Eduvest – Journal of Universal Studies
Volume 6 Number 7, July, 2026
p- ISSN 2775-3735- e-ISSN 2775-3727

Development of the Risk-Weighted Cybersecurity Maturity Index (RWCMI) Based on the NIST Cybersecurity Framework 2.0 for Multi-Entity Organizations

Ekky Cahya Dhitia, Ahmad Muklason
Institut Teknologi Sepuluh Nopember, Indonesia
Email: ekkycahyadhitia@gmail.com, muklason@its.ac.id

Keywords
cybersecurity maturity;
risk-weighted maturity index;
NIST Cybersecurity Framework;
cybersecurity risk;
multi-entity organization.

ABSTRACT
The rapid growth of digital transformation has increased organizational dependence on interconnected technologies while simultaneously expanding cybersecurity risks, particularly in multi-entity organizations with diverse operational characteristics and information system environments. Conventional cybersecurity maturity assessments often provide general capability measurements but have limitations in representing variations in risk exposure across security domains. This study aims to develop the Risk-Weighted Cybersecurity Maturity Index (RWCMI) based on the NIST Cybersecurity Framework (CSF) 2.0 to provide a more contextual measurement of cybersecurity maturity by integrating risk weighting into the maturity assessment process. This research employed a quantitative, model-based evaluation approach using a case study of PTPN Group, consisting of one holding company and ten subsidiaries. Data were collected through cybersecurity maturity questionnaires, expert-based risk assessments, and supporting organizational documents. The RWCMI model integrates maturity scores from 22 NIST CSF 2.0 categories with normalized risk weights derived from expert judgments. The results indicate variations in cybersecurity maturity levels among entities, with several organizations achieving targeted maturity levels while others requiring fundamental improvements. The RWCMI approach successfully identified priority improvement areas, particularly in asset management, data security, identity management, and cybersecurity governance. In conclusion, RWCMI provides a more risk-sensitive cybersecurity maturity measurement framework that supports strategic decision-making, investment prioritization, and continuous improvement of cybersecurity governance in multi-entity organizations.

INTRODUCTION

Digital transformation over the last decade has driven cross-sector organizations to adopt technologies such as cloud computing, the Internet of Things (IoT), data analytics, and cross-functional system integration to improve operational efficiency and decision-making quality. However, increased system connectivity and dependence on digital services have also expanded the attack surface and increased the potential for operational disruptions, data breaches, and economic losses caused by cyber incidents (Romanosky, 2016; ENISA, 2023; World Economic Forum, 2023). The concept of cybersecurity is no longer limited to

information protection but has expanded to include the broader protection of digital assets within cyberspace, requiring a more strategic management approach (Von Solms & Van Niekerk, 2013). Cybersecurity has evolved from the traditional concept of information security into a broader discipline encompassing the protection of digital infrastructure, network systems, applications, and data within an interconnected cyber environment. As organizations become increasingly dependent on digital technologies, cybersecurity is no longer viewed solely as a technical concern but as a strategic issue related to enterprise-wide risk management (Von Solms & Van Niekerk, 2013). Therefore, organizations require cybersecurity governance approaches capable of integrating risk management, security policies, and strategic decision-making in a structured manner.

The challenges of managing cybersecurity have become increasingly complex in multi-entity organizations, which consist of multiple operational units or entities with diverse business processes and information system characteristics. Differences in business processes, levels of digitalization, and information technology architectures among entities can increase the complexity of cybersecurity management at the organizational level. This condition may lead to variations in cybersecurity posture and risk exposure among entities, creating an imbalance of risk across the organization. Furthermore, complex and distributed technology environments create challenges in maintaining consistency in security policies and implementing security controls across organizational entities (ENISA, 2023; Von Solms & Van Niekerk, 2013).

To support systematic cybersecurity management, various standards and frameworks have been developed. ISO/IEC 27001 is an international standard widely used for implementing an Information Security Management System (ISMS), emphasizing a process-based management approach and continuous improvement in information security management (ISO, 2022). In addition, COBIT 2019 provides an information technology governance and management framework designed to align business objectives with effective IT management (ISACA, 2019). Although both frameworks provide comprehensive governance structures, studies indicate that the implementation of information security standards is often compliance-oriented and may not fully support dynamic cybersecurity risk prioritization processes (Culot et al., 2021). As a more flexible and risk-oriented approach, the NIST Cybersecurity Framework (CSF) was developed to help organizations systematically identify, protect, detect, respond to, and recover from cybersecurity threats. The framework provides functions, categories, and subcategories that organizations can use to assess their current cybersecurity posture (current profile) and define their desired future state (target profile). The latest version, NIST Cybersecurity Framework 2.0, expands the framework by introducing Govern as a core function to strengthen cybersecurity governance and its integration into organizational strategic decision-making (NIST, 2024).

