International Journal of Computer Applications Technology and Research
Volume 15–Issue 03, 70 – 82, 2026, ISSN: -2319–8656
DOI:10.7753/IJCATR1503.1013

The Role of CMMI Maturity in Improving Cybersecurity Process Using CMMI Maturity Indicator Level Scale

Enaam Abdelgader Abdalla Farh
College of Computer Science and Information Systems
Aloola Colleges
Al-Ahsa, KSA

Prof: Mudawi Mukhtar Elmusharaf
College of Computer Studies
The National Ribat University
Khartoum, Sudan

Dr. Tarig Abdalkarim Abdalfadil
Faculty of Computer Science and Information Technology
ALNEELAIN UNIVERSITY
Khartoum, Sudan

Abstract:
The study explored the role played by CMMI Maturity in improving cybersecurity process using CMMI maturity indicator level scale through shedding light on certain dimensions represented in cyber process management, level of cyber risk management, level of continuous improvement, training and competence management, change management, and performance and measurement management. The study adopted the descriptive approach. The population consisted of all employees in the cybersecurity departments and divisions in public institutions. 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. The researcher drew on the theoretical literature and previous studies to construct the questionnaire and formulate its statements. The results showed that organizations under study lacked a mature system for identifying, assessing, and effectively managing cyber risks. This reflected a weakness in adopting preventative strategies or clear response plans to address potential cyber threats. There was a lack of sufficient attention to regularly monitoring and evaluating cybersecurity performance. This situation might make it difficult to determine the effectiveness of implemented measures or identify strengths and weaknesses on time. Organizations did not pay sufficient attention to employee comprehensive training or developing their cybersecurity skills. This might reflect weak training programs or a lack of opportunities to acquire the knowledge and experience necessary to address digital risks effectively. The researcher recommended strengthening the cybersecurity culture within organizations through ongoing awareness campaigns targeting all administrative and technical levels.

Keywords: CMMI - Maturity - Cybersecurity - Maturity Indicator Level Scale.

1. Introduction

Process improvement is essential for organizations because it gives tasks structure, efficiency, and consistency, boosting output and quality. Communication, decision-making, planning, management of human resources, operational activities, monitoring, assessment, and continuous improvement are all essential processes [1]. By optimizing current business processes, the organization can meet industry best practices and enhance customer satisfaction. Process improvement can benefit workflows that need to be modified without losing their core functionality [2].

Process improvement models are represented by the well-known models of "CMMI (Capability Maturity Model Integration), "Lean, Six Sigma, and the widely recognized standards defined by ISO (International Organization for Standardization). Their extensive recognition and utilization encompass multiple sectors, including software and manufacturing, where they have demonstrated the ability to strengthen efficiency, productivity, and overall operational effectiveness [3]. According to Rohmah et al. [4], CMMI serves as a framework for process enhancement, offering crucial components that support organizations in achieving more efficient process performance.

The escalation of cyber threats has rendered the enhancement of digital infrastructure security imperative [5]. Organizations can increase their cyber resilience by understanding their environment, purpose, vision, and values, regularly evaluating and improving their cybersecurity measures, coordinating their cybersecurity strategy with overarching objectives, and issuing clear instructions. Enhancing resilience within the organization can also be achieved by promoting knowledge sharing. Organizations should ensure sufficient staff and skills, develop and coordinate resources, and upskill for new environments to eliminate vulnerabilities caused by central dependency points. Furthermore, encouraging an empowered culture can facilitate sound decision-making amid uncertainty and upheaval [6].

Cybersecurity is a technique for safeguarding an organization's resources by identifying threats that could jeopardize the vital data kept in its systems. It also entails identifying, preventing, and responding to threats [7]. A well-designed cybersecurity strategy helps protect individuals and organizations against harmful attacks aimed at accessing, altering, deleting, destroying, or extorting critical data from their systems. Cybersecurity is crucial in thwarting attacks aimed at disabling or impairing a system or device's functionality. The demand for cybersecurity is increasing as the population of individuals, devices, and programmers within contemporary enterprises expands, along with the growing volume of sensitive or confidential information [8].

Organizations can use cybersecurity capability maturity models to enhance cybersecurity practices. These models assess and categorize cybersecurity capabilities across various levels. Various cybersecurity capability maturity models have been created by the industry, often by governmental organizations, to serve as national or international standards. Consequently, organizations have created maturity models for cybersecurity capabilities tailored to their specific requirements [9].

1.1 Problem Statement

Academics or practitioners have developed many MMs to assess domain-specific capabilities. These maturity models for cybersecurity and information security are highly intricate and comprehensive. Due to their complexity, they are not ideal for self-assessment but are well-suited for developing tailored improvement strategies [10]. CCMMs are becoming more important as organizations' cybersecurity posture improves in the fast-changing digital world, where organizations are more vulnerable to cybersecurity threats. CCMMs give businesses a structured way to figure out how good their current cybersecurity is, find important gaps, and set priorities for making things better. However, CCMMs don't always reach their full potential because of problems with the models themselves and problems that come up when they are put into use and adopted. These problems and limitations can make CCMMs much less effective at making cybersecurity better [11].

1.2 Research Questions

- How effective is Cyber Process Management in ensuring that digital processes within an organization are organized and coordinated securely?
- 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?
- What is the Level of Continuous Improvement in Developing Employees’ Skills and Enhancing Their Capabilities to Deal with Cyber Risks?
- To what Extent Does Training and Competence Management Contribute to Developing Employees’ Skills and Enhancing Their Ability to Deal with Cyber Risks?
- 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?
- To What Extent Does Performance and Measurement Management Contribute to Monitoring Cybersecurity Performance Indicators and Improving the Effectiveness of Security Measures within the Organization?

1.3 Research Significance

The body of literature demonstrates the increasing relevance of maturity models, particularly CMMI, in the assessment and enhancement of cybersecurity capabilities across diverse sectors. Yet, the lack of an integrated and empirical relationship with business outcomes and the lack of adaptability to context in current maturity models pose the need for robust, yet flexible, and evidence-supported frameworks. The research aims to overcome this gap by investigating the role that can be played by CMMI Maturity in improving cybersecurity process using CMMI maturity indicator level scale.

