DIGITAL TRANSFORMATION AND ADMINISTRATION INNOVATION

Citation: Rahimiyan, A., Esmaeilpour, M., & Bayat, B. (2026). A Model for Implementing a Cybersecurity Maturity Model in Government Organizations. *Digital Transformation and Administration Innovation,* 4(5), 1-14.

Received date: 2026-02-04 Revised date: 2026-06-04 Accepted date: 2026-06-13 Initial published date: 2026-07-01 Final published date: 2026-09-01

A Model for Implementing a Cybersecurity Maturity Model in Government Organizations

Amirhoseyn Rahimiyan [1], Mansour Esmaeilpour [2*], Behrooz Bayat[3]

1. Department of Management, Ha.C., Islamic Azad University, Hamedan, Iran
2. Department of Computer Engineering, Ha.C., Islamic Azad University, Hamedan, Iran
3. Department of Knowledge and Information Science, Ha.C., Islamic Azad University, Hamedan, Iran

*Correspondence: esmaeilpour@iau.ac.ir

Abstract

The purpose of this study was to develop a model for implementing a cybersecurity maturity model in government organizations. In terms of purpose, the study was applied research, and in terms of methodology, it adopted an exploratory approach. The study population consisted of 13 information technology and cybersecurity managers from selected organizations who either held a doctoral degree or were doctoral candidates. Participants were selected using purposive and snowball sampling methods, and sampling continued until data saturation was achieved. The participants included 7 men and 6 women; 8 were under the age of 40 and 5 were over the age of 40. All participants had academic backgrounds in information security, information technology management, or computer engineering. Data were collected through semi-structured interviews totaling approximately 20 hours. To ensure validity, the interview questions were reviewed and refined by two university professors and three cybersecurity experts. Reliability was assessed using the test–retest method with an interval of 5 to 14 days and the participation of two experts, resulting in an overall reliability coefficient of 74.36%. Using qualitative content analysis, the interview data were analyzed through a systematic process. In the first stage, open coding was conducted, and after eliminating irrelevant data, 190 meaningful statements and conceptual codes were extracted. In the subsequent stage, these concepts were categorized into 26 thematic categories based on semantic and conceptual similarities. Finally, the categories were organized into 10 major themes, including strategic management and security planning, security education and awareness, risk assessment and management, security technologies and infrastructures, information and data security, network and communications security, access and control management, incident response and security improvement, organizational collaboration and communications, and customization and adaptability of solutions. This analytical process led to the development of a comprehensive model encompassing multiple dimensions of cybersecurity management.

Keywords: model implementation, maturity, cybersecurity, content analysis.

1. Introduction

Cybersecurity has emerged as one of the most critical strategic concerns for governments and public organizations in the era of digital transformation. The rapid expansion of digital infrastructures, cloud-based services, interconnected information systems, and data-driven governance has significantly increased the exposure of government organizations to cyber threats. As public institutions increasingly rely on information and communication technologies to deliver services, manage sensitive data, and support national functions, the consequences of cybersecurity failures extend beyond financial losses and operational

disruptions to encompass threats to national security, public trust, and societal stability. Consequently, organizations are required not only to deploy technical security controls but also to establish comprehensive frameworks that enable the systematic development, evaluation, and continuous improvement of cybersecurity capabilities (Möller, 2023; Russo et al., 2024).

In this context, maturity models have gained considerable attention as effective instruments for assessing organizational capabilities and guiding improvement initiatives. Maturity models provide structured mechanisms through which organizations can evaluate their current state, identify capability gaps, prioritize investments, and establish roadmaps for progressive development. Originally developed in quality management and software engineering domains, maturity models have evolved into widely adopted frameworks for assessing organizational readiness and performance across various disciplines. Their increasing popularity stems from their ability to translate complex organizational processes into measurable levels of development and to provide organizations with a clear vision for continuous advancement (Hein-Pensel et al., 2023; Russo et al., 2024).

The application of maturity concepts to cybersecurity has become particularly important due to the dynamic and evolving nature of cyber threats. Traditional security assessment approaches often focus on compliance with predefined controls or standards; however, cybersecurity maturity models emphasize organizational capability development, strategic alignment, and continuous improvement. These models recognize that cybersecurity effectiveness depends not only on technological solutions but also on governance structures, organizational culture, human resources, risk management practices, and institutional learning mechanisms. Therefore, cybersecurity maturity models provide a more comprehensive perspective on security management compared with conventional compliance-oriented approaches (Akhtari et al., 2022; Brezavšček & Baggia, 2025).

Recent years have witnessed a substantial increase in scholarly interest in cybersecurity maturity assessment. Systematic reviews have documented the growing diversity of cybersecurity maturity models and highlighted their application across numerous sectors, including critical infrastructure, healthcare, telecommunications, finance, and public administration. Despite this expansion, researchers have noted considerable variation among existing models regarding their dimensions, assessment criteria, implementation procedures, and contextual suitability. Consequently, organizations often encounter challenges when selecting or adapting a maturity model that appropriately reflects their operational environment and strategic requirements (Brezavšček & Baggia, 2025; Büyüközkan & Güler, 2025; Buzdugan & Căpățână, 2023).

One of the primary advantages of cybersecurity maturity models is their ability to integrate technical, organizational, and managerial aspects of security. Contemporary cybersecurity management requires coordinated actions across multiple domains, including governance, risk management, employee awareness, incident response, technology deployment, and regulatory compliance. Maturity models facilitate the alignment of these domains by establishing structured pathways for capability enhancement and performance evaluation. Such frameworks enable decision-makers to move beyond fragmented security initiatives and adopt holistic approaches to cybersecurity governance (Hindka, 2024; Koolen et al., 2024).

