth assessment.

Figure 3 shows the control components within each domain of the MMCI. Each control within a domain provides a more detailed overview of the measurements within that domain.

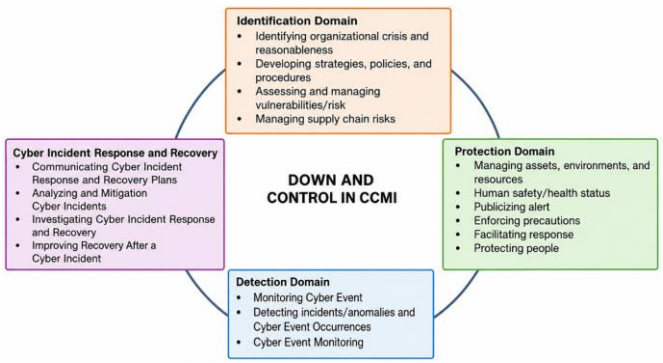

Figure 3. Critical Cybersecurity Maturity Index (CCMI) domain and control

When completing the CCMI measurement instrument, electronic system operators are asked to determine the cybersecurity maturity level for each item (question) by selecting a value from 0 to 6, according to the conditions applicable to their respective electronic system operators. Figure 4 shows the level of cybersecurity maturity ranging from 0 (not implemented), 1 (already implemented in a small number of aspects but not yet formalized), 2 (implemented in limited aspects but not yet formalized), 3 (implemented in most aspects but not yet formalized), 4 (fully and formalized across all aspects), 5 (fully implemented, formalized and subject to periodic monitoring and review) to 6 (fully implemented, formalized and subject to periodic monitoring and review, and improvement) for each control, according to the conditions prevailing in the organization.

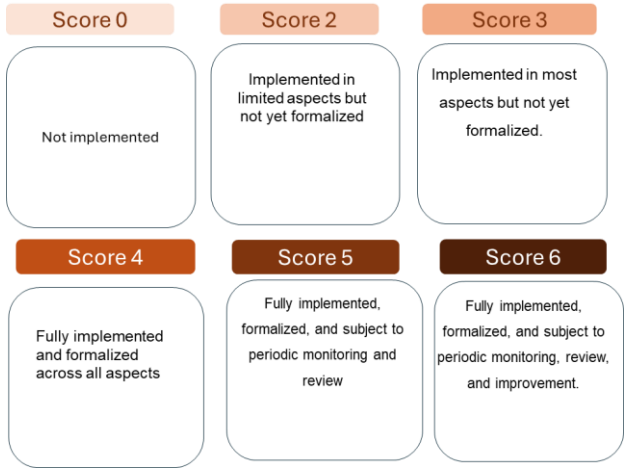

Figure 4. Cyber security maturity leveling

4.2 Critical Cybersecurity Maturity Index formula and leveling

To determine the cybersecurity maturity score and level for an ESO, CCMI uses several formulas. These formulas apply to subcategories, categories, domains, and the total level within a single CCMI. The formula used in the CCMI measurement instrument is as follows:

The sub-category score is obtained from the average of the related control index values.

$$\bar{k_i} = \frac{\sum_{i=1}^{l} k_i}{l}$$

The Cybersecurity Maturity Score per Category is obtained from the average of the sub-category scores in the related Category.

$$\bar{K_i} = \frac{\sum_{i=1}^{m} \bar{k_i}}{m}$$

The Cybersecurity Maturity Score per Domain is obtained from the average Cybersecurity Maturity Score of the Categories in the related Domain

$$M_I/M_P/M_D/M_R = \frac{\sum_{i=1}^{n} \bar{K_i}}{n}$$

Cybersecurity Maturity Score for All Domains/Total obtained by adding the Cybersecurity Maturity Score per Domain after multiplying it by the per-Domain weight.

$$M_T = (25\% * M_I) + (30\% * M_P) + (25\% * M_D) + (20\% * M_R)$$

4.3 Data collection and verification

Data was gathered through a structured survey utilizing a questionnaire adapted from the CCMI instrument. This methodology was selected to engage a diverse participant pool and facilitate robust statistical analysis of the empirical results. The study population included all insurance industry players who utilize electronic systems (ES) in their activities, with the sample determined by the Indonesian Insurance Association. Data collection was conducted through a collaborative process, with respondents completing data online, with assistance from the BSSN team. Each respondent completed the CCMI

questionnaire, which consisted of four domains and 17 control questions, totaling.