1.4 Theoretical Framework

A thorough approach to risk management, Berg's Risk Management Model (2010) entails goal-setting, risk identification, analysis, assessment or selection, treatment, monitoring, review, and stakeholder engagement. Risks can be classified as opportunities or weaknesses and are identified using SWOT and PEST analyses. Risk analysis considers current risks' causes, effects, and potentialities in addition to controls and efficacy [12]. Risk management theory is an integral part of how businesses work and plan. It means finding, evaluating, and reducing possible risks affecting an organization's goals. Risk management theory gives us helpful information about understanding and dealing with risks in several ways. Finding possible risks is the first step in risk management theory. This means looking at internal and external factors that could be threats or opportunities for the business. For instance, a business in a highly regulated field might have to deal with compliance risks, and a tech company might have to deal with cybersecurity risks [13].

2. Literature Review

Businesses are always looking to boost their competitiveness and streamline their operations [14]. Process improvement in business refers to increasing the effectiveness and cost-effectiveness of your operations. Process improvement entails implementing new systems, tactics, and technologies to improve performance and streamline workflows. In today's cutthroat market, it's becoming increasingly crucial as companies look to boost productivity while cutting expenses [15]. Process improvement is fundamentally grounded in a series of identifiable stages encompassing measurement, analysis, and enhancement of the examined processes. A comprehensive approach is essential during the enhancement phase of process management. To effectively enhance processes, organizations should be evaluated at three levels: the overall organization, the implemented processes, and the current positions [16].

Most organisations prioritise digitising business processes and creating new services and customer experiences [14]. According to Stewart [17], CMMs are instruments made to enhance procedures and encourage actions that boost company performance. These models, which date back to the 1990s, show five stages of maturity for every discipline, showing a path of evolutionary improvement from unstructured to structured processes. They assist businesses in determining their present strengths and possible areas for development. From straightforward diagrams for instant insights to extensive documents for in-depth analysis, models can offer profound insights and precise recommendations for enhancements. The idea has become more widely used and applied in many fields, positioning it as a valuable instrument for organizations seeking operational improvement.

The success of the CMM has led to a boom in the development of MMs. MMs aim to offer a methodical, step-by-step framework for achieving excellence. This framework evaluates the existing situation and provides the guidelines needed to improve to achieve enhanced levels of organizational performance. Since MMs are not restrictive, they can be created for any organizational space or process that needs to be improved. They have been applied across various domains, including supply chain management, project management, innovation, business process optimization, new product development, and human capital management [18].

Cybersecurity holds critical importance in a time characterized by rapid digitization, widespread network connectivity, and the transformative impact of technology [19]. The digital landscape introduces unprecedented threats to individuals, enterprises, and nations while fostering innovation and global connectivity. Cyberattacks pose a significant risk to networks, systems, and vital data confidentiality and integrity. Emerging trends in cybersecurity are transforming how businesses protect their systems, networks, and data from cyberattacks. The increasing application of machine learning (ML) and artificial intelligence (AI) in cybersecurity defense is a significant advancement. AI-powered systems improve threat detection by analyzing data in real time, recognizing patterns, and predicting risks, allowing faster and more flexible responses [20].

Numerous standard organizations have adopted a proactive strategy to formulate best practices, guidelines, and additional resources to aid organizations in safeguarding their data and systems. This has resulted in extensive collaboration on the development and execution of cybersecurity standards among entities including the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the International Society of Automation (ISA), ETSI, the International Telecommunication Union - Telecommunication (ITU-T), and the European Union Agency for Network and Information Security [21]. Organizations aiming to leverage technology for growth often face cybersecurity-related obstacles. Organizations need to continuously improve the maturity of their cybersecurity initiatives to cope with the changing threat environment. The efficacy of the Cybersecurity organization is, therefore, essential for the overall Cybersecurity program, business performance, and resilience. Consequently, in recent years, governments globally have intensified their efforts to enhance the protection of their national cyberspaces [22].

A process maturity is a more specific idea than organizational maturity, and it depends on the organization reaching maturity in other areas. Process maturity shows how close a developing process is to being done and can keep improving through feedback and qualitative measures [23]. The process maturity assessment is a strategic process that looks at how ready an organization is to use a process approach and how well the environment supports it. It involves examining the organization’s strategic direction, structure, and culture, which are all critical for keeping the changes that were made. Organizations need to do a process maturity assessment to make sure their process approach works [24].

Cybersecurity threats are growing more complicated for businesses all over the world. To mitigate risks and maintain operational resilience, organizations have adopted cybersecurity frameworks like the NIST Cybersecurity Framework (NIST CSF) to safeguard against data breaches and cyberattacks. Assessing an organization's cybersecurity maturity level and finding any flaws in its structure is essential. The NIST CSF is the most popular framework because of its adaptability and simplicity of use. However, not every organization can implement risk-reduction strategies, so more evaluation and dedication from the top down are required [25].

Risk management is the ongoing process of identifying, assessing, responding to, and monitoring risks. The cybersecurity risk management process is specifically aimed at addressing risks related to cybersecurity. To control the risks related to cybersecurity, Member Organizations should [26]:

- Identify Their Cyber Security Risks – "Cyber Security Risk Identification";
- Determine The Likelihood That Cyber Security Risks Will Occur And The Resulting Impact – "Cyber Security Risk Analysis";
- Determine The Appropriate Response To Cyber Security Risks And Select Relevant Controls – "Cyber Security Risk Response";
- Monitor The Cyber Security Risk Treatment And Review Control Effectiveness – "Cyber Security Risk Monitoring And Review".

This process identifies and assesses cybersecurity risks, ranks them according to their possible impact, and creates suitable risk mitigation plans. To effectively respond to new threats and uphold robust risk management, it is vital to consistently review and strengthen cybersecurity measures. Well-known frameworks, like the "NIST Cybersecurity Framework" and "ISO/IEC 27001", can provide organizations with methodical guidance in managing cybersecurity risks and developing an extensive cybersecurity program [27].

Well-defined procedures also facilitate effective teamwork and coordination. Organizations can control risks and guarantee adherence to legal, regulatory, and industry standards by implementing risk management and compliance procedures. Procedures that help reduce risks, ensure data security, and comply with applicable standards or laws may include checks, controls, and approvals [1]. Data security involves ensuring the confidentiality, integrity, and availability of information. User authentication is employed by the cloud platform to safeguard data privacy. Without a strong authentication system, users' accounts could be accessed without authorization, potentially violating privacy [28].