The importance of cybersecurity maturity assessment is particularly evident in government organizations. Public-sector institutions manage vast amounts of sensitive information and operate critical systems that support governmental functions, public services, and national infrastructures. These organizations often face unique challenges, including complex bureaucratic structures, resource constraints, diverse stakeholder expectations, legacy information systems, and evolving regulatory requirements. Consequently, implementing cybersecurity maturity models in governmental environments requires consideration of organizational, technical, legal, and cultural factors that may differ substantially from those encountered in private-sector organizations (Koolen et al., 2024; Lee et al., 2025).

Several studies have attempted to develop sector-specific cybersecurity maturity models tailored to particular organizational contexts. Research in the healthcare sector has emphasized the necessity of customized maturity frameworks that account for the unique characteristics of hospitals and healthcare systems, where patient safety, data confidentiality, and operational continuity are paramount concerns. These studies demonstrate that generic cybersecurity models may not adequately address sector-specific requirements and that contextual adaptation is often necessary to achieve effective implementation (Ahouanmenou, 2024).

Similarly, telecommunications organizations have been the focus of several maturity model initiatives due to their critical role in national communications infrastructures. Research conducted on large mobile telecommunications operators has proposed conceptual cybersecurity maturity frameworks designed to address sector-specific security challenges. Such studies highlight the significance of integrating governance, technology, risk management, and operational resilience into comprehensive maturity assessment systems (Bijani et al., 2023). Related investigations assessing information systems within telecommunications organizations have further demonstrated the practical value of maturity evaluations in identifying strengths, weaknesses, and improvement opportunities within cybersecurity programs (Abohatem & Ba-Alwi, 2024).

In the field of critical infrastructure protection, researchers have emphasized the strategic importance of cybersecurity maturity for enhancing resilience against increasingly sophisticated cyber threats. Studies focusing on critical infrastructures have proposed maturity frameworks that support the systematic evaluation of cybersecurity capabilities and facilitate long-term security planning. These investigations underscore the necessity of adopting multidimensional approaches that encompass technological, organizational, and managerial dimensions of cybersecurity governance (Akhtari et al., 2023). Similarly, cyber-resilience maturity models have been developed for command-and-control systems, emphasizing preparedness, adaptability, and recovery capabilities in response to future threats (Ramezani et al., 2023).

Another important dimension of cybersecurity maturity concerns organizational culture and human factors. Although advanced technologies play a vital role in protecting organizational assets, numerous security incidents continue to originate from human errors, inadequate awareness, or ineffective organizational practices. Consequently, cybersecurity culture has become a central component of many maturity frameworks. Research examining cybersecurity culture maturity has demonstrated that organizational awareness, leadership commitment, employee participation, and continuous learning significantly influence cybersecurity outcomes. Moreover, systematic assessment of cybersecurity culture can provide organizations with actionable insights for implementing measurable improvement initiatives (Dornheim & Zarnekow, 2024).

Technological innovation has also transformed the landscape of cybersecurity maturity assessment. Emerging technologies such as artificial intelligence, machine learning, advanced analytics, and automated threat detection systems offer unprecedented opportunities for enhancing security capabilities. However, the implementation of these technologies requires standardized governance approaches and clearly defined maturity pathways. Studies investigating defensive machine learning applications have highlighted the need for structured frameworks capable of guiding organizations in the responsible adoption and evaluation of advanced cybersecurity technologies (Alshaikh et al., 2024). Consequently, maturity models increasingly incorporate technology readiness and innovation management as critical assessment dimensions.

In addition to technological considerations, cybersecurity maturity models play an essential role in supporting regulatory compliance and organizational accountability. Organizations face growing pressure to demonstrate that they have implemented appropriate technical and organizational security measures. Maturity assessments provide evidence-based mechanisms for evaluating compliance readiness and identifying areas requiring improvement. By linking security practices to measurable maturity levels, organizations can enhance transparency, facilitate auditing processes, and strengthen stakeholder confidence in their cybersecurity programs (Koolen et al., 2024).

Despite the substantial progress achieved in cybersecurity maturity research, several limitations remain evident in the existing literature. First, many studies focus primarily on developing maturity assessment frameworks while providing limited guidance regarding practical implementation processes. Second, numerous models have been designed for specific industries or organizational contexts, thereby limiting their transferability to government organizations. Third, the majority of existing frameworks emphasize assessment rather than implementation, creating a gap between maturity evaluation and operational improvement. Finally, differences in organizational structures, governance mechanisms, and resource availability necessitate context-sensitive implementation approaches that account for the unique characteristics of public-sector institutions (Brezavšček & Baggia, 2025; Büyüközkan & Güler, 2025; Lee et al., 2025).

In government organizations, the challenge is not merely assessing cybersecurity maturity but establishing practical mechanisms for implementing maturity models in ways that align with organizational objectives, institutional structures, and operational realities. Successful implementation requires the integration of strategic management, risk assessment, technological infrastructure, information security practices, access control mechanisms, incident response capabilities, organizational collaboration, and continuous improvement processes. Furthermore, public organizations must foster security-

aware cultures and ensure leadership commitment to sustain cybersecurity maturity initiatives over time. Although previous studies have contributed valuable insights into cybersecurity maturity assessment, there remains a need for implementation-oriented frameworks capable of translating maturity concepts into actionable organizational practices (Hindka, 2024; Möller, 2023; Rouhani & Mohammadzadeh Chalki, 2024).

