Journal of Arabian Peninsula Centre for Medical and Applied Researches
Volume (1), Issue (4), year/2026
p: 55-79

ISSN/E: 2959-829X || ISSN/P:2059-8303

مجلة مركز جزيرة العرب
للبحوث الطبية والتطبيقية
المجلد (1)، العدد (4)، العام 2026م
ص: 55-79
Received: May 12, 2026 || Accepted: June 01, 2026 ||
Published: June 2, 2026

The Proposed CyPro-CMMI Cybersecurity Maturity Integration Framework [1]

إطار مقترح لدمج نضج الأمن السيبراني CyPro-CMMI [2]

Ms. Enaam Abd Elgader Abd Alla Farh — أ. إنعام عبد القادر عبد الله فرح
College of Computer Science and Information Technology ||Al-Neelain University|| Sudan — كلية علوم الحاسوب وتقنية المعلومات|| جامعة النيلين|| السودان
Email: angamabdo99@gmail.com || Orcid: https://orcid.org/0009-0004-0697-695X || Mobile: 00966555853281

Prof. Dr/ Mudawi Mukhtar Elmusharaf — أ.د/ مضوي مختار المشرف
College of Computer Science and Information Technology ||The National Ribat University||Sudan — كلية علوم الحاسب وتقنية المعلومات|| جامعة الرباط الوطني|| السودان
Email: mudawi5@gmail.com||Orcid: https://orcid.org/0000-0001-6424-0052 ||Mobile: 00249112021120

Dr. Tarig Abdalkarim Abdalfadil — د. طارق عبد الكريم عبد الفاضل
College of Computer Science and Information Technology ||Al-Neelain University||Sudan — كلية علوم الحاسوب وتقنية المعلومات|| جامعة النيلين|| السودان
Email: tarig.abdo@gmail.com || Orcid: https://orcid.org/0009-0009-4489-9701 || Mobile: 00966502427027

Dr. Omar Abdul Rahman Ali Ismil — د. عمر عبد الرحمن علي إسماعيل
College of Computer and Information System||Aloola Colleges Private||KSA — كلية الحاسب الآلي ونظم المعلومات||كليات الأولى الأهلية||المملكة العربية السعودية
Email: ismil8@gmail.com ||Orcid: https://orcid.org/000000027955668X ||Mobile: 00966565597751

Abstract: Contemporary cyber threats have grown more complex, extending beyond internal vulnerabilities to include cross-border risks tied to cloud computing, the Internet of Things (IoT), and emerging technologies. This study explores the feasibility of constructing a cybersecurity framework based on the principles of the Capability Maturity Model Integration (CMMI). Using an analytical approach, system requirements were examined in light of successful international experiences. Findings reveal that the CMMI model serves as an effective mechanism to strengthen institutional capabilities, efficiency, and discipline. The proposed CyPro-CMMI framework offers a structured path to integrate CMMI process improvement practices with globally recognized cybersecurity standards. Key adoption requirements include technical, human, and financial resources; policies and frameworks; education and capacity building; sound governance; collaboration with external organizations; and periodic reporting. The study recommends continuous monitoring of cybersecurity performance indicators to assess policy and procedure effectiveness, support evidence-based decisions, and reinforce a culture of ongoing improvement. This approach ensures operational resilience and the development of adaptive cybersecurity strategies.

Keywords: Cybersecurity, CMMI, Process Improvement, Proposed Framework.

المستخلص: أصبحت التهديدات السيبرانية المعاصرة أكثر تعقيدًا، إذ تجاوزت الثغرات الداخلية لتشمل مخاطر عابرة للحدود مرتبطة بالحوسبة السحابية، وإنترنت الأشياء (IoT)، والتقنيات الناشئة. تستكشف هذه الدراسة إمكانية بناء إطار للأمن السيبراني قائم على مبادئ نموذج تكامل نضج القدرات (CMMI). وباستخدام المنهج التحليلي، تم فحص متطلبات النظام استنادًا إلى التجارب الدولية الناجحة. أظهرت النتائج أن نموذج CMMI يُعد آلية فعّالة لتعزيز قدرات المؤسسات وكفاءتها وانضباطها. ويقدّم إطار CyPro-CMMI المقترح مسارًا منظّمًا لدمج ممارسات تحسين العمليات في CMMI مع المعايير العالمية المعترف بها للأمن السيبراني. وتشمل المتطلبات الرئيسة للتبني الموارد التقنية والبشرية والمالية، السياسات والأطر، التعليم وبناء القدرات، الحوكمة الرشيدة، التعاون مع المنظمات الخارجية، والتقارير الدورية. توصي الدراسة بضرورة المراقبة المستمرة لمؤشرات أداء الأمن السيبراني لتقييم فعالية السياسات والإجراءات، ودعم القرارات المبنية على الأدلة، وترسيخ ثقافة التحسين المستمر. يضمن هذا النهج مرونة العمليات وتطوير استراتيجيات أمن سيبراني تكيفية.

الكلمات المفتاحية: الأمن السيبراني، CMMI، تحسين العمليات، إطار مقترح.

[1]-**Citation in APA format**: Farh, I. A. Q., Elmusharaf, M. M., Abdalfadil, T. A. K., & Ismil, O. A. A. (2026). The proposed CyPro-CMMI cybersecurity maturity integration framework. *Journal of Arabian Peninsula Centre for Medical and Applied Researches, 1(4),* 55–79. https://doi.org/10.56793/pcra23143

[2]- **التوثيق للاقتباس (APA)**: فرح، إنعام عبد القادر.، المشرف، مضوي مختار.، عبد الفاضل، طارق عبد الكريم.، وإسماعيل، عمر عبد الرحمن. (2026). إطار مقترح لدمج نضج الأمن السيبراني CyPro-CMMI. *مجلة مركز جزيرة العرب للبحوث الطبية والتطبيقية، 1* (4)، 55- 79. https://doi.org/10.56793/pcra23143

1. Introduction

Capability Maturity Model Integration (CMMI) is a rigorous conventional methodology characterized by significant formalism and an emphasis on processes. Despite the advancements and faster development enabled by these methods, organizations acknowledge that quality sets them apart and therefore strive to preserve the excellence of their software products. CMMI is currently depicted as a reference model comprising a collection of practices to enhance organizational maturity, emphasizing process improvement and mitigating the risk of process failures to elevate quality (Morais, 2018). Implementing advanced cybersecurity capabilities enhances the organization's maturity in managing cyber risks. Risk levels rise in proportion to the growing number of individuals reliant on critical infrastructure. This is because the threat could have a bigger effect on more people (Ozkan & Spruit, 2019). The potential advantages of CCMMs are undermined when they are not appropriately adopted and implemented. Moreover, insufficient cybersecurity measures leave organizations exposed to evolving cyber threats. To increase the effectiveness of CCMMs, addressing these essential problems and ensuring they are flexible, realistic, and aligned with organizations' unique requirements and limitations is crucial (Liyanage et al., 2024).

1.2 Problem Statement:

Digital threats become more complex, companies should strengthen their cybersecurity mindset (Dornheim & Zarnekow, 2023). Using the MM as an extra strategy can help evaluate and enhance an organization's security posture (Bernardo et al., 2025). Despite the wide use of CMMI in conducting cybersecurity maturity evaluation, there are still sharp gaps. Top of the list is the unavailability of a universally scalable framework that is empirical-validated in alluring cybersecurity levels that simultaneously produce correspondence with commercial targets that are fluid or resource-limited. Another weakness here is that the current models tend to focus mainly on one aspect; technical depth or sector-based imperative and do not achieve an overall interconnection between maturity, quantifiable organizational resilience, and the returns on investment security. Efforts on integration with other frameworks that it complements, e.g., with Agile and NIST standards, are recorded, but actionable templates and consolidated evaluation strategies are still unavailable. Field-observational investigations that have a direct association between a cybersecurity maturity level and performance measures in industries beyond a few industries also are limited, which further limits the strategic overall applicability of available research.

1.3 Research Questions:

1. What are the key cybersecurity domains?
2. How does the CMMI model compare with other cybersecurity frameworks in guiding cybersecurity process maturity improvement?
3. What challenges do organizations face when implementing the CMMI maturity indicator model for cybersecurity, and how can these challenges be mitigated?
4. To what extent does improving cybersecurity maturity through the CMMI model enhance organizational resilience, compliance, and risk management outcomes?

1.4 Research Significance:

This study seeks to propose an enhanced model of the cybersecurity process using the CMMI Maturity Indicator Level Scale. The model has been built to deliver an industry-agnostic, scalable framework that will simultaneously evaluate the maturity and align best cybersecurity practices to organizational performance results. The empirical check procedures and the focus on more measurable metrics are used to improve the practical applicability of the CMMI framework to the cybersecurity planning and the improvement efforts. The paper, furthermore, surpasses the scientific literature by providing a synthesizing framework that enables organizations to maximize the value of their security investments as well as aligning cybersecurity initiatives with the overall business goals in the most strategic fashion, which responds to the necessity of flexible and results-oriented cybersecurity maturity models.

1.5 Underpinning Theories:

The Capability Maturity Theory (CMT) posits that organizations should incrementally cultivate digital transformation capabilities by concentrating on critical improvement priorities to enhance progress (Hortovanyi, 2023). CMT has been utilized to create

maturity models for evaluating safety concerns across various industries. (Trinh & Feng, 2022). The Capacity Maturity Model is predicated on the notion that capability enhancement is a gradual and progressive endeavor. Its fundamental principle is continuous process improvement, delineating capability enhancement into multiple levels, each associated with specific key process areas. The organization has attained a stage where all requisite key process areas are fulfilled. Consequently, the company's process capabilities are perpetually advancing incrementally (Hu & Gao, 2019).

2. Literature Review

Process improvement is based on several interconnected stages, including measurement, analysis, and enhancement of organizational processes. Effective improvement requires a comprehensive approach that evaluates organizations at three levels: the overall organization, implemented processes, and existing job positions (Semrau, 2024). Process maturity reflects the degree to which organizations adopt a continuous process-improvement orientation (Kahrović & Đorđević, 2018).

The Capability Maturity Model (CMM) is a framework designed to organize capabilities and maturity categories within organizations. It provides structured maturity levels and capability descriptors that help organizations evaluate their current processes, define improvement objectives, and establish pathways for continuous enhancement. Maturity Models (MMs) are widely used across fields such as business, information technology, project management, and quality management (Šimić et al., 2025).

Originally developed in the software industry, CMM views software development as a structured process that can be measured, analyzed, standardized, and improved. The framework enables organizations to assess their digital capabilities, identify weaknesses, and improve transformation strategies (Han et al., 2022). CMM evaluates organizations through hierarchical maturity levels using selected indicators to determine the maturity of specific research objects.