In this day and age, cybersecurity is a challenge for enterprises. However, enhancing an organization's internal network security might not be enough because modern enterprises rely on outside parties, and these dependencies could give cybercriminals additional avenues for attack. "Cyber Third-Party Risk Management (C-TPRM)" is a relatively new idea in the corporate sector. Every third party, whether partner or vendor, may represent a security vulnerability. Even with the strongest cybersecurity procedures, a third party could jeopardize an organization's data, clients, and reputation. Companies seek fast and straightforward methods to assess the cybersecurity risks posed by their partners [29].

Risk management departments or groups within organizations frequently manage and report cybersecurity and other external-party risk. These groups are very important for managing risk and ensuring that rules are followed. Although regulations offer guidelines on cybersecurity and external-party risk, a company's vulnerability to hacking may increase if it depends only on them. Businesses that start with regulatory standards are more vulnerable to hacking than those that only use them [30].

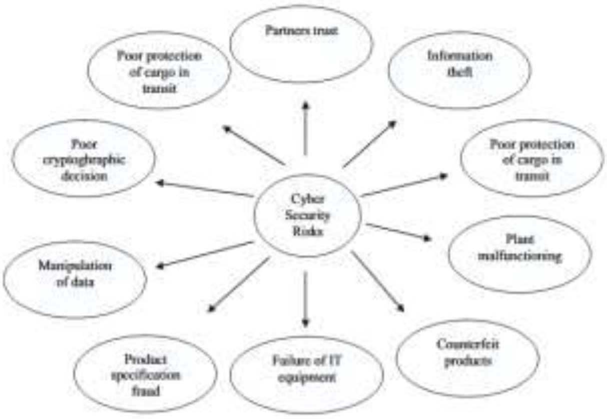

Figure 1. Types of cybersecurity risks
Source [30]

A comprehensive framework should encompass guidelines, standards, and best practices to help organizations efficiently evaluate, reduce, and handle risks associated with third-party vendors. This framework must safeguard sensitive data, systems' integrity, and collaboration between vendors and organizations across all operational tiers. Organizations can attain improved transparency, traceability, and security in third-party vendor relationships by utilizing blockchain's decentralized and immutable ledger. Blockchain guarantees that all transactions and interactions between organizations and vendors are securely documented and authenticated, mitigating the risk of tampering, unauthorized access, and data breaches. Organizations must initiate thorough risk assessments to identify and evaluate cybersecurity threats presented by third-party vendors [31].

Companies need to maintain a solid incident response framework to manage and reduce the impact of any possible breaches. This plan should spell out what needs to be done, who is responsible for what, and how everyone involved should talk to each other in the event of a third-party-related incident. Organizations can improve their resilience, safeguard their resources and maintain stakeholder confidence through comprehensive and forward-thinking third-party risk management. As the world becomes more connected, looking for new ways to protect the organization's interests in external relationships is essential. This ongoing process requires constant vigilance, flexibility, and teamwork. Organizations are by definition material risk cases due to the complexity of the business [32].

3. Methodology:

The study adopted the descriptive approach, as a general study of a phenomenon existing in a particular group, in a specific place and at present; it is a method of analysis and interpretation in an organized scientific manner to reach specific goals for a social problem. The population consists of all employees in the cybersecurity departments and divisions in public institutions. 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.

3.1 Characteristics of the Study Sample:

The frequencies and percentages of the general information for the study sample individuals, which consists of demographic data including (gender, age, academic qualification, job title, years of experience in the field of cybersecurity, type of sector the organization belongs to, and organization size), were calculated as follows:

Distribution of Sample Individuals According to Gender:

Table 1. Distribution of Sample Individuals According to Gender

Gender	Frequencies	Percentages
Male	231	%60.2
Female	153	%39.8
Total	384	%100

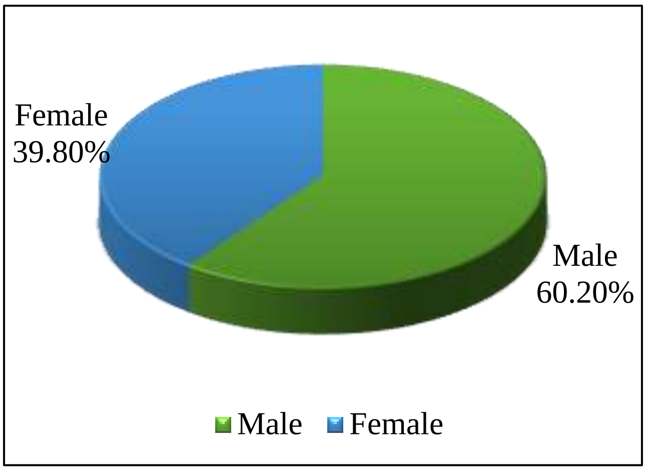

Figure 2. Distribution of Sample Individuals According to Gender

It is clear from the previous figure that the highest percentage obtained by the sample individuals according to gender is (60.2%) for Males, and the lowest percentage is (39.8%) for Females

Distribution of Sample Individuals According to Academic Qualifications:

Table 2. Distribution of Sample Individuals According to Academic Qualifications

Academic Qualifications	Frequencies	Percentages
Diploma	84	%7.6
Bachelor	151	%31.5
Master	104	%41.1
Doctorate	45	%19.8
Total	384	%100

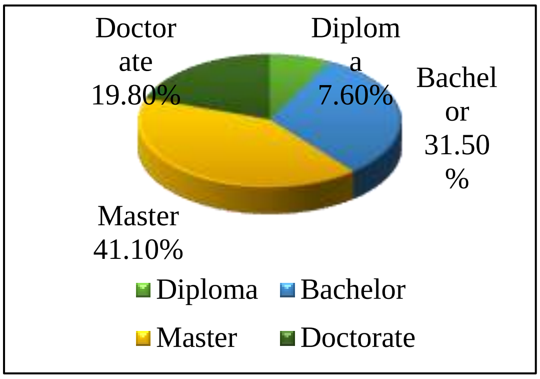

Figure 3. Distribution of Sample Individuals According to Academic Qualifications

It is evident from the previous figure that the highest percentage obtained by the sample individuals according to the academic qualification is (41.1%) for Master, followed by (31.5%), which is related to Bachelor, and (19.8%), which is related to Doctorate. In comparison, the lowest percentage is (7.6%), which is related to Diploma.