Table 1 shows the evaluation indicators for the implementation of the framework domain and activity categories consisting of maturity level categories consisting of levels 1 to 5, and criteria that explain the conditions of cyber implementation in an organization or company.

The data collection, analysis, and verification process involved the following steps:

(1) The BSSN team, together with the Indonesian Insurance Association, determined a sample from the insurance industry population in Indonesia. This sample selection was based on criteria agreed upon by BSSN and the Indonesian Insurance Association.
(2) The insurance industry assisted in completing the questionnaire, with insurance industry players, as Electronic
(3) BSSN, together with the Indonesian Insurance Association, collected, analyzed, and verified the CCMI questionnaires completed by respondents.
(4) BSSN, together with the Indonesian Insurance Association, prepared a cyber maturity profile report and recommendations for improvement.

4.3.1 Measurement results

Tables 2 and 3 show the results of measuring the level of cybersecurity maturity at an insurance company that is an electronic system provider (ESO).

Table 1. Cyber security maturity level domain and worksheet

Maturity Level Category			Criteria				
Level 1	Initial	0.00–1.50	Describes an initial stage of cybersecurity implementation.	Procedures are not yet organized.	Cybersecurity implementation is informal.	Cybersecurity is not performed consistently or continuously.	Risk management and control documents have not been drafted.
Level 2	Repeatable	1.51–2.50	Describes a repeatable stage of cybersecurity implementation.	Procedures are organized.	Cybersecurity implementation remains informal.	Cybersecurity is performed repeatedly but is not yet consistent or continuous.	Risk management and control documents are drafted but not yet formalized/ approved.
Level 3	Defined	2.51–3.50	Describes a well-defined stage of cybersecurity implementation.	Implementation is clearly organized.	Cybersecurity implementation is formal.	Cybersecurity is performed repeatedly and consistently, and is reviewed periodically.	Risk management and control documents are drafted and formalized.
Level 4	Managed	3.51–4.50	Describes a well-managed stage of cybersecurity implementation.	Implementation is well-organized but lacks automation processes.	Cybersecurity implementation is formal.	Cybersecurity is performed repeatedly, and improvements are implemented continuously.	Risk management and control documents are drafted and formalized.
Level 5	Innovative	4.51–5.00	Describes an optimized stage of cybersecurity implementation.	Implementation is well-organized and includes automation processes.	Cybersecurity implementation is formal.	Cybersecurity is performed repeatedly and consistently, and is fully integrated into the organizational culture.	Risk management and control documents are formalized.

Table 2. Result of cybersecurity maturity level measurement

Self Assessment Results	Identification		Protection		Detection		Response & Recover	
2.89	3.15		2.93		2.69		2.80	
	Identifying organizational roles and responsibilities	3.22	Managing identity, authentication, and access control	2.98	Managing cyber incident detection	2.87	Developing incident response and recovery plans	2.58
	Developing strategies, policies, and procedures	2.84	Protecting physical assets	2.67	Analyzing anomalies and cyber incidents	2.54	Analyzing and reporting cyber incidents	2.47
	Assessing and managing cyber security risks	3.12	Protecting data	2.96	Continous monitoring of cyber incidents	2.65	Executing cyber incident response and recovery	3.12
	Managing supply chain risks	3.43	Securing applications	3.01			Security enhancement post-cyber incident	3.01
			Securing networks	2.86				
			Protecting Human Capital	3.12				

Table 3. Results of BSSN team's verification of a self-assessment

BSSN Verification Results	Identification		Protection		Detection		Response & Recover	
2.82	3.03		2.91		2.69		2.67	
	Identifying organizational roles and responsibilities	3.22	Managing identity, authentication, and access control	2.98	Managing cyber incident detection	2.87	Developing incident response and recovery plans	2.58
	Developing strategies, policies, and procedures	2.84	Protecting physical assets	2.67	Analyzing anomalies and cyber incidents	2.54	Analyzing and reporting cyber incidents	2.47
	Assessing and managing cyber security risks	2.89	Protecting data	2.96	Continous monitoring of cyber incidents	2.65	Executing cyber incident response and recovery	3.12
	Managing supply chain risks	3.16	Securing applications	3.01			Security enhancement post-cyber incident	3.01
			Securing networks	2.86				
			Protecting Human Capital	2.98				

Table 2 shows a summary of the results of the cybersecurity maturity level measurement conducted independently by electronic system administrators, with an average score of 2.89. This score falls within the range of 2.51-3.50 and falls into the Level 3 (defined) category. The explanation for Level 3 can be presented as the state of cybersecurity implementation in a well-defined implementation stage, Cybersecurity implementation is also clearly organized, Formal, repeatedly, consistently, and reviewed periodically. Risk management and control management documents have been prepared and established.