The Capability Maturity Model Integration (CMMI) expands this concept by integrating multiple models into one framework that supports process improvement, training, and assessment. CMMI includes three major domains:

- **CMMI-SVC (Services):** Focuses on improving service delivery and management.
- **CMMI-DEV (Development):** Supports product and service development activities.
- **CMMI-ACQ (Acquisition):** Enhances acquisition, outsourcing, and supply chain processes in government and commercial environments (Rohmah et al., 2019).

The maturity concept represents the progression of organizational processes from informal and ad hoc practices to structured, optimized systems with measurable performance indicators. Although CMM was initially created for software development, its principles are applicable to many process-oriented domains (Vanita, 2019). Achieving higher maturity levels requires substantial time, effort, and financial investment.

CMMI provides organizations with a roadmap for systematic process improvement. Organizations improve by defining standard procedures, implementing measurement and analysis mechanisms, setting process goals, and continuously evaluating process performance (Popoola et al., 2024). Maturity Models generally function as benchmarks that help organizations assess current practices, prioritize improvements, and establish future objectives (US Department of Energy, 2021). Some models serve descriptive purposes through assessment, while others are normative and provide guidance for achieving higher maturity levels (Fryt, 2019).

In cybersecurity, organizational maturity has evolved alongside technological development and increasing cyber threats. Early cybersecurity practices focused mainly on basic protection against viruses and unauthorized access, but growing digital dependence transformed cybersecurity into a critical national security concern (Abrahams et al., 2024).

Cybersecurity frameworks exist at national, international, regional, and industry levels. However, many frameworks are considered overly general and difficult to implement because organizations differ in size, structure, and operational needs (Djebbar & Nordström, 2023). Common cybersecurity frameworks include the NIST Cybersecurity Framework (NIST CSF), COBIT 5, CIS Controls, Standard of Good Practice for Information Security (SoGP for IS), and ISO/IEC 27005 (Mbanaso et al., 2019). These frameworks provide organizations with structured methods for managing cyber risks and implementing security controls.

The maturity pyramid illustrates six implementation stages ranging from incomplete processes to optimized systems.

2.2 Level 1: Initial:

At this stage, processes are chaotic, inconsistent, and heavily dependent on individual efforts. Organizations often lack stable environments, and success depends on employee competence rather than standardized methods (Mahmood, 2016). The CMM originated during the late 1980s when the Software Engineering Institute (SEI) was commissioned by the US Department of Defense to address software quality and reliability issues in defense projects (Mansour et al., 2024). Level 1 organizations commonly experience budget overruns, overcommitment, and difficulty repeating successful outcomes.

2.3 Level 2: Managed:

At Level 2, processes become planned, documented, monitored, and repeatable. Organizations establish policies, allocate sufficient resources, involve stakeholders, and ensure processes comply with defined descriptions (Mahmood, 2016). Projects are implemented according to established plans, and process discipline enables organizations to continue operating effectively under pressure (Morais, 2018).

Organizations at this level use trained personnel, quality assurance measures, documentation systems, and basic configuration management tools (Frangky, 2022). BPMM Stage 2 organizations begin building Business Process Management (BPM) capabilities, increasing executive involvement, documenting processes, and using structured methodologies and standards (Kahrović & Đorđević, 2018). However, they remain vulnerable to organizational changes.

2.4 Level 3: Defined:

At Level 3, organizations implement standardized methods for managing processes and information across all projects. Leadership support becomes stronger, information is integrated into organizational systems, and reporting becomes more accurate and timely (Stewart, 2016). The organization ensures that all projects adopt approved and documented software processes for development, testing, and maintenance (Vanita, 2019).

Organizations at this level expand BPM capabilities by using advanced tools such as dynamic modeling, workflow systems, distributed applications, and process-based risk management techniques. They also rely more on internal expertise and provide formal BPM training (Kahrović & Đorđević, 2018). Continuous learning and knowledge sharing become important cultural values.

2.5 Level 4: Quantitatively Managed:

Level 4 organizations manage processes through statistical measurements and quantitative performance indicators. Process managers establish measurable goals for quality and performance while continuously benchmarking and evaluating operations to identify opportunities for improvement (Chahidi et al., 2023). Quality objectives are based on customer and stakeholder needs and are represented through performance indicators that support effective management.

At this stage, organizations achieve predictable performance outcomes and can identify process variations early, enabling continuous improvement and strategic alignment (Morais, 2018). According to Keshta (2019), CMM aims to transform organizations from immature and unstructured systems into disciplined and highly organized environments.

2.6 Level 5: Optimizing:

The highest maturity level emphasizes continuous improvement and innovation. Organizations regularly evaluate cybersecurity goals and integrate cybersecurity controls into enterprise risk management systems (Saudi Arabian Monetary Authority, 2017). Real-time automated monitoring and data-driven feedback mechanisms support ongoing optimization.

Organizations at Level 5 use quantitative performance insights to improve processes continuously (Wibisono & Sensuse, 2018). Key characteristics include automated data collection, advanced feedback systems, improved human resource quality, and enhanced process quality (Frangky, 2022). The focus is on adopting new technologies and refining processes to maintain operational excellence.

Cybersecurity maturity assessments help organizations evaluate strengths, weaknesses, and alignment with industry best practices (Razikin & Widodo, 2021). These assessments identify gaps in security procedures and measure how effectively organizations meet contractual and regulatory requirements.

Several cybersecurity maturity models support organizations in evaluating digital capabilities and resilience against cyber threats. Examples include the Cybersecurity Maturity Framework (CMM), Cyber Resilience Review (CRR), CSIRT Maturity Framework, and SOC-CMM (Lee et al., 2024). These models assist organizations in assessing vulnerabilities, setting priorities, managing risks, improving response capabilities, and ensuring regulatory compliance.

Despite their benefits, many cybersecurity maturity models are highly complex and difficult to use for self-assessment (Ozkan & Spruit, 2019). Furthermore, generalized frameworks often fail to address the unique needs of individual organizations. As organizations become more dependent on critical infrastructure, cyber risks increase significantly because disruptions can affect larger populations.

The effectiveness of Cybersecurity Capability Maturity Models (CCMMs) depends heavily on proper implementation and adaptation to organizational contexts. Inadequate cybersecurity measures expose organizations to evolving cyber threats and weaken resilience. Therefore, organizations must ensure that CCMMs are flexible, practical, and aligned with operational requirements and limitations (Liyanage et al., 2024). Proper implementation strengthens cybersecurity resilience, protects organizational assets, preserves stakeholder trust, and enhances the ability to respond to continuously changing cyber threats.

3. Methodology

The researcher depended on the descriptive analytic approach to offer an alternative approach to integrate the CMMI practices for process improvement, recognizing cybersecurity standards, including ISO 27001, the NIST Cybersecurity Framework, and the MIL Scale. It could provide clear quantitative and qualitative indicators that can help decision-makers assess evolving levels of maturity clarity, identify gap thresholds, and then construct a path for continuing growth.

3.1 Population and Sample:

The population consists of all employees in the cybersecurity departments and divisions in public institutions. Furthermore, the samples were taken as follows:

- **Pilot Sample**: Before applying the questionnaire to the main sample of the study, a pilot test was conducted on a sample of 30 individuals from the population to ensure that the tool was capable of measuring what it was designed to measure accurately and reliably. This process included calculating Cronbach's alpha coefficient to assess the consistency of the questionnaire statements and the Pearson correlation coefficient to evaluate the extent to which each statement is related to the theoretical dimension it represents.
- **Primary sample:** This is the sample on which the study tool was applied after verifying its validity and reliability to achieve the study objectives and answer its questions. Due to the large size of the population, the study sample included (384) individuals using the simple purposive method, and (400) questionnaires were distributed to the sample under study to ensure that there were no missing persons and that the application was applied to the specified sample.

3.2 Study Tool and Procedures for Verifying Its Validity and Reliability:

The researcher reviewed the study's objectives, which aimed to reveal the Improving Cybersecurity Process Using CMMI Maturity Indicator Level Scale. After reviewing the theoretical literature and previous studies on the topic, he found that the most appropriate method for collecting data was a questionnaire. The researcher drew on the theoretical literature and previous studies to construct the questionnaire and formulate its statements. The principal axes and dimensions included in the questionnaire were identified, along with the statements that fall under each dimension. The questionnaire was as follows:

3.3 Description of the Study Tool (Questionnaire):

The final version of the questionnaire consisted of two main parts:

3.3.1 This includes the preliminary information about the study sample, represented by demographic data such as gender, age, academic qualification, job title, years of experience in the field of cybersecurity, type of sector the organization belongs to, and organization size.

3.3.2 This consists of the questionnaire axes, which comprise (6) key axes, as follows:

- **First Axis: Cyber Process Management:** consists of statements (1) to (10).
- **Second Axis: Cyber Risk Management:** consists of statements (11) to (20).
- **Third Axis: Continuous Improvement:** consists of statements (21) to (30).
- **Fourth Axis: Training and Competence Management:** consists of statements (31) to (40).
- **Fifth Axis: Change Management:** consists of statements (41) to (50).
- **Sixth Axis: Performance and Measurement Management:** consists of statements (51) to (60).

A five-point Likert scale (strongly agree, agree, neutral, disagree, strongly disagree) was used to validate the study tool, with responses giving a rate of strongly disagree (1), disagree (2), neutral (3), agree (4), and strongly agree (5).

3.3.3 Validity and Reliability of the Tool:

Experts' Validity: After completing the questionnaire and constructing its statements, it was presented to a group of experts to verify its effectiveness and achievement of the study's objectives, to ensure the relevance of each statement to its respective dimension, the clarity and linguistic accuracy of each statement, and its suitability for achieving the intended goal. The experts also suggested ways to improve the questionnaire by deleting, adding, rephrasing, or making any other modifications they deemed appropriate.

After receiving the reviewed copies from the experts and considering their suggestions, the researcher revised the questionnaire. Some statements were deleted or rephrased based on the agreement of more than (84%) of the experts. Thus, after confirming its face validity, the final version consisted of (60) statements distributed across six axes.

4. Results

4.1 **Question 1:** How effective is Cyber Process Management in ensuring that digital processes within an organization are organized and coordinated securely?