Distribution of Sample Individuals According to Years of Experience in the Field of Cybersecurity:

Table 3. Distribution of Sample Individuals According to Years of Experience in the Field of Cybersecurity

Years of Experience in the Field of Cybersecurity	Frequencies	Percentages
Less than 3 years	23	%6.0
From 3 to 5 years	122	%31.8
From 6 to 10 years	92	%24.0
More than 10 years	147	%38.2
Total	384	%100

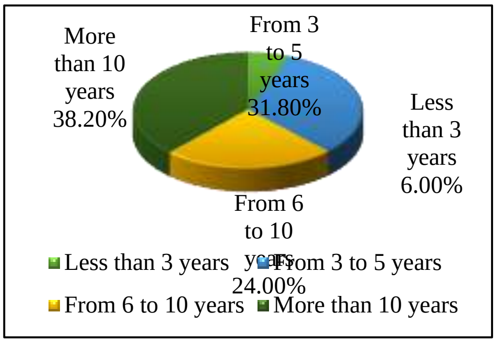

Figure 4. Distribution of Sample Individuals According to Years of Experience in the Field of Cybersecurity

Based on the previous figure, the highest percentage obtained by the sample individuals according to the Years of experience in the field of cybersecurity is (38.2%), which is related to More than 10 years, followed by (31.8%), which is related to From 3 to 5 years, and (24.0%), which is related to From 6 to 10 years, while the lowest percentage is (6.0%), which is related to Less than 3 years.

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:

Description of the Study Tool (Questionnaire):
The final version of the questionnaire consisted of two main parts:

- **First Part:** 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.
- **Second Part:** 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).

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.

- **Validity of the Tool (Questionnaire)** The validity of a tool means ensuring that it will measure what it was designed to measure. Furthermore, the validity of the questionnaire was determined as follows:

A. First Axis: Cyber Process Management: Internal consistency was calculated by computing the Pearson correlation coefficient between each statement's score and the total score of the first axis. The following table demonstrates the results:

Table 4. Pearson Correlation Coefficient Between the Score of Each Statement and the Total Score of the First Axis

Statement number	Correlation coefficient	Statement number	Correlation coefficient	Statement number	Correlation coefficient
1	.858**	2	.846**	3	.765**
4	.811**	5	.852**	6	.870**
7	.860**	8	.783**	9	.880**
10	.911**				

** Statistically significant at the (0.01) level.

It is evident from the previous table that the correlation coefficients of the statements with the total score of the first axis were all statistically significant at the level of (0.01). Additionally, all values of the correlation coefficients were significant, ranging between (.765**-.911**), indicating the availability of a high degree of internal consistency validity for the axis statements.

B. Second Axis: Cyber Risk Management:

Internal consistency was determined by calculating the Pearson correlation coefficient between the score of each statement and the total score of the second axis, as presented in the following:

Table 5. Pearson Correlation Coefficient Between the Score of Each Statement and the Total Score of the Second Axis

Statement number	Correlation coefficient	Statement number	Correlation coefficient	Statement number	Correlation coefficient
11	.925**	12	.888**	13	.846**
14	.862**	15	.802**	16	.903**
17	.821**	18	.775**	19	.769**
20	.785**				

** Statistically significant at the (0.01) level.

The table above reveals that the correlation coefficients of the statements with the total score of the second axis were all statistically significant at the level of (0.01). All correlation coefficients were significant, ranging between (.769**-.925**), which indicates a high degree of internal consistency validity of the axis statements.

C. Third Axis: Continuous Improvement:

By measuring the Pearson correlation coefficient between the score of each statement and the total score of the third axis, internal consistency was ascertained, as seen below:

Table 6. Pearson Correlation Coefficient Between the Score of Each Statement and the Total Score of the Third Axis

Statement number	Correlation coefficient	Statement number	Correlation coefficient	Statement number	Correlation coefficient
21	.825**	22	.859**	23	.875**
24	.843**	25	.805**	26	.778**
27	.741**	28	.917**	29	.883**
30	.912**				

** Statistically significant at the (0.01) level.

From the above, it can be seen that the correlation coefficients of the statements with the total score of the third axis were all statistically significant at the (0.01) level. Moreover, all values of the correlation coefficients were significant, as they ranged between (.741**-.917**), which indicates the availability of a high degree of internal consistency validity of the axis statements.

D. Fourth Axis: Training and Competence Management:

Internal consistency was assessed by estimating the Pearson correlation coefficient between the score of each statement and the total score of the fourth axis, as displayed in the following:

Table 7. Pearson Correlation Coefficient Between the Score of Each Statement and the Total Score of the Fourth Axis

Statement number	Correlation coefficient	Statement number	Correlation coefficient	Statement number	Correlation coefficient
31	.832**	32	.714**	33	.729**
34	.780**	35	.745**	36	.806**
37	.775**	38	.874**	39	.839**
40	.799**				

** Statistically significant at the (0.01) level.

As indicated in the prior table, the correlation coefficients of the statements with the total score of the fourth axis were all statistically significant at the level of (0.01). All values of the correlation coefficients were significant, as they ranged between (.741**-.874**), suggesting a high degree of internal consistency validity of the axis statements.

E. Fifth Axis: Change Management: Internal consistency was identified by obtaining the Pearson correlation coefficient between the score of each statement and the total score of the fifth axis, as shown in the following:

Table 8. Pearson Correlation Coefficient Between the Score of Each Statement and the Total Score of the Fifth Axis

Statement number	Correlation coefficient	Statement number	Correlation coefficient	Statement number	Correlation coefficient
41	.854**	42	.881**	43	.862**
44	.810**	45	.834**	46	.758**
47	.876**	48	.799**	49	.790**
50	.933**				

** Statistically significant at the (0.01) level.

It appears from the preceding table that the correlation coefficients of the statements with the total score of the fifth axis were all statistically significant at the significance level of (0.01). In addition, all values of the correlation coefficients were significant, as they fluctuated between (.758**-.933**), reflecting the availability of a high degree of internal consistency validity of the axis statements.