Given the growing importance of cybersecurity governance in the public sector and the limited availability of implementation-focused models tailored to governmental environments, this study aims to develop a model for implementing a cybersecurity maturity model in government organizations.

2. Methods and Materials

This study was applied in terms of purpose and exploratory in terms of method. The study population consisted of 13 information technology and cybersecurity managers from selected organizations who either held a doctoral degree or were doctoral candidates. Sampling was conducted using purposive and snowball sampling methods and continued until data saturation was reached. The participants included 7 men and 6 women; in terms of age, 8 participants were under 40 years old and 5 were over 40 years old. They had studied in fields related to information security, information technology management, and computer engineering. Data were collected through semi-structured interviews totaling 20 hours. To ensure validity, the interview questions were reviewed and revised by 2 university professors and 3 cybersecurity experts. Reliability was also confirmed through the test–retest method with a time interval of 5 to 14 days and with the participation of two experts, resulting in an overall reliability coefficient of 74.36%. In this study, interview data were analyzed through a systematic process using qualitative content analysis.

Table 1. Sample Characteristics

Characteristic	Number
Gender	
Male	7
Female	6
Education	
Master's degree	6
Doctoral degree	4
Doctoral candidate	3
Age	
Under 40 years	8
Over 40 years	5
Field of Study	
Information Security	4
Information Technology Management	3
Computer Engineering	2
Management	2
Information Technology Engineering	1
Computer Science	1
Interview Duration	
20 hours	13

Table 2. Reliability Percentage

Interview Title	Total Number of Codes	Number of Agreements	Number of Disagreements	Test–Retest Reliability (%)
N1	92	69	23	75%
N2	110	81	29	73.64%
Total	202	150	52	74.36%

The overall test–retest reliability was 74.36%, which is higher than 60%; therefore, it can be concluded that the reliability of the coding in this study was confirmed.

3. Findings and Results

Step 1. Preparing the Protocol and Conducting the Interviews

Initially, a protocol was prepared. Subsequently, interviews were conducted with 13 participants. The questions included in the protocol were as follows:

How can cybersecurity be managed in an integrated manner at the organizational level while supporting all departments?

What preventive programs should be developed to identify vulnerabilities and threats within the organization?

What educational measures should be taken to manage cyber risks in the organization?

How can security systems be effectively updated and improved to counter new threats?

Is institutionalizing a cybersecurity culture within the organization, particularly at the managerial level, necessary? How can this be achieved?

What processes should be implemented in the organization for the continuous assessment of cyber threats and preparedness to counter them?

How can automated security systems be used to identify and counter cyberattacks?

What programs should be developed for managing security crises and responding rapidly to threats?

How can security teams and other organizational departments be encouraged to collaborate toward cybersecurity?

What measures should be taken for the continuous updating and improvement of security infrastructures and systems?

How can emerging technologies such as blockchain be used to protect organizational data?

What measures should be adopted to enhance employees' awareness of cyber threats and risks?

How can multilayered access control systems be used to protect sensitive data?

How can artificial intelligence and other new technologies be used to identify security threats?

In your opinion, what are the most important indicators for implementing a cybersecurity maturity model in an organization?

What is your recommendation for improving the cybersecurity maturity model in government organizations?

How can a secure work environment be provided for employees to protect them from cyber threats?

What legal frameworks should be designed to protect data privacy and sensitive information in the organization?

What programs should be implemented to continuously assess and improve cybersecurity in the organization in order to prevent emerging risks?

Step 2. Open Coding

After removing irrelevant and unclear sentences, 190 meaningful statements and conceptual codes were extracted through open coding. Below, open coding for Interview No. 1 and Interview No. 12 is presented as examples.

Table 3. Open Coding for the First Interview

No.	Meaningful Statement	Initial Code (Concept)	Interview Code
1	The organization should pay attention to the development of emerging technologies to enhance cybersecurity.	Development of emerging technology	A1B1
2	Data security should be managed in an integrated manner across the entire organization.	Integrated data security	A1B2
3	Specific security training should be held for managing cyber risks.	Risk management training	A1B3
4	All employees should become aware of the importance of using encryption for sensitive data.	Awareness of encryption	A1B4
5	Preventive programs should be developed to identify vulnerabilities.	Preventive programs	A1B5
6	Cybersecurity should be institutionalized within organizational management processes.	Institutionalization of security	A1B6
7	The organization should continuously assess cyber threats and maintain preparedness to counter them.	Continuous threat assessment	A1B7
8	Security systems should be flexibly updated to counter emerging threats.	System updating	A1B8
9	Effective interaction should be established among different security teams to reduce security complexities.	Effective team interaction	A1B9
10	Automated security tools should be implemented to identify threats and cyberattacks.	Automated security tools	A1B10
11	Preparedness and rapid response programs should be designed for managing security crises.	Rapid response program	A1B11
12	Infrastructures and network security should be continuously assessed against emerging attacks.	Infrastructure assessment	A1B12
13	Sensitivity toward sensitive information and its maintenance should be increased.	Sensitivity toward sensitive information	A1B13

14	Security support systems, including 24-hour monitoring, should be established in the organization.	24-hour monitoring	A1B14
15	Cybersecurity should be positioned as a strategic priority in organizational policies.	Strategic priority of security	A1B15