Table 1. Frequencies, Percentages, Arithmetic Means, and Standard Deviations of the Sample Responses to the Statements of the First Axis

No.	Statement	Response rate						Mean	SD	Rank	RD
			Strongly agree	Agree	Neutral	Disagree	Strongly disagree				
1	All cybersecurity processes and procedures are regularly documented.	F	77	63	73	51	120	2.81	1.522	10	Moderate
		%	20.1	16.4	19.0	13.3	31.3				
2	Clear policies and guidelines exist for implementing security operations within the organization.	F	121	41	34	117	71	3.06	1.554	7	Moderate
		%	31.5	10.7	8.9	30.5	18.5				
3	Security processes are applied in a standardized manner across all departments.	F	84	60	48	113	79	2.89	1.463	9	Moderate
		%	21.9	15.6	12.5	29.4	20.6				
4	The performance of security processes is monitored regularly.	F	153	92	12	46	81	3.41	1.600	4	High
		%	39.8	24.0	3.1	12.0	21.1				
5	Security processes are reviewed and updated in response to technological changes.	F	147	33	78	43	83	3.31	1.538	6	Moderate
		%	38.3	8.6	20.3	11.2	21.6				
6	A clear mechanism exists for assigning roles and	F	156	93	70	59	6	3.87	1.153	1	High
		%	40.6	24.2	18.2	15.4	1.6				

	responsibilities within security processes.										
7	The effectiveness of cybersecurity operational procedures is regularly evaluated.	F	163	76	36	56	53	3.63	1.486	3	High
		%	42.4	19.8	9.4	14.6	13.8				
8	A central database is available to document daily security activities.	F	164	72	68	61	19	3.78	1.282	2	High
		%	42.7	18.8	17.7	15.9	4.9				
9	Advanced digital tools are used to manage security processes.	F	137	61	64	53	69	3.37	1.519	5	Moderate
		%	35.7	15.9	16.7	13.8	18.0				
10	Senior management adopts a continuous improvement principle for cybersecurity processes.	F	74	84	70	76	80	2.99	1.423	8	Moderate
		%	19.3	21.9	18.2	19.8	20.8				
Overall								3.32	.443	Moderate	

The first axis recorded an overall mean of (3.32) with a standard deviation of (.443), reflecting a moderate response degree. Statement No. (6) A clear mechanism exists for assigning roles and responsibilities within security processes ranked first (mean = 3.87, SD = 1.153, high response), followed by statement No. (8) A central database is available to document daily security activities (mean = 3.78, SD = 1.282, high response). In contrast, statement No. (1) All cybersecurity processes and procedures are regularly documented came last (mean = 2.81, SD = 1.522, moderate response). The standard deviations (1.153–1.600) indicate significant variation in participants' opinions.

Analytically, the moderate overall response suggests weaknesses in implementing secure digital practices, reflecting limited adoption of modern technical and administrative methods. This may stem from insufficient awareness of cyber management importance or the absence of clear policies, both of which negatively affect efficiency and information security.

The high ranking of statement (6) indicates that organizations under study maintain effective systems for defining roles and responsibilities, ensuring coordination among cybersecurity teams, rapid threat response, and reduced errors or overlap. Conversely, the low ranking of statement (1) highlights inadequate attention to documentation processes, likely due to lack of awareness of their role in business continuity and performance evaluation, or the absence of formal policies requiring periodic updates. This underscores the need for structured documentation systems to enhance accountability and strengthen cybersecurity governance.

4.2 **Question 2:** What is the Level of Cyber Risk Management in the Organization's Ability to Identify and Assess Digital Risks, Along with Taking Appropriate Preventive Measures?

Table 2. Frequencies, Percentages, Arithmetic Means, and SD of the Sample Responses to the Statements of the Second Axis

No.	Statement	Response rate						Mean	SD	Rank	RD
			Strongly agree	Agree	Neutral	Disagree	Strongly disagree				
11	A standardized system is in place to identify and assess cyber risks.	F	67	62	60	87	108	2.72	1.462	10	Moderate
		%	17.4	16.1	15.6	22.7	28.1				
12	Risks are classified according to their impact level and likelihood of occurrence.	F	69	74	66	74	101	2.83	1.461	9	Moderate
		%	18.0	19.3	17.2	19.3	26.3				
13		F	83	74	78	73	76	3.04	1.429	5	Moderate

	Clear response plans are prepared for security incidents.	%	21.6	19.3	20.3	19.0	19.8				
14	Regular tests are conducted to identify vulnerabilities and weaknesses in systems.	F	67	80	74	69	94	2.89	1.435	8	Moderate
		%	17.4	20.8	19.3	18.0	24.5				
15	Risk registers are updated periodically based on new analysis.	F	93	79	66	75	71	3.12	1.449	6	Moderate
		%	24.2	20.6	17.2	19.5	18.5				
16	Risk reports are shared regularly with work teams and senior management.	F	122	73	61	62	66	3.32	1.488	4	Moderate
		%	31.8	19.0	15.9	16.1	17.2				
17	Resources are allocated to address high-impact risks.	F	70	80	78	80	76	2.97	1.393	7	Moderate
		%	18.2	20.8	20.3	20.8	19.8				
18	Data analysis tools are used to predict future threats.	F	139	68	50	67	60	3.41	1.503	3	High
		%	36.2	17.7	13.0	17.4	15.6				
19	The effectiveness of risk mitigation policies is evaluated after implementation.	F	211	47	50	39	37	3.93	1.397	1	High
		%	54.9	12.2	13.0	10.2	9.6				
20	An organizational culture exists that supports a risk management awareness at all levels.	F	214	38	44	41	47	3.86	1.479	2	High
		%	55.7	9.9	11.5	10.7	12.2				
Overall								3.21	.460	Moderate	

The second axis recorded an overall mean of (3.21) with a standard deviation of (.460), reflecting a moderate response degree. Statement No. (19) The effectiveness of risk mitigation policies is evaluated after implementation ranked first (mean = 3.93, SD = 1.397, high response), followed by statement No. (20) An organizational culture exists that supports risk management awareness at all levels (mean = 3.86, SD = 1.479, high response). In contrast, statement No. (11) A standardized system is in place to identify and assess cyber risks came last (mean = 2.72, SD = 1.462, moderate response). The standard deviations (1.393–1.503) are relatively high, indicating divergence in participants' opinions.

Analytically, the moderate overall response suggests that organizations lack a mature and unified system for identifying, assessing, and managing cyber risks. This weakness reflects limited adoption of preventative strategies and clear response plans, as well as insufficient employee awareness or specialized training, leaving institutions vulnerable to cyberattacks and their operational impacts.

The high ranking of statement (19) highlights that organizations regularly evaluate the effectiveness of risk mitigation policies, enabling identification of strengths and weaknesses and promoting continuous improvement. This practice reflects management's commitment to ensuring that adopted measures achieve their intended goal of reducing cyber risks. Conversely, the low ranking of statement (11) underscores the absence of standardized mechanisms for risk identification and assessment, leading to inconsistent handling across teams and weak coordination in cybersecurity decision-making. This decline reflects a lack of strategic orientation toward comprehensive risk management, emphasizing the need for a unified system that standardizes criteria and procedures, thereby enhancing organizational resilience against digital threats.

4.3 **Question 3**: What is the Level of Continuous Improvement in Developing Employees' Skills and Enhancing Their Capabilities to Deal with Cyber Risks?

Table 3. Frequencies, Percentages, Arithmetic Means, and SD of the Sample Responses to the Statements of the Third Axis

No.	Statement	Response rate						Mean	SD	Rank	RD
			Strongly agree	Agree	Neutral	Disagree	Strongly disagree				
21	The effectiveness of security strategies is evaluated after each cyber incident.	F	72	75	66	70	101	2.86	1.472	10	Moderate
		%	18.8	19.5	17.2	18.2	26.3				
22	The results of security reviews are used to develop new policies.	F	151	68	59	48	58	3.54	1.482	5	High
		%	39.3	17.7	15.4	12.5	15.1				
23	Regular meetings are held to discuss opportunities to improve cybersecurity.	F	144	56	64	60	60	3.43	1.500	6	High
		%	37.5	14.6	16.7	15.6	15.6				
24	Past mistakes are analyzed to improve security performance.	F	77	70	73	69	95	2.91	1.467	9	Moderate
		%	20.1	18.2	19.0	18.0	24.7				
25	Management encourages innovative ideas for enhancing cybersecurity.	F	184	49	46	48	57	3.66	1.526	4	High
		%	47.9	12.8	12.0	12.5	14.8				
26	A mechanism exists to monitor emerging trends and implement them in security processes.	F	91	59	77	83	74	3.03	1.447	8	Moderate
		%	23.7	15.4	20.1	21.6	19.3				
27	The results of improvements are integrated into the organization's strategic plans.	F	191	40	55	49	49	3.72	1.492	3	High
		%	49.7	10.4	14.3	12.8	12.8				
28	The organization regularly monitors cybersecurity performance indicators.	F	210	34	51	46	43	3.84	1.465	1	High
		%	54.7	8.9	13.3	12.0	11.2				
29	Human and technical resources are allocated to support continuous improvement initiatives.	F	90	79	64	78	73	3.09	1.450	7	Moderate
		%	23.4	20.6	16.7	20.3	19.0				
30	All improvement processes are documented in a dedicated database for future review.	F	194	49	50	47	44	3.79	1.455	2	High
		%	50.5	12.8	13.0	12.2	11.5				
Overall								3.39	.473	Moderate	

The third axis recorded an overall mean of (3.39) with a standard deviation of (.473), reflecting a moderate response degree. Statement No. (28) The organization regularly monitors cybersecurity performance indicators ranked first (mean = 3.84, SD = 1.465, high response), followed by statement No. (30) All improvement processes are documented in a dedicated database for future review (mean = 3.79, SD = 1.455, high response). In contrast, statement No. (21) The effectiveness of security strategies is evaluated after each cyber

incident came last (mean = 2.86, SD = 1.472, moderate response). The standard deviations (1.447–1.526) are relatively high, indicating divergence in participants' opinions.

Analytically, the moderate overall response suggests that organizations do not give sufficient attention to periodically reviewing and developing their processes. This points to weak internal evaluation mechanisms or limited awareness of the importance of continuous improvement, leaving current procedures prone to shortcomings and less adaptable to emerging challenges.

The high ranking of statement (28) indicates that organizations regularly monitor cybersecurity performance indicators, enabling timely assessment of implemented measures, identification of strengths and weaknesses, and continuous improvement. This commitment to monitoring reflects organizational capacity to enhance cybersecurity and ensure efficient protection of data and digital operations. Conversely, the low ranking of statement (21) highlights insufficient evaluation of security strategies after incidents, suggesting that organizations fail to systematically analyze past events or capitalize on lessons learned. This shortcoming may lead to repeated mistakes and weak preparedness for future threats, underscoring the need for structured post-incident evaluation mechanisms.

4.4 **Question 4:** To what Extent Does Training and Competence Management Contribute to Developing Employees' Skills and Enhancing Their Ability to Deal with Cyber Risks?