In line with the need to evaluate cybersecurity capabilities, various cybersecurity maturity models have been developed to help organizations assess cybersecurity implementation maturity levels and identify areas requiring improvement. Maturity models are generally used to measure cybersecurity capability levels across progressive stages and provide guidance for continuous capability enhancement. However, several studies indicate that many maturity models still apply uniform aggregation or weighting approaches across security domains, making them less sensitive to variations in risk levels among specific security areas

\

(Rabii et al., 2020; Büyüközkan & Güler, 2025). Such uniform weighting approaches become increasingly problematic in multi-entity organizations because risk exposure levels and potential impacts may differ significantly among entities and security domains. Without considering risk priorities, cybersecurity maturity assessment results tend to remain descriptive and provide limited support for strategic cybersecurity investment decisions. This condition highlights a research gap in developing cybersecurity maturity evaluation models capable of simultaneously integrating risk dimensions and maturity measurements. Therefore, a cybersecurity maturity assessment approach that combines security control maturity levels with risk-based weighting is required to produce evaluation results that better represent actual organizational risk conditions.

Based on these conditions, this study developed the Risk-Weighted Cybersecurity Maturity Index (RWCMI) based on the NIST Cybersecurity Framework 2.0 as an approach to measuring cybersecurity maturity while incorporating risk weights across security domains. This approach integrates maturity assessments based on the NIST CSF 2.0 category and subcategory structure with risk weights derived from expert judgments, producing a composite index that better represents organizational strategic risk priorities. Thus, this research contributes methodologically to the development of risk-based cybersecurity maturity measurement approaches and supports organizations in aligning cybersecurity implementation capabilities with prioritized risks in a more targeted manner.

This research focuses on three main problems: determining risk weights for NIST CSF 2.0 categories in the context of multi-entity organizations, measuring cybersecurity maturity levels across entities, and integrating these components into the Risk-Weighted Cybersecurity Maturity Index (RWCMI) to evaluate alignment between risk exposure and cybersecurity capabilities. To address these problems, this study aims to determine the relative risk weights of each category through expert judgment, measure cybersecurity maturity based on the NIST CSF 2.0 structure, develop RWCMI as a composite index that reflects maturity adjusted for risk exposure, and analyze the alignment between cybersecurity priorities and implementation capabilities to support strategic decision-making. Theoretically, this study contributes to the cybersecurity evaluation literature by introducing a more contextual risk-weighting approach compared with conventional maturity models. Practically, RWCMI is expected to serve as an evaluation instrument for multi-entity organizations, particularly holding companies, to compare cybersecurity maturity among entities, determine investment priorities, and formulate cybersecurity strengthening strategies in a more objective and adaptive manner.

METHOD

Research Approach and Design

This study employed a quantitative approach with a model-based evaluation design applied to a case study of a multi-entity organization, namely PTPN Group, consisting of PT Perkebunan Nusantara III (Persero) as the holding company and its 10 subsidiaries. The study focused on developing the Risk-Weighted Cybersecurity Maturity Index (RWCMI), which measured organizational cybersecurity maturity while incorporating risk levels across security control domains.

Data Collection

Data is collected through two main paths. First, a maturity assessment questionnaire filled out by employees in each entity related to information technology and cybersecurity management — they assess the extent to which cybersecurity practices have been implemented using a scale of 1 to 5, ranging from unstructured to continuously improved. Second, risk assessment by an expert judgement — at the holding level involving 6 experts, while at each subsidiary there are at least 2 people — who are tasked with assessing the likelihood and impact of cybersecurity risks in each control area. These two types of data are then combined to generate RWCMI values. In addition, internal organizational documents such as security policies, audit reports, and risk management documents are used as supporting data.

Frameworks Used

All measurements refer to the NIST Cybersecurity Framework (CSF) 2.0, which divides cybersecurity management into 22 categories under six main functions: Govern, Identify, Protect, Detect, Respond, and Recover. Each of these categories is the smallest unit in maturity assessment and risk assessment.

How to Calculate RWCMI

Broadly speaking, the calculation process is carried out through the following steps.

1. The maturity score is calculated per category based on the average of respondents' answers, and then aggregated to the function and entity levels.
2. The risk score is determined not by direct multiplication, but rather by mapping the probability and impact values of the experts into the organization's internal risk map, resulting in a number between 1 and 25.
3. The risk score of each category is averaged from all expert assessments, then normalized to a relative risk weight so that the total reaches 100%.
4. The RWCMI value is obtained by multiplying the risk weight and maturity score in each category, then adding them all together — so that the high-risk category automatically contributes more to the final index.

Data Analysis

The results of the study were analyzed from four perspectives: the actual maturity level of each entity, the distribution of risk weight, the comparison of RWCMI values between entities, and the gap analysis between risk and maturity. This gap is used to classify each category into four priority statuses — Improvement, Retained, Needs to Improve, and Controlled — based on a combination of high risk and whether the maturity score meets the set targets. Cross-entity analysis does not produce a single aggregate value for the entire group, but rather compares and synthesizes the results of each company to find common patterns and priorities.

RESULT AND DISCUSSION

Results of Conventional Cyber Maturity Measurement

Conventional cyber maturity measurements are conducted to obtain an initial picture of the level of cybersecurity implementation in each entity before considering the weight of risk. Conventional maturity values are calculated based on the average maturity score in 22 NIST CSF 2.0 categories. In this study, the maturity target used was 3.00.

\

The results of conventional cyber maturity measurements in 11 entities are presented in Table 1.