Table 4. Open Coding for the Twelfth Interview

No.	Meaningful Statement	Initial Code (Concept)	Interview Code
1	A strong security culture should be established at the organizational level and observed by all employees.	Organizational security culture	A12B1
2	Continuous monitoring of security system activities should be carried out to prevent emerging threats.	Continuous monitoring of security systems	A12B2
3	Proactive review and analysis of potential threats should be used to enhance security.	Proactive threat analysis	A12B3
4	New and advanced security equipment should be used to counter cyber threats.	Use of advanced security equipment	A12B4
5	Restricted access policies should be used to ensure the protection of the organization's sensitive data.	Restricted access policies	A12B5
6	Rapid response teams should be used to counter cyberattacks and threats.	Rapid response teams	A12B6
7	Software update processes should be carried out regularly and rapidly.	Rapid software updates	A12B7
8	Periodic security tests should be used to identify system weaknesses.	Periodic security tests	A12B8
9	Users' access levels to sensitive information should be determined based on defined roles.	Determining user access based on role	A12B9
10	Organizational employees should receive regular training on cyber threats.	Continuous employee training	A12B10
11	Different encryption methods should be used to protect sensitive data.	Encryption of sensitive data	A12B11
12	Cyberattacks should be identified and prevented using threat management software.	Threat management software	A12B12
13	Diverse strategies should be used to counter internal and external cyber threats.	Strategies for countering cyber threats	A12B13
14	Continuous security tests should be used to assess threats and weaknesses.	Continuous security testing	A12B14
15	All security measures should be regularly reported and reviewed to ensure their effectiveness.	Reporting and reviewing security measures	A12B15

Step 3. Formation of Categories

Subsequently, these concepts were reviewed and integrated, and they are presented as categories based on their nature and meanings. The number of these categories was 26.

Table 5. Categories

Category	Initial Code (Concept) and Interview Code
1. Technology development and innovation	1. Development of emerging technology (A1B1) 2. Use of artificial intelligence (A6B12) 3. Use of artificial intelligence (A3B8) 4. Use of international standards (A7B2) 5. Use of blockchain (A2B11)
2. Security training and awareness	6. Risk management training (A1B3) 7. Awareness of encryption (A1B4) 8. Continuous employee training (A4B5, A12B10) 9. Continuous employee awareness (A8B2) 10. Security training courses (A11B5) 11. Training of rapid response teams (A2B8) 12. External security consulting (A3B14) 13. Training of rapid response teams (A4B15) 14. Threat awareness training (A5B3) 15. Training for countering specific threats (A6B14) 16. Informing employees (A9B7) 17. Training programs on emerging threats (A9B10) 18. Continuous employee training (A10B14) 19. Specialized training for countering cyber threats (A13B10)
3. Security planning and strategy	20. Institutionalization of security (A1B6) 21. Strategic priority of security (A1B15) 22. Appropriate security strategies (A11B8) 23. Strategies for countering cyber threats (A12B13) 24. Security protocols (A2B6) 25. Reviewing organizational security policies (A4B7) 26. Identifying and resolving security weaknesses (A4B10) 27. Internal and external security measures (A8B10) 28. Departmental security protocols (A9B12) 29. Prioritization of information security (A9B13)

4. Risk and threat assessment and management	30. Continuous threat assessment (A1B7) 31. Assessment of internal threats (A2B3) 32. Assessment of various threats (A7B1) 33. Advanced risk assessment (A11B6) 34. Analysis of abnormal behaviors (A3B4) 35. Identification of software risks (A3B13) 36. Continuous review of threats (A6B1) 37. Risk-based prioritization (A7B8) 38. Centralized threat management (A7B10) 39. Threat risk management (A7B14) 40. Threat assessment and management (A8B7) 41. Periodic vulnerability assessment (A13B1) 42. Crisis management (A3B7) 43. Internal risk management (A6B13) 44. Attention to changes in threats (A3B10)
5. Updating systems and solutions	45. System updating (A1B8) 46. Updating solutions (A2B9) 47. Regular system updating (A7B13) 48. Continuous security updating (A11B2) 49. Comprehensive process updating (A11B15) 50. Security updating (A5B11) 51. Continuous updating (A6B2) 52. Reviewing and updating security programs (A10B10) 53. Coordination of updates (A11B11) 54. Rapid software updates (A12B7) 55. Updating intrusion systems (A3B3) 56. Reviewing and updating security systems (A13B6) 57. Reviewing and updating protocols (A11B14)
6. Monitoring and monitoring systems	58. 24-hour monitoring (A1B14) 59. Periodic monitoring (A2B1) 60. Advanced monitoring (A5B2) 61. Real-time monitoring (A7B9) 62. Continuous traffic monitoring (A10B9) 63. User behavior monitoring (A4B2) 64. 24-hour monitoring (A8B4) 65. Installation of monitoring systems (A8B9) 66. Continuous monitoring of security systems (A12B2)
7. Security assessments	67. Regular security assessment (A10B8) 68. Continuous security assessment (A11B9) 69. Continuous security assessment (A4B14) 70. Reporting and reviewing security measures (A12B15)
8. Access management	71. User management (A3B5) 72. Restricted access control (A4B9) 73. Precise user management (A5B5) 74. Determining user access based on role (A12B9) 75. Restricted access to sensitive information (A13B8) 76. Multilayered access control (A3B2) 77. Reviewing access controls for data (A6B9) 78. Restricting access to data (A9B6) 79. Restricted access policies (A12B5) 80. Access management and data protection (A13B5) 81. Access restriction (A6B15)
9. Response to attacks	82. Rapid response program (A1B11) 83. Emergency support system (A4B11) 84. Detailed review of security operations (A9B14) 85. Attack countermeasure system (A2B4) 86. Countermeasure guidelines (A2B14) 87. Security simulation exercises (A7B11) 88. Countering DDoS attacks (A10B15) 89. Interaction between security processes and technology (A3B12) 90. Countering DDoS attacks using emerging technologies (A13B11) 91. Prevention of DDoS attacks (A6B10) 92. Resistance against external attacks (A8B3)
10. Network security	93. Protection of internal networks (A8B6) 94. Protection of internal networks (A5B13) 95. Network traffic control (A3B11) 96. Use of firewall and VPN (A13B7) 97. Use of secure networks (A13B13) 98. Use of VPN (A6B11) 99. Reviewing internal network security (A7B4) 100. Use of automated tools (A7B6)