Table 4. Frequencies, Percentages, Arithmetic Means, and SD of the Sample Responses to the Statements of the Fourth Axis

No	Statement	Response rate						Mean	SD	Rank	RD
			Strongly agree	Agree	Neutral	Disagree	Strongly disagree				
31	The organization provides regular cybersecurity training programs.	F	68	65	66	59	126	2.71	1.506	10	Moderate
		%	17.7	16.9	17.2	15.4	32.8				
32	Employee training needs are assessed regularly.	F	79	71	86	79	69	3.03	1.392	7	Moderate
		%	20.6	18.5	22.4	20.6	18.0				
33	The training program's content is updated according to the latest technological developments.	F	68	69	69	67	111	2.78	1.475	9	Moderate
		%	17.7	18.0	18.0	17.4	28.9				
34	Management encourages employees to pursue professional cybersecurity certifications.	F	126	53	61	69	75	3.22	1.539	5	Moderate
		%	32.8	13.8	15.9	18.0	19.5				
35	A separate budget is allocated for security training and development programs.	F	77	65	59	81	102	2.83	1.490	8	Moderate
		%	20.1	16.9	15.4	21.1	26.6				
36	The effectiveness of training programs is evaluated after each session.	F	138	77	54	59	56	3.47	1.468	2	High
		%	35.9	20.1	14.1	15.4	14.6				
37	There is a database of the organization's employees' security skills.	F	83	82	75	71	73	3.08	1.422	6	Moderate
		%	21.6	21.4	19.5	18.5	19.0				
38	New employees are trained on cybersecurity policies and procedures.	F	148	63	44	62	67	3.42	1.546	3	High
		%	38.5	16.4	11.5	16.1	17.4				
39	Awareness campaigns are organized to promote a culture of cybersecurity.	F	172	56	49	52	55	3.62	1.506	1	High
		%	44.8	14.6	12.8	13.5	14.3				

40	Training outcomes are measured by the improvement in employees' performance in security practices.	F	113	63	78	74	56	3.27	1.432	4	Moderate
		%	29.4	16.4	20.3	19.3	14.6				
Overall								3.14	.442	Moderate	

The fourth axis recorded an overall mean of (3.14) with a standard deviation of (.442), reflecting a moderate response degree. Statement No. (39) Awareness campaigns are organized to promote a culture of cybersecurity ranked first (mean = 3.62, SD = 1.506, high response), followed by statement No. (36) The effectiveness of training programs is evaluated after each session (mean = 3.47, SD = 1.468, high response). In contrast, statement No. (31) The organization provides regular cybersecurity training programs came last (mean = 2.71, SD = 1.506, moderate response). The standard deviations (1.392–1.546) are relatively high, indicating divergence in participants' opinions.

Analytically, the moderate overall response suggests that organizations do not sufficiently prioritize employee training or the development of cybersecurity skills. This reflects weak or irregular training programs and limited opportunities for employees to acquire the knowledge and experience necessary to address digital risks effectively.

The high ranking of statement (39) highlights organizational reliance on awareness campaigns to educate employees about secure practices and the importance of information protection. Such initiatives contribute to reducing human error and fostering a culture of vigilance against cyber threats. Conversely, the low ranking of statement (31) underscores the lack of regular training programs, which weakens both individual and collective preparedness to confront cyber risks. This shortcoming reduces the effectiveness of existing security measures and reflects the need for structured, continuous training policies that enhance organizational resilience and align with global cybersecurity standards.

4.5 Question 5: To what extent does Change Management contribute to improving an organization's ability to implement changes to cybersecurity systems and policies in an organized manner?

Table 5. Frequencies, Percentages, Arithmetic Means, and SD of the Sample Responses to the Statements of the Fifth Axis

No	Statement	Response rate	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Mean	SD	Rank	RD
41	Clear procedures are applied when making any changes to cybersecurity systems.	F	71	58	81	65	109	2.78	1.468	10	Moderate
		%	18.5	15.1	21.1	16.9	28.4				
42	The impact of any change is assessed before implementing any modification to the security infrastructure.	F	68	67	82	76	91	2.86	1.419	9	Moderate
		%	17.7	17.4	21.4	19.8	23.7				
43	Different work teams are involved in the change planning process.	F	76	93	68	77	70	3.07	1.401	6	Moderate
		%	19.8	24.2	17.7	20.1	18.2				
44	A risk management plan accompanies each change process.	F	81	63	72	80	88	2.92	1.460	8	Moderate
		%	21.1	16.4	18.8	20.8	22.9				
45	New systems are tested before their actual deployment.	F	106	77	92	57	52	3.33	1.374	5	Moderate
		%	27.6	20.1	24.0	14.8	13.5				
46	Security documentation and policies are updated following any significant modification.	F	95	112	83	54	40	3.44	1.285	3	High
		%	24.7	29.2	21.6	14.1	10.4				
47		F	69	83	76	78	78	2.97	1.398	7	Moderate

	Users are informed about the reasons for and objectives of the changes.	%	18.0	21.6	19.8	20.3	20.3				
48	Post-implementation reviews are conducted to measure the impact of the change.	F	135	89	64	52	44	3.57	1.383	2	High
		%	35.1	23.2	16.7	13.5	11.5				
49	All change processes are documented within the corporate knowledge management system.	F	123	58	84	83	36	3.39	1.370	4	Moderate
		%	32.0	15.1	21.9	21.6	9.4				
50	Lessons learned from previous changes are used to improve the management of future changes.	F	189	69	43	48	35	3.86	1.382	1	High
		%	49.2	18.0	11.2	12.5	9.1				
Overall								3.22	.444	Moderate	

The table above shows that the fifth axis recorded an overall mean of (3.22) with a standard deviation of (.444), reflecting a moderate response degree. Statement No. (50) Lessons learned from previous changes are used to improve the management of future changes ranked first (mean = 3.86, SD = 1.382, high response), followed by statement No. (48) Post-implementation reviews are conducted to measure the impact of the change (mean = 3.57, SD = 1.383, high response). In contrast, statement No. (41) Clear procedures are applied when making any changes to cybersecurity systems came last (mean = 2.78, SD = 1.468, moderate response). The standard deviations (1.285–1.468) are relatively high, indicating divergence in participants' opinions.

Analytically, the moderate overall response suggests that organizations face difficulties in implementing effective strategies for managing digital system and policy changes. This weakness may reflect poor planning or insufficient employee preparation, leading to resistance or reduced performance.

The high ranking of statement (50) highlights the importance organizations place on learning from past experiences to improve future change management. This practice helps avoid repeating mistakes, strengthens procedures, and enhances responsiveness to digital transformations, thereby supporting operational stability. Similarly, the second-place ranking of statement (48) reflects attention to post-implementation reviews, which enable organizations to measure impact and refine strategies. Conversely, the low ranking of statement (41) underscores the absence of clear, documented procedures during system modifications, which may result in errors, gaps, or weak employee awareness. This shortcoming highlights the urgent need to establish structured and transparent procedures for every cybersecurity change to ensure stability and reduce risks.

4.6 Question 6: To What Extent Does Performance and Measurement Management Contribute to Monitoring Cybersecurity Performance Indicators and Improving the Effectiveness of Security Measures within the Organization?

Table 6. Frequencies, Percentages, Arithmetic Means, and SD of the Sample Responses to the Statements of the Sixth Axis

No	Statement	Response rate	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Mean	SD	Rank	RD
51	Clear performance indicators are defined to measure	F	50	62	82	73	117	2.62	1.398	10	Moderate
		%	13.0	16.1	21.4	19.0	30.5				
52	Data is collected and analyzed to assess the effectiveness of	F	103	63	71	80	67	3.14	1.459	4	Moderate
		%	26.8	16.4	18.5	20.8	17.4				
53	Performance results are compared with established	F	55	52	93	81	103	2.67	1.375	9	Moderate
		%	14.3	13.5	24.2	21.1	26.8				
54	Security performance reports are regularly presented to	F	33	74	106	99	72	2.73	1.215	8	Moderate
		%	8.6	19.3	27.6	25.8	18.8				

55	Improvement decisions are made based on measurement	F	59	90	72	72	91	2.88	1.405	6	Moderate
		%	15.4	23.4	18.8	18.8	23.7				
56	Advanced measurement tools are used to track security	F	62	65	78	80	99	2.77	1.416	7	Moderate
		%	16.1	16.9	20.3	20.8	25.8				
57	Performance results are documented in periodic	F	88	83	81	77	55	3.19	1.370	3	Moderate
		%	22.9	21.6	21.1	20.1	14.3				
58	Security objectives are reviewed annually to ensure	F	77	72	81	68	86	2.96	1.438	5	Moderate
		%	20.1	18.8	21.1	17.7	22.4				
59	Departments that achieve outstanding security	F	177	81	65	48	13	3.94	1.198	1	High
		%	46.1	21.1	16.9	12.5	3.4				
60	Measurement results are used to develop cybersecurity	F	143	77	77	63	24	3.66	1.295	2	High
		%	37.2	20.1	20.1	16.4	6.3				
Overall								3.06	.443	Moderate	

The table above shows that the sixth axis recorded an overall mean of (3.06) with a standard deviation of (.443), reflecting a moderate response degree. Statement No. (59) Departments that achieve outstanding security performance are incentivized ranked first (mean = 3.94, SD = 1.198, high response), followed by statement No. (60) Measurement results are used to develop cybersecurity strategic plans (mean = 3.66, SD = 1.295, high response). In contrast, statement No. (51) Clear performance indicators are defined to measure cybersecurity efficiency ranked last (mean = 2.62, SD = 1.398, moderate response). The standard deviations across items (1.198–1.459) indicate notable divergence in participants' views.

Analytically, the moderate overall response suggests insufficient emphasis on continuous monitoring and evaluation of cybersecurity performance, which hinders timely identification of strengths and weaknesses. The high ranking of statement (59) highlights organizational focus on rewarding effective teams, fostering motivation, adherence to best practices, and positive competition that enhances institutional resilience. Conversely, the low ranking of statement (51) underscores the absence of clear, measurable indicators, limiting objective evaluation and systematic improvement. This finding emphasizes the need for organizations to establish robust performance metrics to ensure adaptive and evidence-based cybersecurity strategies.

5. The Proposed CyPro-CMMI Cybersecurity Maturity Integration

The Contemporary organizations face escalating cybersecurity challenges, including advanced attacks, systemic breaches, and limited crisis response capabilities. This reality necessitates integrated frameworks that transcend technical solutions, linking quality improvement methodologies with global cybersecurity requirements.

Earlier maturity models proved insufficient—sector-specific, weakly connected to international standards, and lacking precise indicators—resulting in fragmented assessments and unclear pathways for continuous improvement. Addressing these gaps, the CyPro-CMMI model integrates CMMI practices for process enhancement with globally recognized standards such as ISO 27001, the NIST Cybersecurity Framework, and the MIL Scale.

This integration enables organizations to progress systematically from sporadic practices to cycles of continual improvement and innovation. The model provides both quantitative and qualitative indicators, guiding decision-makers in assessing maturity levels, identifying gaps, and constructing sustainable growth trajectories. Ultimately, the proposal advances cyber resilience strategically, embedding security operations within organizational maturity rather than treating them as isolated measures.

