Evaluation of the Impact of Risk Management and Information Security on Cybersecurity Maturity of the Institute ABC Data Management Application

Riana Safitri[1], Darjat[2]
[1]STMIK Widya Utama
[2]Universitas Diponegoro

Article Info

Article history:

Received April, 2024
Revised April, 2024
Accepted April, 2024

Keywords:

Risk Management,
Information Security
Cyber Security Maturity
Data Management Application
Quantitative Analysis

ABSTRACT

In the contemporary digital landscape, organizations face an escalating array of cyber threats that imperil the security and confidentiality of their data assets. This quantitative study investigates the impact of risk management strategies and information security measures on the cyber security maturity of ABC Institute's data management application. Survey data were collected from 122 employees directly engaged in data management and security roles within the institute, and Structural Equation Modeling (SEM) with Partial Least Squares (PLS) was employed for data analysis. The findings reveal significant positive associations between risk management practices, information security measures, and cyber security maturity. These results emphasize the crucial role of comprehensive risk management strategies and robust information security measures in bolstering cyber resilience. Practical recommendations stemming from this study provide actionable insights for organizations aiming to fortify their cyber security posture.

Corresponding Author:

Name: Riana Safitri
Institution: STMIK Widya Utama
Email: rianasafitri07@gmail.com

1. INTRODUCTION

In today's digital landscape, organizations face a variety of cyber threats, including cyberattacks, data breaches, and insider threats, which can compromise sensitive information and disrupt operations [1]–[3]. To address these challenges, organizations must implement robust cybersecurity controls and strategies. These measures involve leveraging technologies such as machine learning, artificial intelligence, and behavioral analysis for proactive defense mechanisms. Additionally, organizations need to focus on identifying and prioritizing context-sensitive cyber vulnerabilities through sophisticated analytics and optimization frameworks. Mitigating cybercrime in an evolving organizational landscape requires a Cyber Crime Mitigation Framework (CCMF) that emphasizes detecting, assessing, analyzing, evaluating, and responding to cyber threats effectively. By understanding the evolving threat landscape, implementing security controls, and prioritizing cybersecurity measures, organizations can improve their cyber resilience and protect their valuable data assets.

ABC Institute, like many other organizations, operates in an environment where data management plays a pivotal role in its day-to-day operations. In today's digital landscape, data management systems face increasing cyber threats, which jeopardize the security and integrity of critical information stored in these systems [4]–[7]. The surge in data production and exchange increases the risk of security breaches, especially in systems such as NoSQL that may not have adequate protection mechanisms. To address these vulnerabilities, innovative approaches such as using blockchain for data management are being explored to enhance security through features such as digital signatures and hash functions. Enhancing the security of data management systems is essential to protect against malicious attacks and ensure the safe operation of critical infrastructure across multiple domains. Efforts to fortify these systems with robust security measures are essential to mitigate risks and maintain data integrity in the face of evolving cyber threats.

The importance of cyber security cannot be overstated, especially in sectors dealing with sensitive information such as educational institutions. ABC Institute recognizes the need to strengthen its cyber security measures to protect its data management application from potential threats. While the institute has implemented various risk management strategies and information security measures, the effectiveness of these initiatives in enhancing cyber security maturity remains a subject of inquiry. The effectiveness of risk management practices and information security measures in influencing the cyber security maturity of ABC Institute's data management application is not well understood. Despite implementing preventive measures, the institute needs empirical evidence to assess the impact of these measures on its overall cyber security posture. Understanding the relationship between risk management, information security, and cyber security maturity is essential for ABC Institute to make informed decisions and allocate resources effectively to mitigate cyber risks.

This study aims to address the following objectives: to investigate the relationship between risk management practices and cyber security maturity, to examine the impact of information security measures on cyber security maturity, to identify key factors within risk management and information security that contribute to cyber security maturity, and to provide actionable insights for enhancing cyber security posture based on empirical findings.

2. LITERATURE REVIEW

Each quote from the book is cited in the text, and cite the source in the bibliography. In-text citations are written like this: (Author's last name, year: page) or (Author's last name, year) for the source of the book. While citations for online sources are written like this: (Last name of author/ editor/ institution, year of posting).

2.1 Cyber Security Maturity

Cybersecurity maturity is essential for organisations to proactively address cyber threats. It involves a comprehensive approach that integrates people, processes and technology to effectively protect digital assets. Mature cybersecurity practices go beyond technical solutions, encompassing robust policies, regular risk assessments, and a security-conscious culture among employees. Various studies emphasise the importance of cybersecurity maturity assessment frameworks, such as the Cyber Resilience Maturity Assessment Tool (CRMAT) [8], the Maturity Model for Secure Software Testing (MMSST) [9], and the need for cybersecurity maturity models such as SWOT analysis [10]. These frameworks help in evaluating and improving an organisation's cybersecurity posture, ensuring readiness to combat evolving cyber risks. However, there is a gap in overarching assessment frameworks for specific sectors such as tech startups [11], which highlights the ongoing need for a customised approach to improving cybersecurity maturity across different industries.