Table 1 Conventional Cyber Maturity Value by Entity

Peringkat	Entities	Maturity Konvensional	Gap to Target 3.00	Remarks
1	PT Perkebunan Nusantara I	4,76	1,76	Above target
2	PT Perkebunan Nusantara IV	3,69	0,69	Above target
3	PT Perkebunan Nusantara III (Persero) / Holding	3,64	0,64	Above target
4	PT Sinergi Gula Nusantara	3,62	0,62	Above target
5	PT Riset Perkebunan Nusantara	3,49	0,49	Above target
6	PT LPP Agro Nusantara	2,99	-0,01	Close to the target
7	PT Kharisma Joint Marketing Nusantara	2,68	-0,32	Below target
8	PT Rumah Sakit Sri Pamela Medika Nusantara	1,24	-1,76	Below target
9	PT Industri Karet Nusantara	1,13	-1,87	Below target
10	PT Kawasan Industri Nusantara	0,86	-2,14	Below target
11	PT Bio Industri Nusantara	0,43	-2,57	Below target

Based on Table 1, there are five entities that already have a conventional maturity value above the target of 3.00, namely PTPN I, PTPN IV, PTPN III (Persero) / Holding, PT SGN, and PT RPN. These achievements show that the implementation of cybersecurity practices in the five entities has generally been at a formal, documented, and relatively consistent level. PT LPP Agro Nusantara has a maturity value of 2.99, so it can be categorized as an entity that is close to the target. This value shows that most cybersecurity practices have begun to be implemented, but there are still areas that need to be strengthened to achieve the minimum maturity target.

Meanwhile, five other entities are still below the target, namely PT KPBN, PT SPMN, PT KINRA, PT IKN, and PT BIN. The low maturity value in this group shows that the implementation of cybersecurity practices still needs improvement, especially in the aspects of policy formality, consistency in the implementation of controls, documentation, and monitoring and evaluation mechanisms. In general, the results of conventional maturity measurements show that there are variations in the level of cybersecurity readiness between entities. This variation reinforces PTPN Group's characteristics as a multi-entity organization, where each company has a different level of cybersecurity implementation. However, conventional maturity values have not taken into account the relative level of risk in each category. Therefore, these results are then compared with the Risk-weighted Cybersecurity Maturity Index (RWCMI) value to obtain a more contextual picture of the maturity of each entity's risk profile.

Results of the Risk-weighted Cybersecurity Maturity Index (RWCMI)

The calculation of the Risk-weighted Cybersecurity Maturity Index (RWCMI) was performed by integrating the actual maturity score and risk weight in each NIST CSF 2.0 category. In contrast to conventional maturity that uses simple averages, RWCMI takes into account the relative importance level of each category based on the normalized risk weight.

In this study, the RWCMI value is calculated using the following equations:

$$RWCMI = \sum(W_i \times M_i)$$

With W_i is the risk weight of category I and M_i is the actual maturity score of category I. Because the total risk weight on each entity is 100%, the value of RWCMI remains in the maturity scale range of 1 to 5.

The results of the RWCMI calculation on 11 entities are presented in Table 2.

Table 2 RWCMI Value and Gap to Target 3.00

Peringkat	Entitas	RWCMI	Gap to Target 3.00	Status Target
1	PT Perkebunan Nusantara I	4,78	1,78	Above target
2	PT Perkebunan Nusantara IV	3,67	0,67	Above target
3	PT Sinergi Gula Nusantara	3,62	0,62	Above target
4	PT Perkebunan Nusantara III (Persero) / Holding	3,61	0,61	Above target
5	PT Riset Perkebunan Nusantara	3,47	0,47	Above target
6	PT LPP Agro Nusantara	2,95	-0,05	Close to the target
7	PT Kharisma Joint Marketing Nusantara	2,68	-0,32	Below target
8	PT Rumah Sakit Sri Pamela Medika Nusantara	1,23	-1,77	Below target
9	PT Industri Karet Nusantara	1,21	-1,79	Below target
10	PT Kawasan Industri Nusantara	0,91	-2,09	Below target
11	PT Bio Industri Nusantara	0,44	-2,56	Below target

Based on Table 2, there are five entities that have an RWCMI value above the target of 3.00, namely PTPN I, PTPN IV, PT SGN, PTPN III (Persero) / Holding, and PT RPN. This achievement shows that the level of cybersecurity maturity in the five entities has relatively met the target after adjusting for the risk weight in each category. The highest RWCMI score obtained by PTPN I was 4.78. This achievement shows that PTPN I has the highest level of risk-based cybersecurity maturity compared to other entities. Meanwhile, PTPN IV, PT SGN, PTPN III (Persero) / Holding, and PT RPN were also above the target, with RWCMI values in the range of 3.47 to 3.67.

PT LPP Agro Nusantara obtained an RWCMI value of 2.95, so it is categorized as close to the target. This value indicates that the entity's cybersecurity maturity level is close to the set minimum limit, but there are still certain categories that need to be improved to reach the target of 3.00. On the other hand, there are five entities with RWCMI values below the target, namely PT KPBN, PT SPMN, PT KINRA, PT IKN, and PT BIN. The lowest RWCMI value was found at PT BIN at 0.44, followed by PT IKN at 0.91, PT KINRA at 1.21, and PT SPMN at 1.23. This condition shows that some entities still need fundamental strengthening in the implementation of cybersecurity practices.

In general, the results of RWCMI show that there is a variation in the level of risk-based cybersecurity maturity between entities. These variations indicate that the cybersecurity readiness of the PTPN Group is not evenly distributed. Therefore, the RWCMI value can be used as a basis for identifying entities that need priority upgrades, especially in categories that have a high risk weight but whose maturity level is still below the target.