5.1 Proposal Elements:

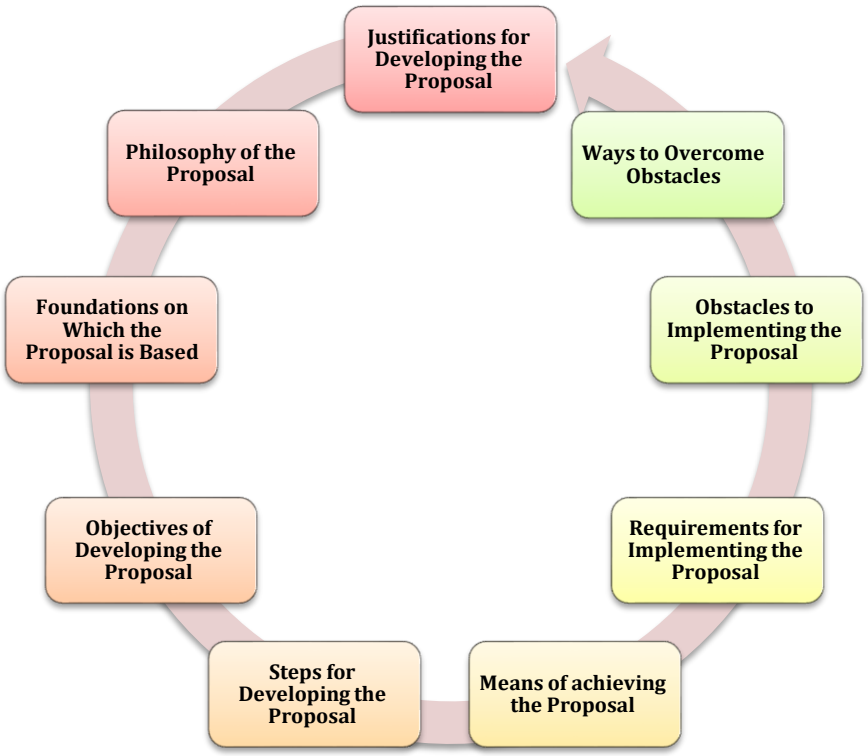

Figure 1. Components of the Proposal. Reference: The researchers' work is based on (Farah, 2024).

Figure 1 illustrates the interconnected components of the proposal, emphasizing its cyclical and iterative nature. The diagram highlights how justifications, objectives, and philosophical foundations serve as the basis for development, while requirements, steps, and means ensure practical implementation. At the same time, obstacles and strategies to overcome them reflect the dynamic challenges inherent in organizational change. This structure underscores that proposal development is not linear but rather a continuous process of refinement, evaluation, and adaptation. The researchers stress that such a framework enhances analytical rigor and strengthens the capacity to achieve sustainable outcomes.

5.2 Justifications for Developing the Proposal:

In the digital era, cyber threats are now more complex than any time in the history of the human race. Organizations are no longer just exposed to threats related to established risks associated with the organization's internal systems, rather they face cross-border threats associated with cloud computing, the Internet of Things (IoT), and emerging technology.

Given that the current threat landscape has evolved, the use of bench-marking process improvement approaches such as CMMI, as well as stand-alone security standards, such as ISO 27001, NIST CSF, and the MIL Scale is no longer enough. Organizations must have a sense of urgency to design a current day cyber security model that is based on CMMI and allows for the two dimensions of process improvement and security preparedness to be managed as a singularly integrated framework.

Practically, the evidence shows that previous models have gaps based on levels of functionality with considerable issues to their overall effectiveness, including:

One challenge with generalization is that some applications may be effective in a certain environment, but not in others due to not having a dynamic and adaptable approach.

Because of the weak direct connection of CMMI maturity levels to cybersecurity standards, organizations tend to make operational improvements without confirming their meeting information security standards, which creates a disconnect between being operationally efficient and being actually protected.

The models tend to lack concrete indicators of maturity which makes measuring progress in security quantitatively and objectively difficult, which leads to being driven by data in decision-making.

As a result, the proposal for the CyPro-CMMI model is a practical response to challenges above by providing a flexible framework for implementation to resolve challenges in the previous models while still remaining compliant with international cybersecurity standards. The integration of maturity indicators in cybersecurity with the CMMI facilitates a complete awareness tool for organizations to evaluate their performance and maturity, measuring their security readiness, and understanding possible pathways for ongoing improvement consistent with modern threats and the nature of digital transformation.

5.3 Philosophy of the Proposal:

The rationale behind the proposal for the CyPro-CMMI model is grounded in the awareness that modern digital challenges are not solely related to software quality or operational efficiencies; they are also related to the maturity of the security practices protecting those operations and systems.

Consequently, synthesizing the improvements in processes proposed in the CMMI framework alongside the cybersecurity maturity benchmarks offered in global standards is the critical first step in developing an integrated system that will simultaneously address risk and promote operational excellence.

The proposal's rationale is established by the notion that any type of development or management process within an organization will not have complete value unless it is cybersafe through mature levels of cybersecurity practices and measures. Conversely, attempting to apply security practices or to manage security while they are detached from improved and documented processes will waste resources, be unsustainable, or difficult to maintain.

The model will also strive to solve these separations by applying a single framework that allows for each level of improvement in CMMI to align with an integrated maturity level of cybersecurity requirements prior to implementation so that improvements in social risk and operational improvement do not take place absent of improvements in cybersecurity posture.

The philosophy of the proposal's framework is that advancement is twofold which looks at improving performance and productivity for one aspect while improving your management of cyber threats and risks as another dimension. These landscapes create opportunity for an organization for an organizational construct to be agile, such that an organization can respond to both, market changes and threats, while also having a metric by which they can measure organizational measures and performance in both and security.

Therefore, to see the CyPro-CMMI to be just simply a technical, or organizational framework to both of an organizations, is much more of a holistic philosophy that does think to all organizations will have to change the way they integrate operations and security as a way of life for to survive and remain relevant in the future marketplace context of digital. This proposal further illustrates that operating any organization successfully, will and should be based on both the organization's ability to manage performance and the organizations ability to protect the performance in parallel with both occurring as continuous methods.

5.4 Foundations on Which the Proposal is Based:

The proposal rests on three interrelated foundations that justify its academic and practical relevance:

- CMMI as a Basis for Operational Improvement: Since its inception, the CMMI model has been recognized as a robust framework for enhancing organizational capability, efficiency, and discipline. It provides a structured pathway for prioritizing processes and ensuring predictable outcomes. Within the cybersecurity dimension, this foundation assures process integrity while strengthening preparedness against digital threats.
- Integration of International Cybersecurity Standards: Global standards remain essential references for safeguarding digital assets and cultivating a proactive security culture. Yet, their fragmented application often leads to duplication or weak alignment with organizational processes. The proposal addresses this by embedding these standards directly into the CMMI framework, ensuring that operational improvement evolves in parallel with internationally recognized cybersecurity controls—eliminating gaps between efficiency and protection.

- Linking CMMI Maturity Levels to Cybersecurity Requirements: Rather than treating security as an isolated add-on, the framework aligns each CMMI maturity level with specific cybersecurity requirements. For instance, progression from Initial to Managed introduces basic security controls alongside improved operational discipline. At advanced stages (Quantitatively Managed and Optimizing), organizations adopt measurement tools and analytical insights, embedding cybersecurity into the maturity journey itself.

By linking CMMI maturity levels to cybersecurity requirements, it demonstrates that each maturity level indicated a journey from basic security awareness to eventually continuous improvement and cybersecurity innovation (see the figure below):

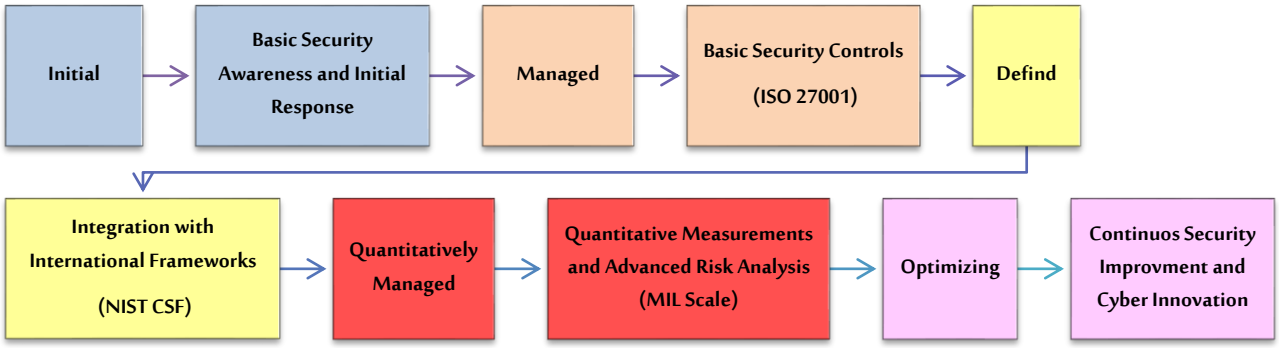

Figure 2. Relationship between CMMI Maturity Levels and Cybersecurity Requirements

5.5 Objectives of Developing the Proposal:

The purpose of this proposal is to provide a user-friendly and actionable framework for the CyPro-CMMI by achieving a set of interrelated objectives:

i. **Enhancing Organizational Readiness to Face Threats**: The proposal seeks to enable organizations to proactively address escalating and complex cyber threats. Rather than relying solely on reactive responses, the model establishes a structured approach for risk identification and mitigation. It also fosters a culture of security awareness and forward-looking practices, equipping organizations to professionally manage cyberattacks while minimizing potential losses.

ii. **Supporting Decision-Making Based on Maturity Indicators**: By integrating the CMMI methodology with cybersecurity standards, the model provides both quantitative and qualitative indicators of organizational maturity in security operations. These metrics empower leaders to make evidence-based decisions when shaping protection strategies or investing in cyber infrastructure. The reliance on factual data ensures rational, realistic, and objective assessments of current capabilities and future readiness.

iii. **Improving Cyber Resilience**: The proposal elevates cyber resilience as a strategic imperative, emphasizing not only prevention but also rapid response and recovery. It advocates for integrated systems that allow organizations to sustain core operations during and after cyber incidents, thereby minimizing disruption. This resilience builds trust among stakeholders and enhances organizational credibility in the face of digital threats.

iv. **Enhancing Integration Between Security Operations and Measures**: The model addresses the traditional disconnect between operational improvement and security measures by embedding cybersecurity within a unified framework. Security is positioned as an essential component of every administrative and operational process, transforming it into a shared responsibility across all organizational levels—from leadership to frontline staff. This integration strengthens governance and embeds cybersecurity into institutional culture.