Table 3 shows the results of the BSSN team's verification of a self-assessment conducted by an electronic system operator. The BSSN team's verification revealed several improvements, including:

(1) In the Identification and Control domains 3 (Assessing and Managing Cybersecurity Risks) and 4 (Managing Supply Chain Risks), scores were improved, with control 3's score decreasing from 3.12 to 2.89 and control 4's score decreasing from 3.43 to 3.16.
(2) In the Protection domain, control 6 (Protecting Human Resources), the score was also corrected from 3.12 to 2.98.
(3) The average assessment score also changed from 2.89 to 2.82. However, these changes did not affect the final score, which remained at Level 3 (defined).

The following are examples of notes and recommendations for improvement resulting from the cybersecurity maturity measurement above:

(1) Protection Domain: Controls: Protecting physical assets.

Notes:

- The ESO has not consistently implemented methods and procedures for protecting physical assets.
- The placement and protection of physical assets are not optimal and disciplined.

Recommendations:

- Establish controls to monitor the implementation of physical asset protection procedures.
- Provide a more secure location for critical physical assets.

(2) Detection Domain: Controls: Analyzing anomalies and cyber events.

Notes:

- The ESO does not routinely and periodically analyze emerging anomalies, resulting in them not being properly handled and potentially leading to cyberattacks.

Recommendations:

- Conduct routine traffic anomaly monitoring. This can be done automatically using a system, or semi-manually by assigning a person to monitor anomalies periodically.
- Provide rules and procedures for the anomaly monitoring system and for prevention and handling efforts.

(3) Response and Recovery Domain: Developing a Cyber Incident Response and Recovery Plan

Note:

- There is no standard document for a cyber incident response and recovery plan.
- The available documents are not yet adapted to current technological developments and cyber threats.

Recommendations:

- Companies should immediately develop and establish documents for cyber incident response and recovery.
- These documents should be regularly reviewed to ensure they are in line with technological developments and cyber threats.

(4) Response and Recovery Domain: Analyzing and Reporting Cyber Incidents.

Note:

- When a cyber incident occurs, no analysis of the attack is prepared, and there is reluctance to report the attack.

Recommendations:

- Companies should prepare a cyber incident analysis and evaluation document.
- A report and evaluation document should be prepared for each incident.

To obtain comprehensive results, cybersecurity maturity levels were measured using the CCMI instrument at several insurance companies selected as samples. The CCMI measurements were conducted on the following samples: 20 general insurance companies, 20 life insurance companies, and 10 sharia insurance companies. The total sample size was 50 companies.

Figure 5 shows a summary of the results of CCMI

implementation on 50 insurance industry samples as electronic system providers (ESOs). The left graph depicts a map of cybersecurity maturity, while the right graph shows statistics on issues within each CyMII domain.

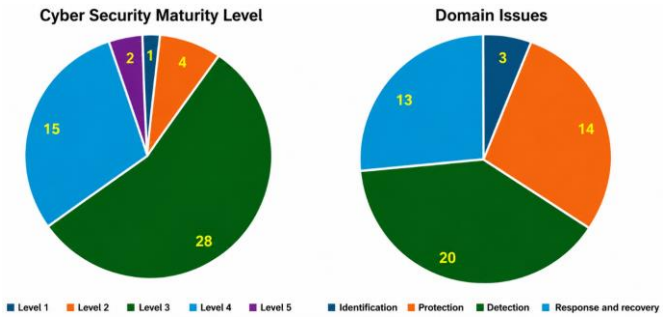

Figure 5. Critical Cybersecurity Maturity Index (CCMI) implementation to samples

The left graph shows that the majority of insurance companies are at level 3 (28 companies), followed by level 4 (15 companies), and two companies at level 5. However, there are still companies with cybersecurity maturity levels at levels 1 and 2.