2.2 Risk Management and Cyber Security

Risk management is critical to achieving cybersecurity maturity as it enables organizations to proactively identify, assess and mitigate potential risks [12]–[14]. By taking a proactive stance, organizations can anticipate emerging threats, prioritize mitigation efforts, and allocate resources effectively to protect their information assets [15]. Key components of effective risk management in cybersecurity include risk assessment, mitigation strategies, incident response planning, and continuous monitoring and improvement [16]. Understanding and controlling risks specific to autonomous intelligent cyber agents (AICA) is critical, as they can introduce new risks that may outweigh the benefits, they offer in cybersecurity defense. In addition, human awareness and cybersecurity training tailored to individual competence levels are essential to strengthen the human element, which is often considered the weakest link in cybersecurity.

2.3 Information Security Measures

Information security focuses on protecting the confidentiality, integrity, and availability of data through measures such as access control, encryption, and intrusion detection systems [17], [18]. Cyber security, a broader concept, encompasses the protection of all cyber assets, including devices and networks, emphasising electronic communication and physical security [19]. Legal aspects of information security in the global space are explored, highlighting the need for increased regulation and international co-operation [20]. In addition, the human factor is recognised as vulnerable to cyberattacks, emphasising the importance of educating personnel, especially in critical sectors such as the armed forces. Effective information security practices not only protect organisational assets and ensure regulatory compliance, but also contribute to improving overall cybersecurity maturity by reducing vulnerabilities and mitigating potential cyber threats.

2.4 Previous Research

Research in the field of cybersecurity resilience and risk management has investigated various aspects that influence an organisation's cyber maturity. Research has highlighted the importance of integrating a flexible security management system with operational resilience [9], which emphasises the need for mature business processes to improve organisational resilience [21]. In addition, the adoption of international standards such as ISO 27005 has been identified as a motivation for organisations to improve information security management and meet regulatory requirements [22]. In addition, senior management awareness regarding cyber resilience has been explored, indicating a difference in approach between IT and business managers, with an emphasis on pre-crisis cyber preparedness [23]. These findings collectively underscore the multi-faceted nature of cyber resilience, which is influenced by factors ranging from security governance models to leadership support and organisational culture. However, there remains a need for empirical research that quantitatively analyzes the impact of risk management practices and information security measures on cyber security maturity, particularly within specific organizational settings such as ABC Institute.

2.5 Conceptual Framework

Building upon the existing literature, this study proposes a conceptual framework that delineates the interplay between risk management, information security, and cybersecurity maturity. The framework posits that effective risk management practices, including risk identification, assessment, mitigation, and monitoring, positively influence information security measures implemented within an organization. In turn, robust information security measures contribute to enhancing the organization's cyber security maturity by safeguarding its digital assets and minimizing the likelihood and impact of cyber incidents.

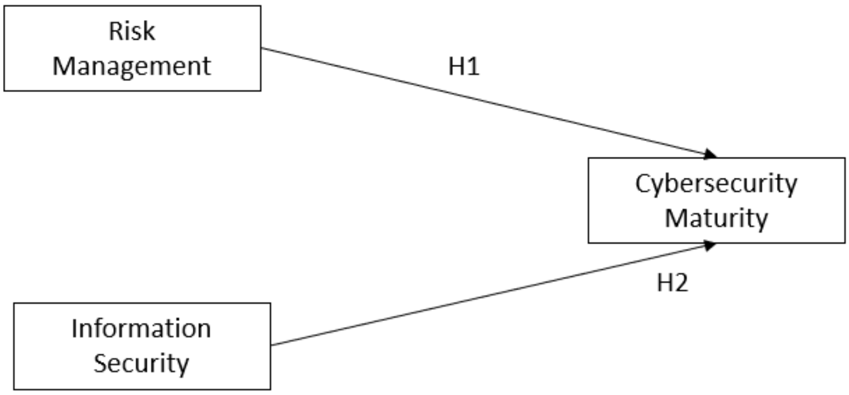

Figure 1. Conceptual Framework

3. METHODS

3.1 Research Design

This study adopts a quantitative research design to empirically investigate the influence of risk management and information security on the cyber security maturity of ABC Institute's data management application. A structured questionnaire survey will be utilized to collect data from employees directly involved in data management and security roles within the institute. The survey questionnaire will be designed based on established scales and validated constructs derived from the relevant literature.

The study population will consist of 122 employees directly engaged in data management and security-related activities within ABC Institute. A purposive sampling technique will be employed to ensure that participants possess the requisite knowledge and experience regarding the subject matter under investigation. The sample size is determined based on the principles of statistical significance and adequacy for structural equation modeling (SEM) analysis using Partial Least Squares (PLS).

Data will be collected through a structured questionnaire administered to the selected participants. The questionnaire will comprise Likert scale items designed to measure respondents' perceptions and attitudes towards various aspects of risk management, information security, and cyber security maturity. Before distribution, the questionnaire will undergo a pilot test to assess its reliability and validity and make necessary revisions.