Accordingly, the objectives of the proposal can be summarized as shown in the following figure:

Figure 3. Objectives of Developing the Proposal

5.6 Steps for Developing the Proposal:

Based on the inclusion of the CyPro-CMMI model in CMMI maturity levels and cybersecurity requirements, establishing steps through which the proposal can be implemented makes the application practical and directly linked to maturity levels, as follows:

1. **Assessment & Baseline:** The organization begins by implementing an initial assessment tool to determine the current maturity level in eight domains (access controls, identity and privacy management, incident response, risk management, compliance and standards, third-party security, cloud security and data privacy, training and security awareness). This assessment aims to establish baselines that can be compared to progress measurements later. This involves data collection, document review, and interviews with officials and stakeholders.
2. **Domain Alignment:** After determining the current state, the key domains are aligned with the organization's operational and strategic needs. For example, financial institutions may focus on compliance and identity management, while technology organizations may prioritize cloud security and incident response. Such alignment ensures that the implementation is not only theoretical but also realistic and suitable to the organizational context.
3. **Improvement Roadmap:** A roadmap is designed to outline how to move from the current level to the next level in each domain. The goal of the roadmap is to provide interim goals, responsibilities, resources needed, and indicators for measuring progress. The roadmap is rooted in the ongoing improvement philosophy used in CMMI.
4. **Implementation by Maturity Level:**

Table 7. The procedures are implemented gradually according to maturity levels:

Level	Procedure
Initial	Establishing basic policies and initial documentation.
Managed	Creating and integrating standard procedures across the organization.
Defined	Introducing quantitative measurement tools and performance indicators for cybersecurity.
Quantitatively Managed	Integrating artificial intelligence technologies.
Optimizing	Advanced analytics for continuous improvement and innovation.

5. **Measurement & Continuous Evaluation** Periodically, performance will be monitored using indicators (e.g. incident response time, compliance rates, the number of remediated vulnerabilities, and employee security awareness). This will create decisions based on actual data and help continuously facilitate improvements.
6. **Enterprise-Wide Integration** As maturity increases, security practices become fully integrated into all aspects of the organization. Cybersecurity may not even have a specific owner in this stage: it is no longer an isolated activity or a team-focused event; it has become part of the cultural fabric and overall organizational strategy.
7. **Optimization & Innovation:** The organization can now pursue utilizing artificial intelligence or automation tools to enhance security capabilities. It can also promote a culture of innovation and experimentation to create new solutions that continue to adapt to future threat opportunities as well.

5.7 Means of achieving the Proposal:

To execute on the proposal, it can be supported by tangible and clear implementation processes, and active means to demonstrate the real-world applicability in an organization, as follows:

- **Technical Instruments:** Security Information and Event Management (SIEM) Systems, Identity and Access Management (IAM) Tools, Compliance Management Tools, Intrusion Detection Systems (IDS/IPS).
- **Policies and Frameworks:** Discipline-specific guides like Access Control, Incident Response, etc., with pre-populated evaluation templates for maturity levels.
- **Education and Capability building**: Day-to-day employee education, Cyber Drills, and internal awareness programs.
- **Proper Governance:** We will construct a committee that's high-level enough about Cybersecurity within the organization to oversee implementation and tie it to the organization significance as a whole.

- **External organizations:** Rely on external third parties/experts to conduct performance reviews for adherence to international standards.
- **Periodic Reporting:** Issue semi-annual or annual reporting that indicates to the organization progress at the maturity level and identifies any lingering issues.

5.8 Integrated Implementation Requirements, Challenges, and Mitigation Mechanisms of the Proposed CyPro-CMMI Cybersecurity Maturity Integration Framework

Table 8. Detailed Implementation Requirements, Challenges, and Mitigation Mechanisms within the Proposed CyPro-CMMI Cybersecurity Maturity Integration Framework

Main Dimension	Detailed Requirement	Associated Challenge	Mitigation Mechanism
Human Requirements	Availability of specialized cybersecurity, risk management, and process-improvement teams	Shortage of qualified cybersecurity professionals and overreliance on limited expertise	Build multidisciplinary teams and implement specialized competency-development programs
	Executive management support and commitment	Resistance to change and weak managerial engagement	Conduct awareness programs linking cybersecurity maturity to strategic objectives
	Supervision by experts from IT, HR, legal, and business functions	Weak coordination among organizational units	Establish cross-functional governance and collaboration mechanisms
	Continuous employee training, workshops, and practical exercises	Insufficient professional competencies	Adopt learning-by-doing approaches and continuous training initiatives
	Organization-wide cybersecurity awareness	Low security awareness and human-related vulnerabilities	Implement awareness campaigns, cyberattack simulations, and security culture programs
Financial and Infrastructure Requirements	Funding for cybersecurity tools and technologies	High implementation and operational costs	Prioritize implementation in high-impact security domains
	Funding for training, consulting, and maturity assessments	Budget constraints and competing organizational priorities	Allocate a dedicated cybersecurity budget within annual plans
	Secure data centers and reliable communication networks	Inadequate infrastructure readiness	Gradually modernize infrastructure according to risk priorities
	Security laboratories and technical equipment	Limited availability of testing and monitoring facilities	Establish phased investment plans and shared-resource models
	Cooperation with accredited security providers	Limited internal resources and expertise	Collaborate with governmental and advisory entities providing technical support
Technical Requirements	Deployment of IAM systems	Weak access governance and privilege management	Implement integrated identity and access management solutions
	Adoption of SIEM platforms	Difficulty detecting and correlating security events	Centralize monitoring and event analysis through SIEM technologies
	Deployment of IDS/IPS solutions	Delayed detection of attacks and malicious activities	Implement automated threat monitoring and prevention mechanisms
	Compliance management platforms	Fragmented compliance processes and standards implementation	Utilize unified compliance and maturity-management platforms
	AI and predictive analytics technologies	Slow threat detection and incident response	Employ predictive security analytics and intelligent monitoring systems

	Cloud security, encryption, and privacy solutions	Risks associated with cloud environments and sensitive data exposure	Implement encryption, privacy controls, and cloud-security governance
	Vulnerability assessment and penetration testing tools	Undiscovered weaknesses and security gaps	Conduct regular vulnerability scanning and penetration-testing exercises
	Compliance with ISO 27001, NIST CSF, and MIL Scale	Complexity of aligning multiple standards	Adopt integrated governance and compliance frameworks
Governance and Regulatory Requirements	Cybersecurity governance structure and oversight committees	Weak governance and fragmented decision-making	Establish permanent cybersecurity committees linked to senior leadership
	Updated policies and procedures	Outdated policies and inconsistent practices	Conduct regular policy reviews aligned with emerging risks
	Alignment with national and international regulations	Regulatory changes and compliance challenges	Continuously update policies according to legal and regulatory requirements
	Security maturity measurement mechanisms	Lack of objective performance evaluation	Develop measurable cybersecurity maturity indicators
	Internal and external audit processes	Inadequate monitoring and accountability	Institutionalize periodic audits and compliance assessments
Partnerships and Continuous Improvement Requirements	Cooperation with national and regional cybersecurity centers	Limited access to advanced expertise and threat intelligence	Develop strategic partnerships and knowledge-sharing mechanisms
	Collaboration with universities and research centers	Weak innovation and limited research support	Establish joint research and capacity-building initiatives
	Continuous evaluation and review mechanisms	Lack of sustained improvement processes	Implement cyclical assessment and continuous-improvement programs
	Benchmarking and organizational learning	Difficulty identifying performance gaps	Adopt benchmarking practices and lessons-learned frameworks

Table 8. provides a comprehensive operationalization framework for implementing the proposed CyPro-CMMI Cybersecurity Maturity Integration Framework by systematically linking implementation requirements with their corresponding challenges and mitigation mechanisms. The table illustrates that cybersecurity maturity is achieved through the simultaneous development of human, financial, technical, governance, and partnership capabilities rather than through technological investments alone. Human-resource readiness and executive commitment emerge as foundational enablers that influence the effectiveness of all other dimensions. Likewise, sustainable funding and infrastructure modernization are critical for supporting advanced cybersecurity technologies and compliance activities. The framework further highlights the strategic role of integrated security technologies, including IAM, SIEM, IDS/IPS, artificial intelligence, and predictive analytics, in strengthening proactive cyber defense capabilities. Governance mechanisms, regulatory alignment, and maturity measurement systems ensure accountability and institutional consistency. Finally, partnerships with cybersecurity centers, universities, and external experts support organizational learning and continuous improvement. Accordingly, the integrated structure presented in the table transforms implementation barriers into actionable improvement opportunities, enhancing the practical applicability, scalability, and long-term sustainability of the CyPro-CMMI framework across diverse organizational environments.

5.9 Assessment of the Proposal:

The model can be assessed through several steps:

1. **Assessment Through:**

- Conducting interviews with work teams and management.
- Reviewing current security policies, procedures, and systems.

- Using checklists related to the model's domains (access control, risk management, incident response, etc.).

2. **Gap Analysis Through:**
   - Comparing the organization's current status with the target level in each of the five maturity domains.
   - Classifying the gaps into:
     - Critical gaps (impacting immediate security).
     - Moderate gaps (needing improvement in the medium term).
     - Minor gaps (can be addressed later).
3. **Developing the Improvement Roadmap Through:**
   - Developing a gradual roadmap that begins with quick actions, such as policy updates or urgent training.
   - Updating medium- and long-term projects, such as:
     - Investing in new technology platforms.
     - Building specialized human capacity.
     - Integrating security into all operational processes.
     - Associating each action with a specific timeline and a designated executive responsible.
4. **Monitoring & Metrics Through:**

- Define periodic performance indicators related to key domains such as the number of detected incidents, policy compliance rate, and response time.
- Conduct quarterly or semi-annual reviews to ensure continuous improvement.
- Use quantitative measurement tools such as CMMI indicators and ISO 27001 to measure maturity levels accurately.

The following figure illustrates an organization's journey from having only initial procedures in place to building a mature, resilient, and scalable cybersecurity environment:

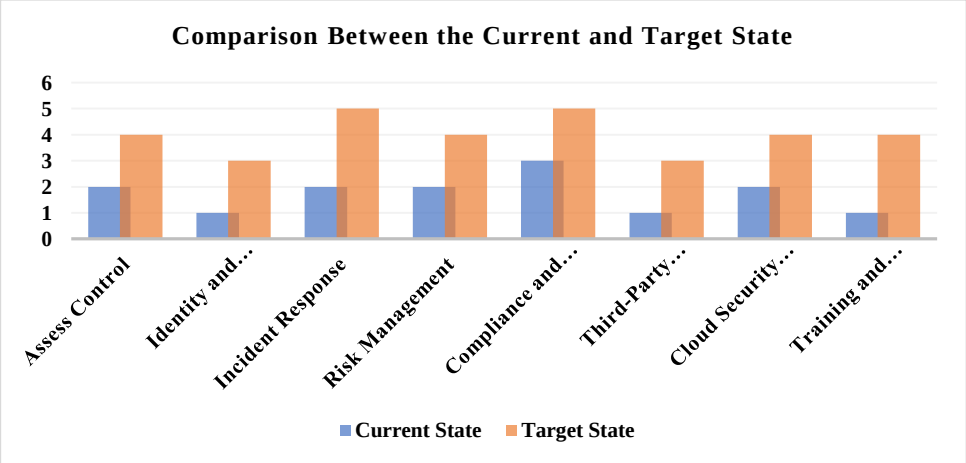

Figure 4. Difference Between the Current State of an Organization and the Target State

The figure reveals the extent to which the organization has transitioned from initial haphazard practices at levels 1-2 in most domains to mature and measured practices at levels 4-5, demonstrating the effectiveness of the proposal, as follows:

This development is not limited to raising the numerical level, but also means:

- The existence of unified policies instead of haphazard ones.
- The introduction of quantitative measurement and indicators instead of impromptu decisions.
- Establishing a continuous improvement and innovation culture in some domains, such as incident response.