\

Comparative Analysis of Conventional Maturity and RWCMI

A comparative analysis between conventional maturity and the Risk-weighted Cybersecurity Maturity Index (RWCMI) was conducted to see the effect of risk weighting on the results of cybersecurity maturity measurement. Conventional maturity is calculated using the average maturity score of all categories, while RWCMI is calculated by considering the risk weights of each category. Comparison of conventional maturity values and RWCMI in 11 entities is presented in Table 3.

Table 3 Comparison of Conventional and RWCMI Maturity

No	Entitas	Maturity Konvensional	RWCMI	Selisih RWCMI - Maturity	Interpretasi
1	PT Perkebunan Nusantara III (Persero) / Holding	3,64	3,61	-0,02	RWCMI is slightly lower
2	PT Perkebunan Nusantara I	4,76	4,78	0,02	RWCMI is slightly higher
3	PT Perkebunan Nusantara IV	3,69	3,67	-0,01	RWCMI is slightly lower
4	PT Sinergi Gula Nusantara	3,62	3,62	0,00	Relatively the same
5	PT Kharisma Joint Marketing Nusantara	2,68	2,68	0,00	Relatively the same
6	PT Riset Perkebunan Nusantara	3,49	3,47	-0,02	RWCMI is slightly lower
7	PT LPP Agro Nusantara	2,99	2,95	-0,04	Lower RWCMI
8	PT Industri Karet Nusantara	1,13	1,21	0,08	RWCMI is higher
9	PT Rumah Sakit Sri Pamela Medika Nusantara	1,24	1,23	-0,01	RWCMI is slightly lower
10	PT Kawasan Industri Nusantara	0,86	0,91	0,05	RWCMI is higher
11	PT Bio Industri Nusantara	0,43	0,44	0,01	RWCMI is slightly higher

Based on Table 3, most entities show a relatively small difference between conventional maturity values and RWCMIs. This condition suggests that the distribution of maturity scores in some entities is relatively balanced to the distribution of their risk weight. Nonetheless, the difference in values remains analytically important because it shows the effect of risk weighting on the maturity aggregation results. Entities with lower RWCMI values than conventional maturity are PTPN III (Persero) / Holding, PTPN IV, PT RPN, PT LPP Agro Nusantara, and PT SPMN. This condition indicates that the category with a higher risk weight in the entity tends to have a relatively lower maturity score than the other categories. Thus, there is a need to strengthen categories that have a greater risk contribution to an entity's cybersecurity profile. On the other hand, PTPN I, PT KINRA, PT IKN, and PT BIN have higher RWCMI values than conventional maturity. This suggests that the category with a higher risk weight in the entity relatively has a slightly better maturity score than the other category. However, this interpretation needs to be read together with the absolute value of RWCMI. In PT KINRA, PT

IKN, and PT BIN, although RWCMI is higher than conventional maturity, the index value is still below the target of 3.00 so it still needs to be improved overall.

Meanwhile, PT SGN and PT KPBN show relatively the same conventional maturity value and RWCMI. This condition indicates that the contribution of risk weight does not result in a significant change in the aggregate value of maturity, so that the distribution of maturity in the high-risk category and the other categories is relatively balanced. In general, this comparison shows that RWCMI provides additional perspective compared to conventional maturity measurements. Conventional maturity values provide an overview of the level of cybersecurity implementation, while RWCMI shows how the maturity achievement changes when adjusted for the relative risk level in each category. Thus, RWCMI can be used to assess the alignment between cybersecurity capabilities and risk priorities in each entity.

Results of Classification of Priority Status Improvement

An upgrade priority status classification was performed to identify cybersecurity categories that needed to be prioritized based on a combination of risk weight and actual maturity score. In this study, the category with a risk weight that was at or above the 75th percentile (P75) was categorized as a high-risk group. Meanwhile, the actual maturity score is compared to the maturity target of 3.00. Based on the combination of these two criteria, each NIST CSF 2.0 category is classified into four statuses, namely Improvement Priority, Maintain, Need to Improve, and Controlled. The criteria for the classification of priority status of the upgrade are presented in Table 4.

Table 4 Criteria for Classification of Priority Status of Improvement

Conditions	Criteria	Status	Interpretive Meaning
High risk and maturity have not met targets	Risk weight ≥ P75 and maturity < 3.00	Improvement Priorities	The category has a relatively high risk, but the level of maturity is not adequate.
High risk and maturity meet targets	Risk weight ≥ P75 and maturity ≥ 3.00	Maintain	The category has a relatively high risk and the level of maturity has met the target, so it is necessary to maintain consistency.
The risk is not yet high and the maturity has not met the target	Risk weight < P75 and maturity < 3.00	Needs to Be Improved	The category still needs improvement, even if it doesn't include the highest risk group.
Risks are not yet included in the high and maturity of meeting the target	Risk weight < P75 and maturity ≥ 3.00	Controlled	The category has met the maturity target and does not include the highest risk group.

The results of the priority status classification of 11 entities are presented in Table 5.