11. Encryption and information security	101. Strong data encryption (A4B6) 102. Information encryption (A6B8) 103. Encryption in public networks (A9B4) 104. Encryption of sensitive data (A12B11) 105. Encryption of communications (A10B7) 106. Integrated data security (A1B2) 107. Two-factor authentication (A9B11) 108. Secure password management (A10B13)
12. Detection and identification of threats and vulnerabilities	109. Identification of emerging threats (A8B1) 110. Identification of vulnerabilities (A8B8) 111. Identification of vulnerabilities (A3B9) 112. Identification of cyber threats using advanced software (A11B10) 113. Analysis of abnormal behavior (A4B13) 114. Automated threat detection systems (A13B3) 115. Assessment of weaknesses (A5B4) 116. Use of advanced algorithms 117. Identification and countering of cyberattacks (A9B8) 118. Identification of unusual behavior (A10B4) 119. Threat analysis (A8B5) 120. Proactive threat analysis (A12B3) 121. Intrusion detection systems (A5B14) 122. Use of intrusion detection systems (A9B5)
13. Data analysis and big data	123. Advanced data analysis (A5B7) 124. Big data analysis (A6B6) 125. Analysis of security events (A7B7) 126. Prediction of attacks based on big data (A7B12) 127. Analytical systems for threat identification (A13B9)
14. Security teams	128. Effective team interaction (A1B9) 129. Collaboration among security teams (A2B2) 130. Rapid response teams (A12B6) 131. Rapid response teams (A9B3) 132. Rapid response teams (A9B15) 133. Immediate response team (A11B13)
15. Establishing security and preventing attacks and phishing	134. Phishing prevention (A10B11) 135. Phishing prevention (A4B3) 136. Prevention of unauthorized access (A5B9) 137. Preventive intrusion measures (A11B1) 138. Preventive programs (A1B5) 139. Preventive strategies (A6B3) 140. Dealing with phishing attacks (A13B14) 141. Awareness of phishing attacks (A6B4)
16. Security culture	142. Security culture-building (A2B13) 143. Organizational security culture (A12B1) 144. Employee accountability (A5B8)
17. Security tools	145. Automated security tools (A1B10) 146. Monitoring tools (A2B7) 147. Use of IDS/IPS (A11B4) 148. Threat management software (A12B12) 149. Use of advanced security equipment (A12B4) 150. Use of advanced software in threat detection (A4B4) 151. Protection of information systems using specific security tools (A10B1)
18. Security simulation and testing	152. Simulation of cyberattacks (A10B3) 153. Regular penetration testing (A11B3) 154. Regular penetration testing (A3B15) 155. Security simulation analysis (A9B1) 156. Periodic security tests (A12B8) 157. Continuous security testing (A12B14)
19. Collaboration and communications	158. Collaboration to enhance security (A7B3) 159. Coordination of security solutions (A4B8) 160. International collaborations (A10B5) 161. Alignment of security with macro-level objectives (A5B6)
20. Process documentation	162. Documentation of security measures (A7B15) 163. Regular backup (A4B12)
21. Reviewing and revising processes	164. Reviewing and revising security processes (A9B2) 165. Continuous process review (A5B15)
22. Use and strengthening of security infrastructures and systems	166. Strengthening the security of hardware infrastructures (A10B12) 167. Regular review of devices and systems (A13B12) 168. Global security infrastructures (A2B5) 169. Use of international standards for infrastructure design (A5B12) 170. Infrastructure assessment (A1B12) 171. Hardening of security systems (A11B12)

23. Communications security	172. Secure communications (A6B7) 173. Strengthening security communications (A2B15) 174. Security at all organizational levels (A13B4) 175. Secure work environment (A2B10)
24. Security of sensitive information and information privacy protection	176. Protection of sensitive information (A13B2) 177. Legal framework for protecting the privacy of sensitive information (A2B12) 178. Sensitivity toward sensitive information (A1B13) 179. Protection of sensitive data (A11B7) 180. Secure data storage (A5B10) 181. Secure data transmission (A3B6) 182. Personal information security (A4B1)
25. Customization, adaptability, and provision of dedicated security solutions	183. Design based on the organization's security needs (A3B1) 184. Design of secure systems (A5B1) 185. Separate implementation of security to counter specific threats (A6B5) 186. Customized security solutions for threat prevention (A13B5) 187. Dedicated security solutions (A10B2) 188. Attention to system scale and adaptability (A7B5) 189. System scale and adaptability (A9B9)
26. Leadership and policy governance by senior managers	190. Role of senior managers in policies (A10B6)

Step 4. Formation of Themes

In this step, based on the 26 categories obtained, themes or domains were formed, resulting in 10 themes.