The right graph illustrates the domains that pose challenges for the insurance industry regarding cybersecurity maturity. The most common issues relate to the detection domain (20 companies), followed by the Protection domain (14 companies), and the Response and Recovery domain (13 companies).

5. CONCLUSIONS

Beyond summarizing the maturity levels, this study contributes the CCMI as a specialized instrument that bridges the gap between generic international standards and the specific regulatory requirements of the Indonesian insurance sector. It provides a structured weighting logic that prioritizes high-risk domains like Protection and Detection, offering a more nuanced assessment tool for regulators and industry players in emerging digital economies.

This study contributes to the cybersecurity literature by introducing the CCMI, a specialized instrument designed to bridge the gap between universal standards (NIST CSF and ISO 27001) and the unique regulatory demands of the Indonesian insurance sector. The research confirms that while the industry has achieved a Level 3 (Defined) maturity, there remains a critical capability gap in the Detection and Response domains, where 40% of the sampled companies struggle with real-time anomaly monitoring.

This study develops the CCMI framework as an instrument for measuring the level of cybersecurity maturity in the insurance industry. The implementation of CCMI in the insurance industry produces a profile and map of the strengths and readiness of the insurance industry in Indonesia to cyber threats in the digital transformation process in the insurance industry. CCMI provides a structured profile and map of the level of cybersecurity maturity of the insurance industry in Indonesia that can be used by insurance industry players, insurance associations in Indonesia, and regulators (BI and OJK) to conduct evaluations, improvements, and policies to protect the Indonesian insurance industry from cyber threats.

While traditional assessments using NIST CSF or COBIT provide a high-level overview, the CCMI scoring logic demonstrates greater sensitivity to the specific regulatory and technical constraints of the Indonesian insurance landscape. This is consistent with the observation on the rapid digital transformation of Indonesian *insurtech*, which necessitates more granular metrics than those used in general IT firms. Furthermore, the results differ from the findings in the Vietnamese banking sector, where strategic prioritization of risk is more advanced, suggesting that the Indonesian insurance industry requires a more specialized, baseline-driven approach for future benchmarking.

Despite its practical utility, this study is subject to several limitations. First, the geographic focus is restricted to the Indonesian landscape, which may limit the generalizability of the findings to other jurisdictions. Second, with a sample size of 50 entities, the maturity profile reflects key market leaders but may not fully capture the constraints of smaller, emerging insurtech firms. Lastly, the current validation of the CCMI relies on qualitative expert consensus through FGDs. Future research should aim to address these gaps by performing longitudinal assessments to track maturity evolution over time and incorporating quantitative validation methods, such as Confirmatory Factor Analysis (CFA), to test the framework's statistical reliability. Expanding the CCMI's application to other financial sub-sectors, such as banking or pension funds, would further enhance its robustness and facilitate cross-sectoral cybersecurity benchmarking.

ACKNOWLEDGMENT

I would like to express my gratitude to the Minister of Higher Education, Science, and Technology for funding this study under the Research Program Implementation Contract (Doctoral Dissertation Research Scheme), Fiscal Year 2026 (Contract No.: 254-11/UN7.D2/PP/IV/2026). We extend our sincere thanks to the BSSN Team, the Indonesian Insurance Association, Bank Indonesia (BI), the Financial Services Authority (OJK). This activity is also supported by the Research Cluster for Mathematical Modeling and Optimization, Diponegoro University, Semarang, Indonesia.

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] Ji, X.L., Li, W.Q. (2022). Digital transformation: A review and research framework. Frontiers in Business, Economics and Management, 5(3): 21-27. https://doi.org/10.54097/fbem.v5i3.1898

[4] President of the Republic of Indonesia. (2022). Presidential Regulation No. 82 of 2022 on the protection of vital information infrastructure. https://peraturan.bpk.go.id/Details/211029/perpres-no-