Table 5 Priority Status Distribution by Entity

Yes	Entities	Improvement Priorities	Maintain	Needs to Be Improved	Controlled
1	PT Perkebunan Nusantara III (Persero) / Holding	1	5	0	16
2	PT Perkebunan Nusantara I	0	6	0	16
3	PT Perkebunan Nusantara IV	0	7	0	15

\

4	PT Sinergi Gula Nusantara	0	9	0	13
5	PT Kharisma Joint Marketing Nusantara	5	1	11	5
6	PT Riset Perkebunan Nusantara	0	7	0	15
7	PT LPP Agro Nusantara	3	3	8	8
8	PT Industri Karet Nusantara	6	0	16	0
9	PT Rumah Sakit Sri Pamela Medika Nusantara	6	0	16	0
10	PT Kawasan Industri Nusantara	9	0	13	0
11	PT Bio Industri Nusantara	6	0	16	0

Based on Table 5, there are four entities that do not have a category with Priority Repair status, namely PTPN I, PTPN IV, PT SGN, and PT RPN. This condition indicates that the high-risk category of the entity already has a level of maturity that meets the target. Therefore, the high-risk category in that group of entities is more in the Maintain state. PTPN III (Persero) / Holding has one category with Repair Priority status and five categories with Maintain status. This shows that in general, the high-risk category in holding has adequate maturity, although there is still one area that needs to be the focus of improvement.

The entity with the highest number of Improvement Priorities is PT Kawasan Industri Nusantara, which is 9 categories. This condition shows that there is a considerable mismatch between the weight of risk and the level of maturity in several cybersecurity categories. In addition, PT KINRA, PT SPMN, and PT BIN each have 6 Priority Repair categories, while PT KPBN has 5 categories and PT LPPAN has 3 categories. In addition to the Repair Priority category, the Need to Improve status is also important to note. PT KINRA, PT SPMN, and PT BIN each have 16 categories with Need to Improve status. This shows that although not all categories are included in the highest risk groups, the maturity level in most categories is still below the target. As such, these entities require a more fundamental and comprehensive upgrade. In general, the results of the priority status classification show that risk-based and maturity-based analysis is able to distinguish between areas that need to be prioritized immediately and those that need to be improved gradually. The category with the status of Improvement Priority is the main focus because it has a high risk weight and has not reached the maturity target. Meanwhile, the category with the status of Maintain needs to be maintained because it has met the target in areas with a relatively high risk.

To strengthen the priority analysis, the results of the classification are then analyzed based on the frequency of occurrence of the category as Improvement Priority across entities. This analysis aims to identify cybersecurity categories that have a pattern of recurring problems in several entities, so that it can be the basis for prioritizing improvements at the group level. The results of the analysis are presented in Table 6.

Table 6 Most Frequently Prioritized Categories for Improvement

No	Category	Entity Frequency	Related Entities	Implications
1	ID.AM - Asset Management	4	PT LPPAN, PT IKN, PT KINRA, PT BIN	Strengthening inventory and IT asset management is an important foundation to support other security controls.
2	GV.OC - Organizational Context	3	PT KPBN, PT IKN, PT SPMN	Cybersecurity needs to be more aligned with the context of organizations, business processes, and reliance on digital services.
3	GV. SC - Cybersecurity Supply Chain Risk Management	3	PT KPBN, PT IKN, PT SPMN	Risk management of third parties, vendors, and external services needs to be strengthened.
4	PR.DS - Data Security	3	PT KPBN, PT IKN, PT SPMN	Data protection needs to be strengthened, both in terms of confidentiality, integrity, and availability.
5	PR. AA - Identity Management, Authentication, and Access Control	3	PT IKN, PT SPMN, PT KINRA	Access control and user identity management need to be an improvement priority.
6	GV.RM - Risk Management Strategy	2	PT KPBN, PT LPPAN	Cybersecurity risk management strategies need to be clarified and integrated into organizational governance.
7	ID.RA - Risk Assessment	2	PT LPPAN, PT SPMN	Mechanisms for identifying, analyzing, and evaluating cybersecurity risks need to be improved.
8	GV. RR - Roles, Responsibilities, and Authority	2	PT IKN, PT BIN	The role and accountability of cybersecurity needs to be formulated more clearly.
9	GV. PO - Policy	2	PT IKN, PT BIN	Cybersecurity policies need to be strengthened as a basis for formal control.
10	GV. OV - Surveillance	2	PT IKN, PT BIN	The mechanism for monitoring and evaluating cybersecurity needs to be improved.
11	RC. RP - Incident Recovery Plan Implementation	2	PT SPMN, PT BIN	Service recovery readiness after cybersecurity incidents needs to be strengthened.
12	DE. AE - Adverse Event Analysis	2	PT KINRA, PT BIN	The ability to analyze cybersecurity incidents needs to be improved.

Comparative Analysis Between Entities

A comparative analysis between entities was conducted to obtain an overview of the variation in the level of cybersecurity maturity, RWCMI value, risk distribution, and priority status of improvement in 11 PTPN Group entities. This analysis is important because the research was conducted on multi-entity organizations that have different operational characteristics, levels of digitalization, and risk profiles.

\

A summary of the comparison between entities is presented in Table 7.