F. Sixth Axis: Performance and Measurement Management: The following explains how the Pearson correlation coefficient between the score of each statement and the total score of the sixth axis was used to identify internal consistency:

Table 9. Pearson Correlation Coefficient Between the Score of Each Statement and the Total Score of the Sixth Axis

Statement number	Correlation coefficient	Statement number	Correlation coefficient	Statement number	Correlation coefficient
51	.850**	52	.790**	53	.897**
54	.830**	55	.743**	56	.796**
57	.816**	58	.822**	59	.862**
60	.857**				

** Statistically significant at the (0.01) level.

According to the above, the correlation coefficients of the statements with the total score of the sixth axis were all statistically significant at the level of (0.01). All values of the correlation coefficients were significant, fluctuating between (0.897**-0.743**), signifying the availability of a high degree of internal consistency validity of the axis statements

Reliability of the Tool (Questionnaire):

Tool reliability refers to ensuring that the answer will be almost the same when the tool is repeatedly administered to the same people at different times. The reliability of the questionnaire is as follows:

- **Reliability of the First Axis: Cyber Process Management:** Cronbach's alpha was used to assess the reliability of the statements in the first axis. The results are shown in the following table:

Table 10. Cronbach's Alpha Coefficient for the Statements of the First Axis

First Axis	Cronbach's alpha
Overall reliability coefficient	.954

The previous table presents that the reliability coefficient value for the statements of the first axis was high, with an overall reliability coefficient of (.954). These reliability coefficient values indicate the validity of the questionnaire's first axis for application and the possibility of relying on and trusting its results.

- **Reliability of the Second Axis: Cyber Risk Management:** Cronbach's alpha was utilized to determine the reliability of the statements in the second axis. The outcomes are presented in the following table:

Table 11. Cronbach's Alpha Coefficient for the Statements of the Second Axis

Second Axis	Cronbach's alpha
Overall reliability coefficient	.952

The previous table exhibits that the reliability coefficient for the statements of the second axis was high, as the overall reliability coefficient reached (.952). These reliability coefficients indicate that the questionnaire's second axis is valid for use and that its results can be relied on and trusted.

- **Reliability of the Third Axis: Continuous Improvement:** The reliability of the statements in the third axis was evaluated using Cronbach's alpha. The following table displays the results:

Table 12. Cronbach's Alpha Coefficient for the Statements of the Third Axis

Third Axis	Cronbach's alpha
Overall reliability coefficient	.955

Based on the above, the reliability coefficient for the statements of the third axis came in a high value, as the value of the overall reliability coefficient reached (.955). These reliability coefficients reflect that the third axis of the questionnaire is valid for implementation and that its results are reliable and trustworthy.

- **Reliability of the Fourth Axis: Training and Competence Management:** The following table indicates how Cronbach's alpha was employed to evaluate the reliability of the statements in the fourth axis:

Table 13. Cronbach's Alpha Coefficient for the Statements of the Fourth Axis

Fourth Axis	Cronbach's alpha
Overall reliability coefficient	.933

From the preceding table, it is clear that the reliability coefficient for the statements of the fourth axis received a high value, with an overall reliability coefficient of (.933). These values of reliability coefficients indicate the validity of the fourth axis of the questionnaire for application and the possibility of relying on and trusting its results.

- **Reliability of the Fifth Axis: Change Management:** Cronbach's alpha was applied to assess the reliability of the statements in the fifth axis, as shown in the following table:

Table 14. Cronbach's Alpha Coefficient for the Statements of the Fifth Axis

Fifth Axis	Cronbach's alpha
Overall reliability coefficient	.953

It is evident from the previous table that the reliability coefficient for the statements of the fifth axis had a high value, as the value of the overall reliability coefficient reached (.953). These values of reliability coefficients indicate the validity of the fifth axis of the questionnaire for application and the possibility of relying on and trusting its results.

- **Reliability of the Sixth Axis: Performance and Measurement Management:** Cronbach's alpha was applied to measure the reliability of the statements in the sixth axis, as indicated in the table below:

Table 15. Cronbach's Alpha Coefficient for the Statements of the Sixth Axis

Sixth Axis	Cronbach's alpha
Overall reliability coefficient	.948

The table above shows that the value of the reliability coefficient for the statements of the sixth axis was high, as the value of the overall reliability coefficient reached (.948). These reliability coefficient values indicate the validity of the questionnaire's sixth axis for application and the possibility of relying on and trusting its results.

4. Presentation, Discussion, and Interpretation of the Results:

4.1 Question 1: How effective is Cyber Process Management in ensuring that digital processes within an organization are organized and coordinated securely? To answer this question, the frequencies, percentages, arithmetic means, and standard deviations of the first axis statements were calculated. Then these statements were ranked in descending order according to the mean of each statement, as shown in the following table:

Table 16. 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 responsibilities within security processes.	F	156	93	70	59	6	3.87	1.153	1	High
		%	40.6	24.2	18.2	15.4	1.6				
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 table above shows that the overall mean for the first axis was (3.32), with a standard deviation of (.443) and a (moderate) response degree. Statement No. (6) A clear mechanism exists for assigning roles and responsibilities within security processes, ranked first with a mean of (3.87), a standard deviation of (1.153), and a (high) response degree. Statement No. (8) A central database is available to document daily security activities, which came in the second place with a mean of (3.78), a standard deviation of (1.282), and a high response degree. Finally, statement No. (1) All cybersecurity processes and procedures are regularly documented, with a mean of (2.81), a standard deviation of (1.522), and a (moderate) response degree. The standard deviations for the statements in the first axis ranged between (1.600-1.153), which are high values, indicating a variation in the opinions of the study sample regarding those statements. The first axis received a moderate response, which can be explained by the fact that the implementation of secure digital practices within organizations remains weak. This suggests a deficiency in adopting modern technical and administrative methods that ensure the protection and continuity of digital processes. This may be due to a lack of awareness of the importance of cyber management or to the absence of policies and procedures governing this area, both of which negatively impact work efficiency and information security. The first place obtained by the statement No. (6) A clear mechanism exists for assigning roles and responsibilities within security processes, with a high response, suggesting that the organizations under study possess an effective organizational system that clearly and accurately defines the tasks and responsibilities of each individual or department. This reflects good coordination among cybersecurity teams, enabling rapid responses to threats and minimizing the likelihood of errors or task overlap.