82-tahun-2022.
[5] 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 and IT Research Journal, 4(3): 220-243. https://doi.org/10.51594/csitrj.v4i3.659
[6] United States. Superintendent of Documents. (1992). National Institute of Standards and Technology. US Government Printing Office. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.
[7] Rosdiana, H., Reja, R., Setiawan, B.H. (2026). The role of the national cyber and crypto agency (BSSN) in Indonesia's cybersecurity architecture. Journal of Social, Political, and Humanities Research Cluster. 5(1): 872-882. https://doi.org/10.55606/jurrish.v5i1.8471
[8] Sulistyowati, D., Handayani, F., Suryanto, Y. (2020). Comparative analysis and design of cybersecurity maturity assessment methodology using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. International Journal on Informatics Visualization, 4(4): 225-230. https://doi.org/10.30630/joiv.4.4.482
[9] Marican, M.N.Y., Razak, S.A., Selamat, A., Othman, S.H. (2023). Cyber security maturity assessment framework for technology startups: A systematic literature review. IEEE Access, 11: 5442-5452. https://doi.org/10.1109/ACCESS.2022.3229766
[10] Jauhari, M.A., Wardijono, B.A., Hegarini, E. (2024). Measuring cyberscurity maturity in information technology companies using the center of internet security controls framework. Jurnal Saintekom: Sains, Teknologi, Komputer Dan Manajemen, 14(1): 72-83. https://doi.org/10.33020/saintekom.v14i1.610
[11] Majid, M., HAMID, A. (2017). Assessing the productivity of insurance companies in Indonesia: A non-parametric approach. Journal of Applied Economic Sciences, 12(6): 1593-1605.
[12] Susanto, A. (2022). Digital transformation of the insurance industry: The potential of insurance technology (Insurtech) in Indonesia. Journal of Humanities, Social Sciences and Business, 2(1): 54-62. https://doi.org/10.55047/jhssb.v2i1.375
[13] Otoritas Jasa Keuangan. (2023). Roadmap for the development and strengthening of the Indonesian insurance industry 2023-2027: Restoring confidence through industrial reform. https://www.ojk.go.id/id/berita-dan-kegiatan/info-terkini/Documents/Pages/Peta-Jalan-Pengembangan-dan-Penguatan-Perasuransian-Indonesia-2023-2027/Peta%20Jalan%20Pengembangan%20dan%20Penguatan%20Perasuransian%20Indonesia%202023-2027.pdf.
[14] Joenaedi, F., Tarina, D. (2024). Cyber insurance as a risk mitigation tool and company compliance instrument with Indonesia's personal data protection law. Unram Law Review, 8(2): 243-257. https://doi.org/10.29303/ulrev.v8i2.380
[15] 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 of Quality Research, 15(3): 845-856. https://doi.org/10.24874/IJQR15.03-10
[16] Asakpa, S.T. (2023). From risk to resilience: Strengthening cyber security in financial institutions. International Journal of Advanced Research Ideas and Innovations in Technology, 9(6): 137-145.
[17] 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
[18] Supristiowadi, E., Sucahyo, Y.G. (2018). Information security risk management in the financial application system at the agency level (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
[19] Badan Siber dan Sandi Negara. (2023). Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2023 tentang Pengukuran Tingkat Kematangan Keamanan Siber. Berita Negara Republik Indonesia Tahun 2023. https://peraturan.bpk.go.id/Details/291280/peraturan-bssn-no-10-tahun-2023Nomor 875.
[20] 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
[21] Bank Indonesia. (2024). Peraturan Bank Indonesia Nomor 2 Tahun 2024 tentang Keamanan Sistem Informasi dan Ketahanan Siber bagi Penyelenggara Sistem Pembayaran, Pelaku Pasar Uang dan Pasar Valuta Asing, serta Pihak Lain yang Diatur dan Diawasi Bank Indonesia. Lembaran Negara Republik Indonesia Tahun 2024 Nomor 9/BI. https://peraturan.bpk.go.id/Details/301533/peraturan-bi-no-2-tahun-2024
[22] 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

NOMENCLATURE

$\bar{kl}$	Sub-category score
$\sum_{i=1}^{l} k_i$	Sum of all control scores in the related sub-category
l	Number of controls in the related sub-category
$\bar{K}_l$	Cybersecurity Maturity Score of the Category
$\sum_{i=1}^{m} \bar{k}_l$	Sum of all sub-category scores in the related Category
m	Number of sub-categories in the related Category
$M_I/M_P/M_D/M_R$	Cybersecurity Maturity of the Identification/Protection/Detection/Mitigation and Recovery Domain
$\sum_{i=1}^{n} \bar{K}_l$	Sum of all Cybersecurity Maturity Scores of the Categories in the related Domain
n	Number of Categories in the related Domain
M_T	Cybersecurity Maturity of All Domains/Total