Table 7 Comparative Matrix Between Entities

Yes	Entitas	Maturity Konvensional	RW CMI	Risk Dominance	Improvement Priorities	General Interpretation
1	PT Perkebunan Nusantara I	4,76	4,78	Moderate	0	Very high maturity and high-risk categories have met the target.
2	PT Perkebunan Nusantara IV	3,69	3,67	Low to Moderate	0	Maturity above target with a relatively lower risk profile.
3	PT Sinergi Gula Nusantara	3,62	3,62	Moderate to High dan High	0	Maturity meets targets despite a relatively high risk profile.
4	PT Perkebunan Nusantara III (Persero) / Holding	3,64	3,61	High	1	Maturity is above target, but there is still one high-risk area that needs improvement.
5	PT Riset Perkebunan Nusantara	3,49	3,47	Moderate to High	0	Maturity above target with relatively high risk categories has been controlled.
6	PT LPP Agro Nusantara	2,99	2,95	Low to Moderate dan Moderate	3	Close to the target, but still has several priority categories for improvement.
7	PT Kharisma Joint Marketing Nusantara	2,68	2,68	Moderate	5	below target and has several high-risk categories with low maturity.
8	PT Rumah Sakit Sri Pamela Medika Nusantara	1,24	1,23	Moderate to High	6	Low maturity with a relatively high risk profile, so it requires fundamental improvement.
9	PT Industri Karet Nusantara	1,13	1,21	Low	6	Maturity is low even though the risk distribution is relatively low, so it needs to strengthen the foundation.
10	PT Kawasan Industri Nusantara	0,86	0,91	Moderate	9	Maturity is very low and has the highest number of repair priorities.
11	PT Bio Industri Nusantara	0,43	0,44	Low	6	Maturity is lowest and requires a thorough upgrade to basic cybersecurity controls.

Based on Table 7, there are quite clear differences between entities. PTPN I showed the highest achievements, both in the conventional maturity value and RWCMI. This entity also does not have a category with Repair Priority status, so it can be categorized as the entity with the strongest cybersecurity maturity conditions in the results of this study. The next group is entities with RWCMI values above the target, namely PTPN IV, PT SGN, PTPN III (Persero) / Holding, and PT RPN. This group shows that the relative level of cybersecurity maturity has met the target. However, the risk pattern is different. PT SGN and PTPN III have a higher risk

distribution than PTPN IV, so the risk management needs of both entities still need to be considered even though the RWCMI value is above the target.

PT LPP Agro Nusantara is in a position close to the target, with a RWCMI value of 2.95. This position indicates that the entity is in a transition phase towards the minimum maturity target. However, the existence of three Improvement Priority categories indicates that there are still high-risk areas that have not been supported by an adequate level of maturity.

Entities such as PT KPBN, PT SPMN, PT KINRA, PT IKN, and PT BIN are under the RWCMI target. This group needs more attention because the risk-based maturity value has not reached the minimum target. Among these groups, PT IKN has the highest number of Improvement Priorities, namely 9 categories, while PT BIN has the lowest RWCMI value of 0.44. This condition suggests that the priority of improvement needs to be seen not only from the value of the index, but also from the number of categories that have a mismatch between risk and maturity.

Analytically, the results of the comparison between entities can be grouped into three clusters. First, mature and relatively restrained entities, i.e. entities with RWCMI values above the target and low or no Improvement Priority amounts. Second, transition entities, which are entities that are close to targets but still have priority categories that need improvement. Third, entities with fundamental improvement needs, namely entities with RWCMI far below the target and many categories with maturity below the target.

The grouping is presented in Table 8.

Table 8 Inter-Entity Cybersecurity Maturity Cluster

Cluster	General Criteria	Entities	Implications
Mature and relatively controlled entities	RWCMI ≥ 3.00 and low or no Repair Priority	PTPN I, PTPN IV, PT SGN, PTPN III, PT RPN	Focus on maintenance, monitoring, and continuous improvement.
Transition entities	RWCMI is close to the target and still has some Improvement Priorities	PT LPPAN and PT KPBN	Focus on accelerating the fulfillment of maturity targets and the completion of high-risk categories.
Entities with fundamental improvement needs	RWCMI is well below target and many categories of low maturity	PT SPMN, PT KINRA, PT IKN, PT BIN	Focus on strengthening basic controls, governance, documentation, asset management, data security, and access control.

Based on Table 8, the differences between entities show that cybersecurity improvement strategies cannot be implemented uniformly. Mature entities require continuous reinforcement and monitoring of control consistency. Transition entities need targeted improvements to categories that are still below the target. Meanwhile, entities with fundamental improvement needs need a more comprehensive strengthening program, especially on basic cybersecurity controls. Thus, the results of inter-entity comparisons show that the RWCMI model can support multi-entity analysis in a more contextual manner. This model not only shows the maturity value of each entity, but also helps identify differences in risk profiles, readiness levels, and improvement priority needs in each company.

\

Discussion of Research Results

The results show that the Risk-weighted Cybersecurity Maturity Index (RWCMI) model can be used to evaluate cybersecurity maturity in multi-entity organizations by considering the risk dimensions in each NIST CSF 2.0 category. This model not only generates a cybersecurity maturity value, but also provides a basis for analyzing the suitability between the level of risk and cybersecurity capabilities of each entity. In general, the results of the study show that there are variations in maturity levels, risk weight, and priority of improvement between PTPN Group entities. Some entities already have a RWCMI value above the target of 3.00, while others are still below the target. This condition shows that the cybersecurity readiness of the PTPN Group is not fully evenly distributed, so an evaluation approach is needed that is able to capture differences in characteristics between entities.