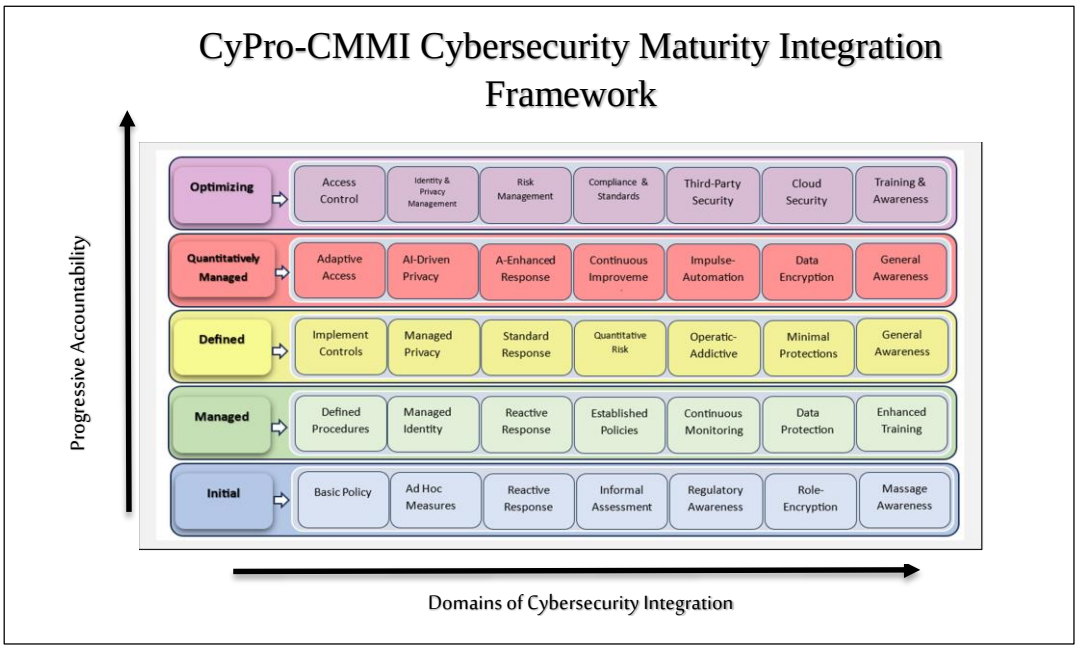

Figure 5. The Proposed CyPro-CMMI Cybersecurity Maturity Integration Framework

6.Discussion

Developing effective cybersecurity risk management techniques is fundamental to organizational resilience in the evolving landscape of digital threats. As threats grow more complex, companies must strengthen their cybersecurity mindset (Dornheim & Zarnekow, 2023). Organizations today face not only internal risks but also cross-border challenges linked to cloud computing, IoT, and emerging technologies. According to Bernardo et al. (2025), using the MM as an additional strategy can enhance evaluation and strengthen security posture. The results confirmed that the CMMI model is a highly effective approach for building organizational capability, efficiency, and discipline, offering a structured way to integrate process improvement with internationally recognized cybersecurity standards. Djebbar & Nordström (2023) further emphasize that cybersecurity standards provide a systematic method for managing and evaluating threats. Importantly, security is not treated as separate from process improvement; rather, each CMMI maturity level aligns with specific cybersecurity requirements.

Compared to other frameworks, the CMMI model proved effective in guiding cybersecurity maturity through unified policies instead of fragmented ones, quantitative indicators instead of ad hoc decisions, and fostering a culture of continuous improvement and innovation, particularly in incident response. Requirements for embedding the CyPro-CMMI model include policies and frameworks, education and capability building, governance, collaboration with external organizations, and periodic reporting. However, technical, human, financial, and regulatory challenges must be addressed to ensure successful implementation. Transforming these obstacles into opportunities enhances realism and applicability across diverse institutions.

Based on these findings, the researchers recommend regular monitoring of cybersecurity performance indicators to evaluate the effectiveness of policies and procedures, adopting continuous improvement to refine processes, and ensuring efficient performance and robust strategies. There is a pressing need for comprehensive cyber risk management policies encompassing assessment, prevention, response, and post-incident review to minimize threats and strengthen organizational security.

7. Study Recommendations

1. Strengthening the cybersecurity culture within organizations through ongoing awareness campaigns targeting all administrative and technical levels.

2. Adopting clear mechanisms to regularly document security processes and procedures to ensure performance tracking and results analysis.
3. Implementing systematic change management procedures that include planning, communication, training, and follow-up to ensure employee acceptance of changes and achieve cybersecurity objectives.
4. Utilizing lessons learned from previous changes to improve future change management strategies and enhance the organization's ability to respond to new challenges.
5. Monitoring cybersecurity performance indicators regularly to evaluate the effectiveness of policies and procedures and make data-driven decisions.
6. Encouraging departments and teams that achieve outstanding performance in cybersecurity to boost motivation and improve compliance with security procedures.
7. Adopting a continuous improvement approach to review and develop processes regularly to ensure efficient performance and effective cybersecurity strategies.
8. **Study Suggestions: Conduct Future Studies on:**
    1) The impact of CMMI maturity levels on the effectiveness of cybersecurity policies.
    2) Applying the CMMI model to strengthen organizational performance in cybersecurity risk management.

References

1. Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., Adegbite, A. O., & Hassan, A. O. (2024). A review of cybersecurity strategies in modern organizations: Examining the evolution and effectiveness of cybersecurity measures for data protection. Computer Science & IT Research Journal, 5(1), 1–25. https://doi.org/10.51594/csitrj.v5i1.699
2. Frangky, F. (2022). Measuring the maturity level of the organization in the process software development using the CMMI-Dev method. Paradigma - Jurnal Komputer dan Informatika, 24(2), 108–116. https://jurnal.bsi.ac.id/index.php/paradigma/article/download/1358/927
3. Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom. Applied Sciences, 10(10), Article 3660. https://doi.org/10.3390/app10103660
4. Baker, Z. (2024). Capability Maturity Model in 2025: Benefits, Levels & Examples. Edstellar, Accessed on 30/07/2025 at https://www.edstellar.com/blog/capability-maturity-model
5. Brett. A. (2024). What Is Access Control and Why Do Cyber Essentials and ISO 27001 Require It?. Accessed on 28/07/2025 at https://www.itgovernance.co.uk/blog/what-is-access-control
6. CISA Cyber+Infrastructure. (2020). Cyber Resilience Review (CRR). Method Description and Self-Assessment User Guide. Available at https://www.cisa.gov/sites/default/files/publications/2_CRR%25204.0_Self-Assessment_User_Guide_April_2020.pdf
7. Dawson, S. (2024). What is the Difference between CMMI DEV and CMMI SVC?. Core Business Solutions. Accessed on 31/07/2025 at https://www.thecoresolution.com/what-is-the-difference-between-cmmi-dev-and-cmmi-svc
8. Edureka higherEd. (2023). What is Process Improvement? Why is it important?. Accessed on 27/07/2025 at https://www.edureka.co/blog/process-improvement/.
9. FasterCapital. (2025). Risk management theory: How to Incorporate Risk Management Theory into Your Business Practice and Strategy. Acessed on 29/07/2025 at https://fastercapital.com/content/Risk-management-theory--How-to-Incorporate-Risk-Management-Theory-into-Your-Business-Practice-and-Strategy.html
10. Garousi, V., Arkan, S., Urul, G., Karapıçak, Ç. M. & Felderer, M. (2015). Assessing the maturity of software testing services using CMMI-SVC: An industrial case study. Aexiv, https://arxiv.org/abs/2005.12570
11. Gourisetti, S. N., Mix, S., Mylrea, M., Bonebrake, C. & Touhiduzzaman. (2019). Secure Design and Development Cybersecurity Capability Maturity Model (SD2-C2M2): Next- Generation Cyber Resilience by Design. 2019 Northwest Cybersecurity Symposium, Available at https://sd2-c2m2.pnnl.gov/documents/SD2-C2M2_Next-Generation_Cyber_Resilience_by_Design.pdf
12. Gupta, D., Elluri, L., Jain, A., Moni, S. S. & Aslan, O. (2024). Blockchain-Enhanced Framework for Secure Third-Party Vendor Risk Management and Vigilant Security Controls. Arxiv, https://arxiv.org/abs/2411.13447