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? To resolve this question, the frequencies, percentages, arithmetic means, and standard deviations of the second axis statements were determined. Subsequently, these statements were arranged in descending order according to the mean of each statement, as shown in the following table:

Table 17. Frequencies, Percentages, Arithmetic Means, and Standard Deviations 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	Clear response plans are prepared for security incidents.	F	83	74	78	73	76	3.04	1.429	5	Moderate
		%	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 table above reveals that the overall mean for the second axis came with an arithmetic mean of (3.21), a standard deviation of (.460), and a response level of (moderate). In the first place was statement No. (19) The effectiveness of risk mitigation policies is evaluated after implementation, with a mean of (3.93), a SD of (1.397), and a RD of (high). Moreover, statement No. (20) An organizational culture exists that supports a risk management awareness at all levels, came in second place with a mean of (3.86), a SD of (1.479), and a RD of (high). It was followed in last place by statement No. (11) A standardized system is in place to identify and assess cyber risks with a mean of (2.72), a SD of (1.462), and a RD of (moderate), while the standard deviations for the statements of the second axis ranged between (1.503-1.393), which are high values, indicating the divergence of opinions of the study sample towards those statements.

The second axis received a moderate response, which can be explained by the fact that the organizations under study lack a mature system for identifying, assessing, and effectively managing cyber risks. This reflects a weakness in adopting preventative strategies or clear response plans to address potential cyber threats. The decline may also be attributed to limited employee awareness of the importance of digital risk management or a lack of specialized training in this area, making the organizations more vulnerable to cyberattacks and their operational impacts. The fact that statement No. (19) The effectiveness of risk mitigation policies is evaluated after implementation, which had the first place and received a high response degree, which can be explained by the fact that the organizations regularly and realistically monitor the results of security measures. This practice enables the identification of strengths and weaknesses in adopted policies and promotes their continuous improvement. It also reflects management's commitment to ensuring that the measures taken achieve the desired goal of reducing cyber risks. The fact that statement No. (11) A standardized system is in place to identify and assess cyber risks, which came last, with a moderate response, which can be interpreted as the fact that institutions lack a unified and clear mechanism for classifying and measuring risks. This may lead to differences in how risks are handled across teams and to weak coordination in cybersecurity decision-making. The decline also reflects a lack of strategic orientation towards comprehensive, systematic risk management, which calls for the development of a unified system that helps standardize criteria and procedures and enhance the ability to address digital threats more efficiently

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

The frequencies, percentages, arithmetic means, and standard deviations of the third axis statements were obtained in order to respond to this question. The following table illustrates how these statements were then sorted in descending order based on the mean of each statement:

Table 18. Frequencies, Percentages, Arithmetic Means, and Standard Deviations 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

According to the above, the third axis had an overall mean of (3.39), a standard deviation of (.473), and a (moderate) response. Statement No. (28) The organization regularly monitors cybersecurity performance indicators, ranked first with a mean of (3.84), a standard deviation of (1.465), and a (high) response degree. The second place was obtained by the statement No. (30) All improvement processes are documented in a dedicated database for future review, with a mean of (3.79), a standard deviation of (1.455), and a (high) response degree. Finally, statement No. (21) The effectiveness of security strategies is evaluated after each cyber incident, obtained the last place with a mean of (2.86), a standard deviation of (1.472), and a (moderate) response degree, meanwhile the standard deviations for the statements in the third axis ranged between (1.526 and 1.447), which are high values indicating a variation in the opinions of the sample towards those statements.

The third axis received a moderate response, suggesting that organizations do not give sufficient attention to periodically reviewing and developing their processes. This may point to weak internal evaluation mechanisms or a lack of awareness of the importance of continuous performance improvement, making current procedures prone to shortcomings or unable to adapt to new changes and challenges. The fact that statement No. (28) The organization regularly monitors cybersecurity performance indicators, ranked first with a high response degree, which can be interpreted as indicating that organizations regularly and attentively monitor their security performance results. This allows them to quickly assess the effectiveness of implemented measures, identify strengths and weaknesses, and make appropriate decisions to improve performance continuously. Furthermore, the commitment to periodic monitoring mechanisms reflects the organization's ability to enhance cybersecurity and ensure the continued protection of data and digital operations more efficiently.

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?

The frequencies, percentages, arithmetic means, and standard deviations of the fourth axis statements were gathered in order to reply to this question. The table below presents how these statements were subsequently placed in descending order based on the mean of each statement:

Table 19. Frequencies, Percentages, Arithmetic Means, and Standard Deviations 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 table above indicates that the overall mean for the fourth axis was (3.14), with a standard deviation of (.442) and a (moderate) response. Statement No. (39) Awareness campaigns are organized to promote a culture of cybersecurity, ranked first with a mean of (3.62), a standard deviation of (1.506), and a (high) response degree. The second place was given to the statement No. (36) The effectiveness of training programs is evaluated after each session, with a mean of (3.47), a standard deviation of (1.468), and a (high) response. Furthermore, the last place was occupied by statement No. (31) The organization provides regular cybersecurity training programs, with a mean of (2.71), a standard deviation of (1.506), and a (moderate) response. In contrast, the standard deviations of the statements of the fourth axis ranged between (1.392-1.546), which are high values, demonstrating a divergence in the opinions of the study sample towards those statements. The fourth axis received a moderate response degree. This can be explained by the fact that organizations do not pay sufficient attention to employee training or developing their cybersecurity skills. This may reflect weak training programs or a lack of opportunities to acquire the knowledge and experience necessary to address digital risks effectively. The first-place ranking of statement No. (39) Awareness campaigns are organized to promote a culture of cybersecurity, with a high response, which can be explained by the fact that organizations regularly educate their employees about secure practices and the importance of information protection. This attention contributes to raising awareness of cyber threats and reducing human error that could lead to security problems. The last-place ranking of statement No. (31) The organization provides regular cybersecurity training programs with a moderate response, which can be explained by the fact that organizations do not regularly offer employee training programs to enhance their skills and abilities in dealing with digital risks. This situation may lead to weak individual and collective preparedness to confront cyber threats, thereby reducing the effectiveness of existing security measures.

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?