The results also show that conventional maturity approaches are not yet fully sufficient to describe cybersecurity improvement priorities. Conventional maturity values provide an overview of the level of implementation of controls, but do not take into account the relative level of risk in each category. By integrating risk weights into maturity measurements, RWCMI provides more contextual results because higher-risk categories have a greater contribution to the final index value. In addition to generating index values, the RWCMI model also allows the classification of categories into Improvement, Retained, Needs to Improve, and Controlled Priority status. This classification provides more operational information because it is able to distinguish categories that have high risk but have not been supported by an adequate level of maturity. Thus, the results of the research are not only descriptive, but can also be used as a basis for determining cybersecurity improvement priorities at the entity and group level.

Conformity of Results with Research Design

The results of the study show that the stages designed in the research design have produced outputs that are in accordance with the development of the RWCMI model. The instrument development stage produced a measurement instrument based on NIST CSF 2.0 which included 6 functions, 22 categories, and 195 question items. The instrument is the basis for obtaining cybersecurity maturity data on each entity. The risk assessment stage through expert judgement produces a risk score and risk weight in each category. The risk score is obtained through probability and impact mapping based on the Organization's Internal Risk Map, then normalized to a total risk weight of 100% for each entity. These results show that the risk weight determination process has been carried out consistently in accordance with the methodology design.

The maturity measurement stage produces conventional maturity values on 11 entities. The measurement results show that there is a variation in the level of maturity between entities, ranging from entities that are already above the target to entities that still need fundamental strengthening. Furthermore, the integration between the maturity score and the risk weight results in the RWCMI value on each entity. The final stage in research design is realized through the analysis of the gap between risk and maturity. This analysis results in an upgrade priority status classification based on a combination of risk weights and actual maturity scores. Thus, all stages in the research design have produced interconnected outputs, ranging from instruments, risk scores, risk weights, maturity values, RWCMI values, to priority status of improvement.

Table 9 Suitability of Research Design and Research Results

Stages of Research Design	Research Output
Development of measurement instruments	NIST CSF 2.0-based instrument with 6 functions, 22 categories, and 195 question points
Data collection *Maturity assessment*	Cybersecurity maturity score for each entity
Expert judgement risk assessment	Risk score based on probability and impact mapped through the Organization's Internal Risk Map
Normalization of risk weights	Risk weighting per category with a total of 100% on each entity
Conventional maturity calculations	Conventional maturity values on 11 entities
RWCMI Calculation	Risk-based cybersecurity maturity index value in 11 entities
Risk and maturity gap analysis	Priority Status of Repair, Maintain, Need to Be Improved, and Controlled
Multi-entity analytics	Comparison of maturity, RWCMI, risk distribution, and improvement priorities between entities

Based on Table 9, the results of the study have followed the flow of research design systematically. Each stage produces an output that is used as input for the next stage. This suggests that the RWCMI model can be applied in a structured manner to evaluate the risk-based cybersecurity maturity in multi-entity organizations.

RWCMI's Contribution to the Conventional Maturity Approach

The results of the study show that RWCMI provides additional perspective compared to the conventional maturity approach. In the conventional approach, all cybersecurity categories are treated as having equal weight in the aggregation process. This approach can provide an overview of the level of implementation of controls, but it does not yet show whether the higher-risk categories have an adequate level of maturity.

Through RWCMI, the maturity score in each category is combined with the risk weight obtained through expert judgement. Thus, categories with a higher risk weight will contribute more to the final index value. This approach makes the measurement results more sensitive to the risk profile of each entity. A comparison between conventional maturity and RWCMI shows that in some entities, RWCMI values are lower than conventional maturity. This condition indicates that the high-risk weight category still has a relatively lower maturity score than the other categories. In contrast, in certain entities, RWCMI values were higher than conventional maturity, suggesting that categories with a relative high risk weight had better maturity achievements.

Thus, RWCMI's main contribution lies in its ability to link the level of implementation of cybersecurity controls to the level of relative risk. RWCMI not only answers the question of how mature an entity's cybersecurity is, but also shows whether it has been in the areas most relevant to the organization's risk profile.

Practical Implications for PTPN Group's Cybersecurity Governance

The results of the study provide several practical implications for PTPN Group's cybersecurity governance, namely

1. The results of RWCMI can be used by the holding to obtain a comparative picture of the level of cybersecurity maturity in each entity. With the RWCMI value, the holding can

\

identify entities that have met the target, entities that are close to the target, and entities that still need fundamental improvement.

2. The results of the priority status classification can be used to determine more targeted areas of improvement. Categories with Improvement Priority status need to be the main focus because they show a mismatch between high risk and inadequate maturity. Meanwhile, categories with Maintain status still need to be maintained because they have a high risk even though they have met the maturity target.
3. A pattern of categories that often appear as Improvement Priorities across entities can be the basis for the preparation of cybersecurity programs at the group level. Findings such as ID.AM - Asset Management, GV. SC - Supply Chain Risk Management Cybersecurity, PR.DS - Data Security, and PR. AA - Identity Management, Authentication, and Access Control indicates that the upgrade priorities are not only related to technical aspects, but also to governance, data protection, access management, and third-party management.
4. The results of the research can support the preparation of a roadmap for improving cybersecurity that is more risk-based. Entities with RWCMI values above target can be directed to continuous reinforcement and monitoring of control effectiveness. Entities that are close to the target need acceleration in priority categories. Meanwhile, entities with RWCMI well below target need fundamental strengthening, especially in terms of policy, documentation, asset management, access control, and incident response and recovery readiness.