Table 6. Themes

Themes	Related Categories
1. Strategic management and security planning	[1] Security planning and strategy [2] Leadership and policy governance by senior managers [3] Process documentation [4] Reviewing and revising processes
2. Security training and culture-building	[5] Security training and awareness [6] Security culture [7] Establishing security and preventing attacks and phishing
3. Risk assessment and management	[8] Risk and threat assessment and management [9] Security assessments [10] Detection and identification of threats and vulnerabilities
4. Security technology and infrastructures	[11] Technology development and innovation [12] Updating systems and solutions [13] Use and strengthening of security infrastructures and systems [14] Security tools
5. Information and data security	[15] Encryption and information security [16] Security of sensitive information and information privacy protection [17] Data analysis and big data
6. Network and communications security	[18] Network security [19] Communications security
7. Access and control management	[20] Access management [21] Monitoring and monitoring systems
8. Incident response and security improvement	[22] Response to attacks [23] Security simulation and testing
9. Organizational collaboration and communications	[24] Collaboration and communications [25] Security teams
10. Customization and adaptability of solutions	[26] Customization, adaptability, and provision of dedicated security solutions

Figure 1. Model for Implementing a Cybersecurity Maturity Model in Government Organizations

4. Discussion and Conclusion

The findings of the present study resulted in the development of a comprehensive model for implementing a cybersecurity maturity model in government organizations. Through qualitative content analysis of expert interviews, 190 conceptual codes were extracted and subsequently categorized into 26 categories and 10 overarching themes, including strategic management and security planning, security training and awareness culture development, risk assessment and management, security technologies and infrastructures, information and data security, network and communications security, access and control management, incident response and security improvement, organizational collaboration and communications, and customization and adaptability of solutions. These findings indicate that cybersecurity maturity implementation in government organizations is a multidimensional phenomenon that extends beyond technological considerations and requires simultaneous attention to managerial, organizational, cultural, human, legal, and technical dimensions.

One of the most important findings of this study was the identification of strategic management and security planning as a central theme in cybersecurity maturity implementation. The extracted categories associated with this theme included security strategy and planning, leadership and policy governance by senior managers, process documentation, and continuous review and improvement. This finding suggests that cybersecurity maturity cannot be achieved solely through technological investments but requires strong governance structures, strategic direction, and leadership commitment. The importance of governance and strategic alignment has been repeatedly emphasized in previous cybersecurity maturity literature. Researchers have argued that mature cybersecurity programs emerge when security objectives are integrated into organizational strategies and supported by executive leadership (Koolen et al., 2024; Möller, 2023). Similarly, studies examining cybersecurity maturity frameworks have highlighted governance and strategic planning as foundational dimensions influencing the success

of cybersecurity initiatives (Büyüközkan & Güler, 2025; Hindka, 2024). Therefore, the prominence of strategic management in the current model is consistent with existing theoretical and empirical evidence.

Another significant result was the emergence of security training and awareness culture development as a major theme. This theme encompassed security awareness programs, employee education, organizational security culture, phishing prevention, and preventive security behaviors. The finding highlights the critical role of human factors in cybersecurity maturity implementation. Government organizations often rely heavily on employee compliance, awareness, and security-conscious behavior to prevent cyber incidents. Consequently, cybersecurity maturity requires not only technological safeguards but also the cultivation of a security-oriented culture. This result aligns closely with studies emphasizing cybersecurity culture maturity as a determinant of organizational security effectiveness. Research has demonstrated that employee awareness, organizational learning, leadership commitment, and shared security values significantly contribute to improving cybersecurity capabilities (Dornheim & Zarnekow, 2024). Furthermore, studies focusing on cybersecurity maturity trends have consistently recognized training and awareness as key maturity dimensions that support organizational resilience against evolving threats (Brezavšček & Baggia, 2025; Buzdugan & Căpățână, 2023).

The present study also identified risk assessment and management as a core component of cybersecurity maturity implementation. This theme included continuous threat assessment, vulnerability identification, risk prioritization, threat monitoring, crisis management, and security evaluations. Such findings reflect the dynamic nature of cybersecurity, where organizations must continuously monitor emerging threats and adapt their security practices accordingly. Effective cybersecurity maturity depends on an organization's ability to systematically identify, evaluate, and mitigate risks before they materialize into significant incidents. This finding supports previous studies that have emphasized risk management as a central pillar of cybersecurity maturity models. For example, cybersecurity maturity frameworks proposed for critical infrastructures and command-and-control systems have highlighted proactive risk assessment and resilience planning as essential capabilities for confronting future threats (Akhtari et al., 2023; Ramezani et al., 2023). Likewise, maturity assessment studies have consistently reported that advanced organizations distinguish themselves through systematic risk management processes and continuous monitoring mechanisms (Abohatem & Ba-Alwi, 2024; Rouhani & Mohammadzadeh Chalki, 2024).

Another noteworthy outcome concerns the role of security technologies and infrastructures. Participants emphasized technology development and innovation, system updates, infrastructure strengthening, security tools, artificial intelligence, blockchain, and advanced monitoring systems as important dimensions of cybersecurity maturity implementation. These findings demonstrate that technological readiness remains a critical component of cybersecurity capability development. However, the results suggest that technology should be viewed as an enabler rather than the sole determinant of maturity. This interpretation is consistent with recent literature indicating that advanced technologies such as artificial intelligence, machine learning, and automated threat detection systems can significantly enhance cybersecurity effectiveness when implemented within structured governance frameworks (Alshaikh et al., 2024). Additionally, studies examining cybersecurity capability maturity have emphasized that technology investments must be integrated with organizational processes and governance mechanisms to achieve sustainable improvements in cybersecurity performance (Hindka, 2024; Lee et al., 2025).