13. Hadyan, N. N., Budiardjo, E. K. & Ferdinansyah, A. (2019). Evaluation of Capability Level and Improvements Prioritization on Device Accreditation Services Based On CMMI-SVC Framework Continuous Representation. Association for Computing Machinery, APIT '19: Proceedings of the 2019 Asia Pacific Information Technology Conference, 84 – 90, https://doi.org/10.1145/3314527.33145
14. Han, X., Zhang, M., Hu, Y., & Huang, Y. (2022). Study on the digital transformation capability of cost consultation enterprises based on maturity model. Sustainability, 14(16), 10038. https://doi.org/10.3390/su141610038
15. Haque, A., Gochhayat, S. P., Shetty, S., & Krishnappa, B. (2020). Cloud-Based Simulation Platform for Quantifying Cyber-Physical Systems Resilience. In book: Simulation for Cyber-Physical Systems Engineering (pp.349-384). DOI:10.1007/978-3-030-51909-4_14
16. Herrmann, D. & Pridöhl, H. (20Siksha 19). Basic Concepts and Models of Cybersecurity. In M. Christen et al. (eds.), The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology 21, Springer Nature Switzerland, https://doi.org/10.1007/978-3-030-29053-5_2
17. Hortoványi, L., Morgan, R. E., Vuksanović Herceg, I., Djuričin, D., Hanák, R., Horváth, D., Mocan, M. L., Romanova, A., & Szabó, R. Z. (2023). Assessment of digital maturity: The role of resources and capabilities in digital transformation in B2B firms. International Journal of Production Research, 61(23), 8043–8061. https://doi.org/10.1080/00207543.2022.2164087
18. Infrastructure Security Agency (CISA). (2021). Cybersecurity Incident & Vulnerability Response Playbooks. CISA Publication, available at https://www.cisa.gov/sites/default/files/202408/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf
19. Javed, S. A. (2022). Cyber security; Etiology and Importance. Creative Commons CC BY license 2022, 1-7. https://doi.org/10.20944/preprints202208.0235.v1
20. Kashmar, N., Adda, M., Atieh, M. & Ibrahim, H. (2021). Access Control In Cybersecurity And Social Media. In book: Cybersécurité et médias sociaux (pp.69-105). Université Laval, DOI:10.1515/9782763753294-005
21. KPMG. (2024). Third Party Risk Management. Available at https://assets.kpmg.com/content/dam/kpmgsites/ch/pdf/third-party-risk-management-boardroom-perspective.pdf
22. Liyanage, L., Arachchilage, N. A. G. & Russello, G. (2024). Sok: Identifying Limitations And Bridging Gaps Of Cybersecurity CMMs (Ccmms). Arxiv, Https://Arxiv.Org/Abs/2408.16140
23. Maleh, Y. (2022). Understanding Cybersecurity Standards. In book Cybersecurity in Morocco (pp. 13-27), Springer Nature Switzerland AG, DOI:10.1007/978-3-031-18475-8_2
24. Mansour, O. H., Raslan, A. & Ramadan, N. (2024). A Proposed Approach for Measuring Maturity Level of Software Delivery. Journal of Software Engineering and Applications, 17(2024), 228-245.
25. Marikyan, D.& Papagiannidis, S. (2025). Technology Acceptance Model: A review. In S. Papagiannidis (Ed), TheoryHub Book. Available at https://open.ncl.ac.uk / ISBN:9781739604400
26. Mohsin, K. (2022). Data Privacy and Cybersecurity. SSRN, https://ssrn.com/abstract=4299439
27. Mugo, D. G., Njagi, K., Chemwei, B., & Motanya, J. O. (2017). The TAM and its application to the utilization of mobile learning technologies. British Journal of Mathematics & Computer Science, 20(4), 1–8. http://dx.doi.org/10.9734/BJMCS/2017/29015
28. Ogega, S. (2023). Evaluating The Influence Of Some Factors On Capability MM Integration For Development (Cmmi-dev) Maturity LevelModel Integration For Development (Cmmi-dev) Maturity Level. Electronic Theses and Dissertations.8. https://scholars.indianastate.edu/etds/8?utm_source=scholars.indianastate.edu%2Fetds%2F8&utm_medium=PDF&utm_campaign=PDFCoverPages
29. Omazić, M., Labaš, D. & Uroić, P. (2023). Contingency Theory. In S. O. Idowu et al. (eds.), Encyclopedia of Sustainable Management. Springer Nature Switzerland AG, https://doi.org/10.1007/978-3-030-02006-4_1098-1
30. Payne, Y. (2022). Risk Management Theory Explained. Accessed on 28/07/2025 at https://www.iienstitu.com/en/blog/risk-management-theory-explained
31. Phillips Consulting Limited (PCL). (2019). CMMI-DEV 2.0 ML3. Available at https://www.academia.edu/42289609/CMMI_DEV_2_0_ML3
32. Rea-Guaman, A M., Feliu, T. S., Manzano, J. A. C. & Garcia, I. D. S. (2017). Comparative Study of Cybersecurity Capability Maturity Models. Conference: International Conference on Software Process Improvement and Capability Determination. DOI:10.1007/978-3-319-67383-7_8
33. Shohoud, M. (2023) Study the Effectiveness of ISO 27001 to Mitigate the Cyber Security Threats in the Egyptian Downstream Oil and Gas Industry. Journal of Information Security, 14, 152-180. https://doi.org/10.4236/jis.2023.142010.
34. Trigyn Technologies. (2025). What is CMMI DEV Level 5?. Access on 31/072025 https://www.trigyn.com/insights/what-cmmi-dev-level-5
35. Trinh, M. T. T. & Feng, Y. (2022). MM for Resilient Safety Culture Development in Construction Companies. Buildings 2022, 12, 733. https://doi.org/10.3390/buildings12060733

36. Türetken, O., & Van Looy, A. (2024). Capability and MMs in business process management. In P. Grefen, & I. Vanderfeesten (Eds.), Handbook on Business Process Management and Digital Transformation: Research Handbooks in Information Systems (pp. 303–331). Edgar Elgar. https://doi.org/10.4337/9781802206098.00022.
37. US Department of Energy. (2021). Cybersecurity Capability Maturity Model, Version 2.0. US Department of Energy Publication, Available at https://www.energy.gov/sites/default/files/2021-07/C2M2%20Version%202.0%20July%202021_508.pdf
38. US Department of Energy. (2022). Cybersecurity Capability Maturity Model C2M2. Available at https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf
39. Visure. (2025). Understanding the Different Models of CMMI: A Comprehensive Overview. Accessed on 29/07/2025 at https://visuresolutions.com/cmmi-guide/models/
40. World Health Organization (WHO). (2025). Cybersecurity and privacy maturity assessment and strengthening for digital health information systems. World Health Organization Publication, Document number: WHO/EURO:2025-11827-51599-78854 (PDF). Available at https://iris.who.int/bitstream/handle/10665/380838/WHO-EURO-2025-11827-51599-78854-eng.pdf?sequence=2
41. Saudi Arabian Monetary Authority. (2017). Cyber Security Framework Saudi Arabian Monetary Authority. Version 1.0, 1-56. Available at https://www.sama.gov.sa/en-US/RulesInstructions/CyberSecurity/Cyber%20Security%20Framework.pdf
42. Schmitz, C., Schmid, M., Harborth, D. & Pape, S. (2021). Maturity Level Assessments of Information Security Controls: An Empirical Analysis of Practitioners' Assessment Capabilities. In Computers & Security, 108(4), https://doi.org/10.3390/su141610038
43. Semrau, J. (2024). Process Improvement: A Key Element Of Effective Organization Management. in Scientific Papers of Silesian University of Technology Organization and Management Series 194. https://doi.org/10.3390/su141610038
44. Fryt, M. (2019). Process MMs – applicability and usability review World Scientific News, 129, 51–71. https://doi.org/10.1080/00207543.2022.2164087
45. Han, X., Zhang, M., Hu, Y., & Huang, Y. (2022). Study on the digital transformation capability of cost consultation enterprises based on maturity model. Sustainability, 14(16), 10038. https://doi.org/10.3390/su141610038
46. Hortovanyi, L., Morgan, R. E., Herceg, I. V., Djuricin, D., Hanak, R., Horvath, D., & Szabo, R. Z. (2023). Assessment of digital maturity: The role of resources and capabilities in digital transformation in B2B firms. International Journal of Production Research, 61(23), 8043–8061. https://doi.org/10.1080/00207543.2022.2164087
47. Hu, J., & Gao, S. (2019). Research and application of capability maturity model for Chinese intelligent manufacturing. Procedia CIRP, 83, 794–799. https://doi.org/10.1080/00207543.2022.2164087
48. Liyanage, L., Arachchilage, N. A. G., & Russello, G. (2024). SoK: Identifying limitations and bridging gaps of cybersecurity capability maturity models (CCMMs) (arXiv:2408.16140). https://doi.org/10.51594/csitrj.v5i1.699
49. Mansour, O. H., Raslan, A., & Ramadan, N. (2024). A proposed approach for measuring maturity level of software delivery. Journal of Software Engineering and Applications, 17(4), 228–245. https://doi.org/10.51594/csitrj.v5i1.699
50. Mbanaso, U. M., Abrahams, L., & Apene, O. Z. (2019). Conceptual design of a cybersecurity resilience maturity measurement (CRMM) framework. The African Journal of Information and Communication (AJIC), 23, 1–26. https://doi.org/10.3390/buildings12060733
51. Popoola, O. A., Adama, H. E., Okeke, C. D., & Akinoso, A. E. (2024). Cross-industry frameworks for business process reengineering: Conceptual models and practical executions. World Journal of Advanced Research and Reviews, 22(1), 1198–1208. https://doi.org/10.51594/csitrj.v5i1.699
52. Razikin, K., & Widodo, A. (2021). General cybersecurity maturity assessment model: Best practice to achieve payment card industry-data security standard (PCI-DSS) compliance. CommIT (Communication and Information Technology) Journal, 15(2), 91–104. https://doi.org/10.51594/csitrj.v5i1.699
53. Rohmah, U. N., Rachmadi, A., & Perdanakusuma, A. R. (2019). Penilaian tingkat kapabilitas proses akuisisi pengembangan sistem informasi menggunakan CMMI for Acquisition (CMMI-ACQ) Versi 1.3 (Studi Kasus: Dinas Komunikasi dan Informatika Kabupaten Tulungagung). Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 3(2), 2097–2104. https://jurnal.bsi.ac.id/index.php/paradigma/article/download/1358/927
54. Semrau, J. (2024). Process improvement: A key element of effective organization management. Scientific Papers of Silesian University of Technology. Organization and Management Series, 2024(194), 385–398. https://doi.org/10.1080/00207543.2022.2164087

55. Šimić, D., Ređep, N. B., Rako, S., Kadoić, N., Petegem, W. V., Rienties, B., Lanzo, N. C., Eichhorn, M., Guàrdia, L., Softić, S. K., & Tillmann, A. (2025). HELA-CMM: Capability MM for adoption of learning analytics in higher education. International Journal of Educational Technology in Higher Education, 22, Article 25. https://doi.org/10.51594/csitrj.v5i1.699
56. Trinh, M. T. T., & Feng, Y. (2022). MM for resilient safety culture development in construction companies. Buildings, 12(6), Article 733. https://doi.org/10.3390/buildings12060733
57. US Department of Energy. (2021). Cybersecurity capability maturity model (Version 2.0). https://www.energy.gov/sites/default/files/2021-07/C2M2 Version 2.0 July 2021_508.pdf
58. Vanita. (2019). Capability maturity model. International Journal of Research and Analytical Reviews (IJRAR), 6(1), 172–177. https://doi.org/10.1080/00207543.2022.2164087

Publishing and Ethical Statements / بيانات النشر والالتزام الأخلاقي

N	Publication Data in English		بيانات النشر بالعربية		م
1	Authors' Contributions	- First Author: Design, methodology, data collection, analysis, and drafting. - Second Author: Supervision, summarizing, development. - Third Author: Supervision, summarizing, final review for publication. - Forth Author: summarizing, final review for publication.	الباحث الأول: التصميم، المنهجية، جمع وتحليل البيانات، وكتابة المسودة. الباحث الثاني: الإشراف العلمي، تلخيص وتطوير الأبحاث. الباحث الثالث: الإشراف العلمي، والمراجعة النهائية للنشر. الباحث الرابع: تلخيص، والمراجعة النهائية للنشر.	مساهمة الباحثين	1
2	Conflict of Interest	No conflicts of interest.	لا يوجد أي تضارب مصالح	تضارب المصالح	2
3	Funding Sources	Self-funded (No external grant).	تمويل ذاتي (لا يوجد دعم خارجي).	مصادر التمويل	3
4	Copyright & licensed under		CC BY-NC-ND)	حقوق النشر مرخص بموجب	4
5	Review Process	Double-blind peer review	تحكيم مزدوج التعمية	الية التحكيم	5
6	Plagiarism Check	Verified via	(iThenticate)	تم التحقق عبر نظام فحص الانتحال	6
7	Data Availability	Available upon request.	متاحة عند الطلب.	إتاحة البيانات	7