Thus, RWCMI can be used as an instrument to support decision-making in PTPN Group's cybersecurity governance. This model helps organizations not only see the level of maturity in the aggregate, but also determine improvement priorities based on the relationship between cybersecurity risk and capabilities.

CONCLUSION

This study concludes that the Risk-Weighted Cybersecurity Maturity Index (RWCMI) is a cybersecurity maturity evaluation model that integrates security control maturity levels with risk weighting based on the NIST Cybersecurity Framework (CSF) 2.0, resulting in a more proportionate assessment approach for multi-entity organizations. The implementation of RWCMI across 11 PTPN Group entities demonstrated variations in cybersecurity maturity levels, with some entities achieving the targeted maturity level while others still requiring improvement, particularly in the asset management (ID.AM) category, which emerged as a top priority. The results indicate that RWCMI can assist organizations in identifying improvement priorities, comparing cybersecurity readiness among entities, and supporting risk-based cybersecurity decision-making. Therefore, this model is recommended as an instrument for continuous evaluation and monitoring to strengthen cybersecurity governance in a more effective manner and align security improvements with the risk profile of each entity.

REFERENCES

Aguilera, R. V., Judge, W. Q., & Terjesen, S. A. (2015). Corporate governance and multinational enterprises. *Academy of Management Annals, 9*(1), 483–531. https://doi.org/10.1080/19416520.2015.1024505

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their

foundation. *European Journal of Operational Research, 253*(1), 1–13. https://doi.org/10.1016/j.ejor.2015.12.023

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. *Long Range Planning, 48*(4), 265–276. https://doi.org/10.1016/j.lrp.2014.07.005

Büyüközkan, G., & Güler, M. (2025). Cybersecurity maturity model: Systematic literature review and a proposed model. *Technological Forecasting and Social Change, 213*, Article 123996. https://doi.org/10.1016/j.techfore.2025.123996

Cortez, E. (2022). Cybersecurity governance: Aligning cybersecurity with corporate governance frameworks. *Journal of Cyber Policy, 7*(2), 249–266. https://doi.org/10.1080/23738871.2022.2032464

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. *The TQM Journal, 33*(7), 76–105. https://doi.org/10.1108/TQM-09-2020-0202

European Union Agency for Cybersecurity. (2023). *ENISA threat landscape 2023*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Hubbard, D. W., & Seiersen, R. (2016). *How to measure anything in cybersecurity risk*. John Wiley & Sons.

ISACA. (2019). *COBIT 2019 framework: Governance and management objectives*. ISACA.

International Organization for Standardization. (2018). *ISO 31000:2018 risk management—Guidelines*.

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 information security, cybersecurity and privacy protection—Information security management systems—Requirements*.

Modi, C., Kuzminykh, I., & Ghita, B. (2023). Cybersecurity governance: A systematic literature review of governance mechanisms and organizational capabilities. *Computers & Security, 124*, Article 102992. https://doi.org/10.1016/j.cose.2022.102992

Modi, R., Kuzminykh, A., & Ghita, B. (2023). Cybersecurity metrics for governance decision-making: A systematic perspective. *Computers & Security, 129*, Article 103221. https://doi.org/10.1016/j.cose.2023.103221

National Institute of Standards and Technology. (2018). *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy* (SP 800-37 Rev. 2). https://doi.org/10.6028/NIST.SP.800-37r2

National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0*. https://doi.org/10.6028/NIST.CSWP.29

Power, M. (2007). *Organized uncertainty: Designing a world of risk management*. Oxford University Press.

Rabii, A., Assoul, S., Touhami, O., & Roudies, O. (2020). Information and cyber security maturity models: A systematic literature review. *Information & Computer Security, 28*(4), 627–644. https://doi.org/10.1108/ICS-03-2019-0039

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity, 2*(2), 121–135. https://doi.org/10.1093/cybsec/tyw001

Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal, 28*(13), 1319–

\

1350. https://doi.org/10.1002/smj.640

Turel, O., Liu, P., & Bart, C. (2019). Board-level information technology governance effects on organizational performance. *European Journal of Information Systems, 28*(3), 321–337. https://doi.org/10.1080/0960085X.2019.1567025

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Weill, P., & Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business School Press.

Wiley, J. (2024). Adaptive cybersecurity maturity models for organizations with resource constraints. *Journal of Cybersecurity and Privacy, 4*(1), 45–62. https://doi.org/10.1002/isd2.12350

World Economic Forum. (2023). *Global cybersecurity outlook 2023*. https://www.weforum.org/publications/global-cybersecurity-outlook-2023

Yeoh, W., Liu, M., Shore, M., & Jiang, F. (2023). Zero trust cybersecurity: Critical success factors and a maturity assessment framework. *Computers & Security, 132*, Article 103412. https://doi.org/10.1016/j.cose.2023.103412

Yeoh, W., Wang, S., Popovič, A., & Chowdhury, N. H. (2022). A systematic synthesis of critical success factors for cybersecurity. *Computers & Security, 118*, Article 102724. https://doi.org/10.1016/j.cose.2022.102724