The findings further revealed that information and data security constitute a distinct and essential domain of cybersecurity maturity implementation. This theme included encryption, privacy protection, secure data storage, secure data transmission, authentication mechanisms, and data analytics. Government organizations frequently manage sensitive personal, financial, and national information, making data protection a strategic priority. The prominence of this theme indicates that cybersecurity maturity requires comprehensive mechanisms for safeguarding information assets throughout their lifecycle. Similar conclusions have been reported in previous studies, where information protection and privacy preservation were identified as fundamental dimensions of cybersecurity maturity assessment frameworks (Ahouanmenou, 2024; Koolen et al., 2024). Furthermore, maturity models developed for healthcare and telecommunications sectors have consistently emphasized the protection of sensitive information as a critical capability area (Ahouanmenou, 2024; Bijani et al., 2023).

Network and communications security emerged as another important theme. The identified categories included secure communications, network protection, traffic monitoring, VPN utilization, firewalls, and secure networking infrastructures. These findings reflect the increasing importance of network security in contemporary digital ecosystems where government

organizations depend on interconnected systems and external communications. Cybersecurity maturity requires organizations to secure both internal and external communication channels against unauthorized access and malicious activities. This result is consistent with studies examining cybersecurity maturity models in critical infrastructure and telecommunications environments, where network security capabilities have been recognized as indispensable elements of organizational resilience (Akhtari et al., 2023; Bijani et al., 2023).

The study also identified access and control management as a fundamental cybersecurity maturity dimension. This theme incorporated user management, role-based access control, restricted access policies, multilayered access mechanisms, monitoring systems, and user activity supervision. These findings underscore the necessity of ensuring that organizational resources and sensitive information are accessible only to authorized individuals. Effective access management reduces insider threats, limits attack surfaces, and strengthens accountability mechanisms. Previous maturity model research similarly highlights access control and identity management as essential capabilities for achieving advanced cybersecurity maturity levels (Akhtari et al., 2022; Hindka, 2024). Moreover, cybersecurity maturity assessments frequently identify deficiencies in access governance as significant barriers to organizational security effectiveness (Rouhani & Mohammadzadeh Chalki, 2024).

Incident response and security improvement represented another major theme in the proposed model. The associated categories included rapid response programs, attack mitigation mechanisms, penetration testing, security simulations, emergency support systems, and operational security reviews. This finding indicates that cybersecurity maturity extends beyond prevention and includes preparedness, response, recovery, and continuous improvement capabilities. Organizations that possess mature incident response processes are better equipped to minimize the impact of cyberattacks and learn from security events. This observation aligns with research on cyber-resilience maturity, which emphasizes adaptive response mechanisms and recovery capabilities as key components of organizational preparedness against emerging threats (Ramezani et al., 2023). Similarly, maturity assessment studies have stressed the importance of security testing, simulation exercises, and incident management in strengthening cybersecurity resilience (Brezavšček & Baggia, 2025; Möller, 2023).

The emergence of organizational collaboration and communications as a distinct theme highlights the social and interdepartmental nature of cybersecurity management. The identified categories included collaboration among security teams, coordination of security initiatives, international cooperation, and alignment of security objectives with broader organizational goals. These findings suggest that cybersecurity maturity requires coordinated efforts across departments and stakeholders rather than isolated technical activities. Effective collaboration facilitates information sharing, improves situational awareness, and supports integrated security decision-making. Previous studies have similarly emphasized the value of organizational coordination and multidisciplinary approaches in enhancing cybersecurity maturity and resilience (Büyüközkan & Güler, 2025; Russo et al., 2024).

Finally, customization and adaptability of solutions emerged as a critical theme. Participants emphasized the need for tailored security designs, context-specific solutions, scalability, and adaptive security mechanisms. This finding reflects growing recognition that cybersecurity maturity models cannot be universally applied without modification. Government organizations possess unique structures, missions, regulatory obligations, and threat environments that necessitate customized implementation strategies. This result strongly supports recent literature advocating context-sensitive maturity models and adaptive implementation frameworks. Research conducted in developing countries and resource-constrained environments has shown that cybersecurity maturity initiatives are most effective when adapted to organizational realities and local conditions (Lee et al., 2025). Similarly, scholars have argued that maturity models should be sufficiently flexible to accommodate sector-specific and organizational-specific requirements (Ahouanmenou, 2024; Büyüközkan & Güler, 2025).

Overall, the findings of this study demonstrate that cybersecurity maturity implementation in government organizations is a comprehensive and multidimensional process requiring the integration of governance, culture, risk management, technology, information protection, network security, access control, incident response, collaboration, and adaptability. The proposed model extends existing cybersecurity maturity literature by shifting attention from assessment-oriented frameworks toward implementation-oriented mechanisms. While previous studies have primarily focused on measuring maturity levels, the present study contributes a practical implementation framework that can guide government organizations in systematically developing

cybersecurity capabilities and achieving sustainable cybersecurity maturity (Akhtari et al., 2022; Brezavšček & Baggia, 2025; Büyüközkan & Güler, 2025).

This study has several limitations that should be considered when interpreting the findings. First, the sample consisted of only 13 experts and managers, which may limit the generalizability of the results to all government organizations. Second, participants were selected through purposive and snowball sampling, which may have introduced selection bias. Third, the study relied exclusively on qualitative data obtained through interviews, making the findings dependent on participants' experiences and perceptions. Fourth, the proposed model has not yet been quantitatively validated or empirically tested within operational government organizations. Finally, differences in organizational size, technological maturity, governance structures, and regulatory environments may influence the applicability of the model across different governmental contexts.

Future studies should quantitatively validate the proposed model using large samples from diverse government organizations. Researchers may also examine the causal relationships among the identified themes and evaluate their relative contributions to cybersecurity maturity implementation. Comparative studies across different sectors, such as healthcare, finance, defense, and telecommunications, could provide additional insights into sector-specific implementation requirements. Longitudinal investigations may explore how cybersecurity maturity evolves over time following model implementation. Furthermore, future research could integrate emerging technologies such as artificial intelligence, machine learning, blockchain, and predictive analytics into the proposed framework and assess their impact on organizational cybersecurity maturity.