In order to reply to this, the frequencies, percentages, arithmetic means, and standard deviations of the fifth axis statements were collected. These statements were then arranged in descending order based on the mean of each statement, as displayed below:

Table 20. Frequencies, Percentages, Arithmetic Means, and Standard Deviations of the Sample Responses to the Statements of the Fifth Axis

No.	Statement		Response rate					Mean	SD	Rank	RD
			Strongly agree	Agree	Neutral	Disagree	Strongly disagree				
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	Users are informed about the reasons for and objectives of the changes.	F	69	83	76	78	78	2.97	1.398	7	Moderate
		%	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 had an overall mean of (3.22), a standard deviation of (.444), and a (moderate) response degree. Statement No. (50) Lessons learned from previous changes are used to improve the management of future changes, which came in first place with a mean of (3.86), a standard deviation of (1.382), and a high response degree. Besides, statement No. (48) Post-implementation reviews are conducted to measure the impact of the change, which came in second place with a mean of (3.57), a standard deviation of (1.383), and a (high) response. Statement No. (41) Clear procedures are applied when making any changes to cybersecurity systems, had the last place with a mean of (2.78), a standard deviation of (1.468), and a (moderate) response, whereas the standard deviations of the statements of the fifth axis ranged between (1.468-1.285), which are high values, indicating the divergence of opinions of the study sample towards those statements. The fifth axis received a moderate response, indicating that organizations face difficulties in implementing effective strategies for managing changes related to digital systems and policies. This decline may reflect weak planning or insufficient preparation of employees when introducing changes to cyber processes, potentially leading to resistance to change or a decline in performance.

The fact that Statement No. (50) Lessons learned from previous changes are used to improve the management of future changes, ranked first, with a high response, suggesting that organizations place significant importance on learning from past experiences when implementing new changes. This focus helps avoid repeating mistakes and improve procedures and policies to meet new challenges. Furthermore, the commitment to applying lessons learned reflects the organization’s ability to improve change management efficiency and ensure the effective implementation of improvements that support operational stability and enhance the organization’s responsiveness to digital transformations.

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?

To address this, the frequencies, percentages, arithmetic means, and standard deviations of the sixth axis statements were assembled. These statements were then arranged in descending order based on the mean of each statement, as displayed below:

Table 21. Frequencies, Percentages, Arithmetic Means, and Standard Deviations of the Sample Responses to the Statements of the Sixth Axis

No.	Statement		Response rate					Mean	SD	Rank	RD
			Strongly agree	Agree	Neutral	Disagree	Strongly disagree				
51	Clear performance indicators are defined to measure cybersecurity efficiency.	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 security systems.	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 goals and standards.	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 senior management.	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 and analysis results.	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 performance indicators.	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 reports.	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 alignment with emerging trends.	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 performance are incentivized.	**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 strategic plans.	**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 overall mean for the sixth axis was (3.06), with a standard deviation of (.443) and a (moderate) response degree. The first position was obtained by statement No. (59) Departments that achieve outstanding security performance are incentivized, with a mean of (3.94), a standard deviation of (1.198), and a (high) response. Finally, statement No. (51) Clear performance indicators are defined to measure cybersecurity efficiency, had the last place with a mean of (2.62), a standard deviation of (1.398), and a (moderate) response. In contrast, the standard deviations of the statements in the sixth axis ranged between (1.459 and 1.198), which are high values, indicating a divergence in the opinions of the study sample towards those statements.

The sixth axis showed a moderate response degree, which can be explained by a lack of sufficient attention to regularly monitoring and evaluating cybersecurity performance. This situation may make it difficult to determine the effectiveness of implemented measures or identify strengths and weaknesses on time. The fact that statement No. (59) Departments that achieve outstanding security performance are incentivized, ranked first with a high response, which can be explained by the attention given to recognizing and rewarding teams that achieve good results in cybersecurity. This focus helps boost motivation and encourages employees to adhere to effective security practices. It also fosters a spirit of positive competition among teams and enhances the organization's overall performance in protecting data and digital systems.

5. Discussion

The effectiveness of Cyber Process Management in ensuring the secure organization and coordination of digital processes within the organization had a mean of (3.32), a standard deviation of (.443), and a (moderate) response degree. The level of Cyber Risk Management in the organization’s ability to identify and assess digital risks, as well as take appropriate preventive measures, came with a mean of (3.21), a standard deviation of (.460), and a (moderate) response.

The level of Continuous Improvement in developing employees’ skills and enhancing their abilities to deal with cyber risks came with a mean of (3.39), a standard deviation of (.473), and a (moderate) response degree. The extent to which Training and Competence Management contributes to developing employees’ skills and enhancing their abilities to deal with cyber risks had a mean of (3.14), a standard deviation of (.442), and a (moderate) response degreehe extent to which Change Management contributes to improving the organization’s ability to implement changes to cyber systems and policies in an organized manner had a mean of (3.22), a standard deviation of (.444), and a (moderate) response degree. The extent to which Change Management contributes to improving the organization’s ability to implement changes to cyber systems and policies in an organized manner had a mean of (3.22), a standard deviation of (.444), and a (moderate) response degree. The extent to which Performance and Measurement Management contributes to monitoring cyber performance indicators and improving the effectiveness of security measures within the organization came with a mean of (3.06), a standard deviation of (.443), and a (moderate) response degree.

Organizations need to continuously improve the maturity of their cybersecurity initiatives to cope with the changing threat environment (Hindka, 2024). The problem lies in the fact that organizations under study lack a mature system for identifying, assessing, and effectively managing cyber risks. This reflects a weakness in adopting preventative strategies or clear response plans to address potential cyber threats. There is a lack of sufficient attention to regularly monitoring and evaluating cybersecurity performance. This is inconsistent with Semrau (2024), who confirmed that organizations should be evaluated at three levels: the overall organization, the implemented processes, and the current positions. This situation may make it difficult to determine the effectiveness of implemented measures or identify strengths and weaknesses on time. In this context, Gupta et al. (2024) confirm that there is a need for a comprehensive framework that includes guidelines, standards, and best practices to help organizations efficiently evaluate, reduce, and handle risks associated cybersecurity. Organizations do not pay sufficient attention to employee comprehensive training or developing their cybersecurity skills. This may reflect weak training programs or a lack of opportunities to acquire the knowledge and experience necessary to address digital risks effectively. The researcher recommended strengthening the cybersecurity culture within organizations through ongoing awareness campaigns targeting all administrative and technical levels. There is a need for developing comprehensive cyber risk management policies that include assessment, prevention, response, and post-incident review to minimize digital threats and improve security performance, developing regular training programs aimed at enhancing employee efficiency in dealing with cyber risks and improving their practical skills. Furthermore, there is a critical need for implementing systematic change management procedures that include planning, communication, training, and follow-up to ensure employee acceptance of changes and achieve cybersecurity objectives.