Government organizations should adopt a holistic approach to cybersecurity maturity implementation by simultaneously addressing technological, managerial, cultural, and human factors. Senior leaders should actively support cybersecurity initiatives and integrate security objectives into strategic planning processes. Continuous employee education and cybersecurity awareness programs should be established to strengthen organizational security culture. Regular risk assessments, vulnerability evaluations, and security audits should be institutionalized to ensure proactive threat management. Organizations should invest in modern security infrastructures, advanced monitoring systems, and incident response capabilities while ensuring that security solutions remain adaptable to evolving threats. Finally, interdepartmental collaboration, knowledge sharing, and continuous process improvement should be encouraged to promote sustainable cybersecurity maturity across government institutions.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all who helped us through this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Abohatem, A. Y., & Ba-Alwi, F. M. (2024). Cybersecurity Maturity Assessment of Information Systems for Yemen Telecoms. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(8s), 539-548.

Ahouanmenou, S. (2024). Towards a Cybersecurity Maturity Model Specific for the Healthcare Sector: Focus on Hospitals. International Conference on Research Challenges in Information Science, Cham. https://doi.org/10.1007/978-3-031-59468-7_16

Akhtari, M., Keramati, M., & Mousavi, S. A. E. (2022). A Comparative Comparison of Cybersecurity and Information Security Maturity Models and Extraction of Common Cybersecurity Indicators. *Passive Defense*, *13*(4), 21-38.

Akhtari, M., Keramati, M. A., & Amin Mousavi, S. A. (2023). Presenting a Cybersecurity Maturity Model for Critical Infrastructures. *Technology Development*, 22-32.

Alshaikh, O., Parkinson, S., & Khan, S. (2024). Exploring Perceptions of Decision-Makers and Specialists in Defensive Machine Learning Cybersecurity Applications: The Need for a Standardized Approach. *Computers & Security*, *139*, 103694. https://doi.org/10.1016/j.cose.2023.103694

Bijani, S., Talebi, M., Entezari, M. H., & Saleh Esfahani, M. (2023). A Conceptual Cybersecurity Maturity Model for the Country's Large Telecommunication Operators: Mobile Operators. *National Security*, *13*(48), 137-154.

Brezavšček, A., & Baggia, A. (2025). Recent Trends in Information and Cyber Security Maturity Assessment: A Systematic Literature Review. *Systems*, *13*(1), 52. https://doi.org/10.3390/systems13010052

Büyüközkan, G., & Güler, M. (2025). Cybersecurity Maturity Model: Systematic Literature Review and a Proposed Model. *Technological Forecasting and Social Change*, *213*, 123996. https://doi.org/10.1016/j.techfore.2025.123996

Buzdugan, A., & Căpățână, G. (2023). The Trends in Cybersecurity Maturity Models. Education, Research and Business Technologies: Proceedings of 21st International Conference on Informatics in Economy (IE 2022), Singapore. https://doi.org/10.1007/978-981-19-6755-9_18

Dornheim, P., & Zarnekow, R. (2024). Determining Cybersecurity Culture Maturity and Deriving Verifiable Improvement Measures. *Information & Computer Security*, *32*(2), 179-196. https://doi.org/10.1108/ICS-07-2023-0116

Hein-Pensel, F., Winkler, H., Brückner, A., Wölke, M., Jabs, I., Mayan, I. J., & Zinke-Wehlmann, C. (2023). Maturity Assessment for Industry 5.0: A Review of Existing Maturity Models. *Journal of Manufacturing Systems*, *66*, 200-210. https://doi.org/10.1016/j.jmsy.2022.12.009

Hindka, M. (2024). Design and Analysis of Cybersecurity Capability Maturity Model. *International Research Journal of Modernization in Engineering Technology and Science*, *06*(03).

Koolen, C., Wuyts, K., Joosen, W., & Valcke, P. (2024). From Insight to Compliance: Appropriate Technical and Organizational Security Measures through the Lens of Cybersecurity Maturity Models. *Computer Law & Security Review*, *52*, 105914. https://doi.org/10.1016/j.clsr.2023.105914

Lee, G., Kim, S., Lee, I., Brown, S., & Carbajal, Y. A. (2025). Adapting Cybersecurity Maturity Models for Resource-Constrained Settings: A Case Study of Peru. *The Electronic Journal of Information Systems in Developing Countries*, *91*(1), e12350. https://doi.org/10.1002/isd2.12350

Möller, D. P. (2023). Cybersecurity Maturity Models and SWOT Analysis. In *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices* (pp. 305-346). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-26845-8_7

Ramezani, R., Sepehri, M., & Aminzadeh, A. M. (2023). A Cyber-Resilience Maturity Model for Command-and-Control Systems in Confronting Future Threats. *Defense Futures Studies*, *8*(30), 39-66.

Rouhani, A., & Mohammadzadeh Chalki, M. S. (2024). Assessment of Security Maturity Level in Payment Service Provider Companies. Twenty-Second National Conference on Computer Science and Engineering and Information Technology, Babol.

Russo, N., Reis, L., Silveira, C., & Mamede, H. S. (2024). Towards a Comprehensive Framework for the Multidisciplinary Evaluation of Organizational Maturity on Business Continuity Program Management: A Systematic Literature Review. *Information Security Journal: A Global Perspective*, *33*(1), 54-72. https://doi.org/10.1080/19393555.2023.2195577