6. References

1 Kastner M, Bezjak MI, Babuder M.2023. Business Process Improvement. Improvement Of Internal Certification Processes. Journal of Engineering, Management and Information Technology.1(4):199–206.

2 Mwilu OM, Wainaina L.2021. Influence of Process Improvement on Organizational Performance at Consolbase Limited. International Journal of Research and Innovation in Social Science (IJRISS.5(6):193–7.

3 Almazidi A, Anuar S.2024. Comparative Analysis of Software Process Improvement Models. Open International Journal of Informatics.12(1):1–15.

4 Rohmah UN, Rachmadi A, Perdanakusuma AR.2019. Penilaian Tingkat Kapabilitas Proses Akuisisi Pengembangan Sistem Informasi Menggunakan CMMI For Acquisition(CMMI-ACQ)Versi 1.3 (Studi Kasus: Dinas Komunikasi dan Informatika KabupatenTulungagung. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer.3(2):2097–104.

5 Hamdani SWA, Abbas H, Janjua AR, Shahid WB, Amjad MF, Malik J, et al.2021. Cybersecurity Standards in the Context of Operating System: Practical Aspects, Analysis, and Comparisons. ACM Computing Surveys.45(3):36–57.

6 Munusamy T, Khodadadi T, Zamani M.2023. Enhancing Cyber Security in Organisations by Establishing Attributes Towards Achieving Cyber Resilience. Preprints org.

7 Garba AA, Bade AM, Yahuza M, Nuhu YU.2020. Cybersecurity capability maturity models review and application domain. International Journal of Engineering & Technology.9(3):779–84.

8 Abuhamra AEA, Ali NMA, Ali AMA.2024. Concept of cyber security. International Journal of Advances in Engineering and Management (IJAEM.6(4):63–6.

9 Rea-Guaman AM, Feliu TS, Manzano JAC, Garcia IDS. Comparative Study of Cybersecurity Capability Maturity Models. 2017. Conference: International Conference on Software Process Improvement and Capability Determination; 2017.

10 Ozkan B, Spruit M. A Questionnaire Model for Cybersecurity Maturity Assessment for Critical Infrastructures. 2019. In: Fournaris A, Lampropoulos K, Tordera E, editors. Lecture Notes in Computer Science (LNCS) 11398 11398, Information and Operational Technology Security Systems First International Workshop, IOSec 2018, CIPSEC Project. Heraklion, Crete, Greece: Springer; p. 49–60.

11 Liyanage L, Arachchilage NAG, Russello G.2024. SoK: Identifying limitations and bridging gaps of cybersecurity capability maturity models (CCMMs.1–35.

12 Badin P, Hamid H.2022. Risk Management Theory And Model In Teacher Characters Building Course: A Literature Review. Anp Journal Of Social Science And Humanities.3(1):10–8.

13 FasterCapital.2025. Risk management theory: How to Incorporate Risk Management Theory into Your Business Practice and Strategy.

14 Türetken O, Looy A. Capability and MMs in business process management. 2024. In: Grefen P, Vanderfeesten I, editors. Handbook on Business Process Management and Digital Transformation: Research Handbooks in Information Systems303–31.

15 higherEd E.2023. What is Process Improvement? Why is it important?

16 Semrau J. Process Improvement: A Key Element Of Effective Organization Management. 2024. Scientific Papers of Silesian University of Technology Organization and Management Series 194.

17 Stewart A.2016. Conservation Capability MM A model for assessing organisational performance and identifying potential improvements.

18 Adekunle SA, Aigbavboa C, Ejohwomu O, Ikuabe M, Ogunbayo B.2022. A Critical Review of MM Development in the Digitisation Era. Buildings.12(2022):1–15.

19 Loishyn AA, Hohoniants S, Tkach MY, Tyshchenko MH, Tarasenko NM, Kyvliuk VS.2021. Development of the Concept of Cybersecurity of the Organization. TEM Journal.10(3):1447–53.

20 Yadav R, Kashyap G, Kumawat A, Sharma D.2019. Cybersecurity: Protecting Networks, Systems, and Data from Cyberattacks. Turkish Journal of Computer and Mathematics Education.10(3):1565–8.

21 Djebbar F, Nordström K.2023. A Comparative Analysis of Industrial Cybersecurity Standards. IEEE Access.4(2023):1–20.

22 Hindka M.2024. Design and Analysis of Cyber Security Capability Maturity Model. International Research Journal of Modernization in Engineering Technology and Science.6(3):1706–10.

23 Fryt M.2019. Process MMs – Applicability and Usability Review. WSN:129.

24 Mielcarek P.2017. Processes maturity of organization – concept and implementation. Management Forum.5(4):8–12.

25 Bernardo LM, S, Magalhães J.2025. An Evaluation Framework for Cybersecurity Maturity Aligned with the NIST CSF. Electronics.14(7):1–20.

26 Authority SAM.2017. Cyber Security Framework Saudi Arabian Monetary Authority. Version.1(0):1–56.

27 Parsola J.2022. Cybersecurity Risk Assessment and Management for Organizational Security. NeuroQuantology.20(5):5330–7.

28 Haque A, Gochhayat SP, Shetty S, Krishnappa B. Cloud-Based Simulation Platform for Quantifying Cyber-Physical Systems Resilience. 2020. In book: Simulation for Cyber-Physical Systems Engineering349–84.

29 Keskin OF, Caramancion KM, Tatar I, Raza O, Tatar U.2021. Cyber Third-Party Risk Management: A Comparison of Non- Intrusive Risk Scoring Reports. Electronics.10(1168):1–20.

30 Rasner GC. Cybersecurity and Third-Party Risk 2021. Inc, SBN: John Wiley & Sons;2021.

31 Gupta G. 2022 Managing Compliance and Auditing in Cloud [Ph.D. Thesis]: JAMK University of Applied Sciences.

32 Menexiadis ME, Xanthopoulos MC.2023. Understanding the Importance of Effective Third-Party Risk Management on Data Governance. Management Studies.11(6):307–11.