3.2 Data Analysis

The collected data will be analyzed using Structural Equation Modeling (SEM) with Partial Least Squares (PLS) approach, which is particularly suitable for examining complex relationships among latent variables and observed variables, making it ideal for exploring the interplay between risk management, information security, and cyber security maturity. The analysis will proceed in several stages: firstly, assessing the measurement model to ensure the reliability and validity of the constructs used in the study, including evaluating internal consistency using Cronbach's alpha and composite reliability (CR), and examining convergent and discriminant validity through factor loadings and average variance extracted (AVE). Once the measurement model is validated, the structural relationships between latent constructs will be examined using SEM-PLS, assessing the direct and indirect effects of risk management practices and information security measures on cyber security maturity, examining path coefficients, significance levels, and coefficient of determination (R^2) to evaluate the strength and significance of the relationships. The final stage of analysis involves assessing the overall fit and validity of the structural model, utilizing goodness-of-fit indices such as the goodness-of-fit index (GoF), standardized root means square residual (SRMR), and normed fit index (NFI) to evaluate the adequacy of the model fit, while sensitivity analysis and bootstrapping techniques will be employed to test the robustness of the findings and identify any potential outliers or influential cases.

4. RESULTS AND DISCUSSION

4.1 Demographic Profile of the Sample

The demographic profile of the sample population comprising 122 employees directly involved in data management and security-related roles within ABC Institute is presented below:

Table 1. Demographic Sample

Demographic Characteristic	Frequency	Percentage
Gender:		
Male	78	63.93%
Female	44	36.07%
Age Group:		
20-30 years	35	28.69%
31-40 years	48	39.34%
41-50 years	29	23.77%
Over 50 years	10	8.20%
Job Position:		
Data Analyst	25	20.49%
IT Security Specialist	38	31.15%
Data Administrator	27	22.13%
Network Engineer	32	26.23%

Source: Data processed by the author (2024)

The majority of respondents were male (63.93%), with 36.07% female respondents. In terms of age distribution, the highest percentage of respondents fell within the 31-40 years age group (39.34%), followed by the 20-30 years age group (28.69%). Regarding job positions, IT Security Specialists constituted the largest proportion (31.15%), followed by Network Engineers (26.23%), Data Administrators (22.13%), and Data Analysts (20.49%).

4.2 Measurement Model

The measurement model assesses the reliability and validity of the constructs used in the study, namely Risk Management, Information Security, and Cybersecurity Maturity. Table 2 presents the loading factors, Cronbach's alpha values, composite reliability, and average variance extracted (AVE) for each observed variable within the measurement model.

Table 2. Validity and Reliability

Variable	Code	Loading Factor	Cronbach's Alpha	Composite Reliability	Average Variance Extracted (AVE)
Risk Management	RM.1	0.863	0.916	0.941	0.799
	RM.2	0.931			
	RM.3	0.914			
	RM.4	0.865			
Information Security	IS.1	0.871	0.902	0.931	0.773
	IS.2	0.901			
	IS.3	0.906			
	IS.4	0.836			
Cybersecurity Maturity	CM.1	0.899	0.887	0.922	0.747
	CM.2	0.884			
	CM.3	0.857			

	CM.4	0.815			

Source: Data processed by the author (2024)

The assessment of the measurement model reveals strong reliability and validity across all constructs. Risk Management (RM) exhibits loading factors exceeding 0.70 for all items, indicating robust relationships with the latent construct. Additionally, a high Cronbach's alpha of 0.916 reflects excellent internal consistency reliability within RM, complemented by a composite reliability of 0.941, indicating strong reliability. Similarly, Information Security (IS) demonstrates significant loading factors and high internal consistency (α = 0.902) and composite reliability (0.931). Convergent validity is evident with an AVE of 0.799 for RM and 0.773 for IS, surpassing the recommended threshold of 0.50. Likewise, Cybersecurity Maturity (CM) exhibits strong loading factors, high internal consistency (α = 0.887), and composite reliability (0.922), ensuring reliability. Although the AVE for CM slightly falls to 0.747, it still indicates adequate convergent validity, signifying robust construct representation. These findings collectively confirm the reliability and validity of the measurement model across all constructs.

Table 3. Discriminant Validity

	Cybersecurity Maturity	Information Security	Risk Management
Cybersecurity Maturity	0.764		
Information Security	0.607	0.779	
Risk Management	0.717	0.586	0.794

Source: Data processed by the author (2024)

The correlation matrix analysis confirms discriminant validity among the constructs. Cybersecurity Maturity exhibits a perfect correlation with itself, as expected. Information Security also correlates perfectly with itself. The correlation between Information Security and Cybersecurity Maturity (0.607) is lower than the square root of the AVE for Information Security (0.773), establishing their distinctiveness. Similarly, Risk Management correlates perfectly with itself, and its correlation with Cybersecurity Maturity (0.717) is lower than the square root of the AVE for Risk Management (0.799), confirming discriminant validity. Furthermore, the correlation between Risk Management and Information Security (0.586) is lower than the square root of the AVE for Risk Management, providing additional evidence of their distinctiveness. These results validate the discriminant validity of the constructs, indicating that Cybersecurity Maturity, Information Security, and Risk Management are distinct entities within the research model.

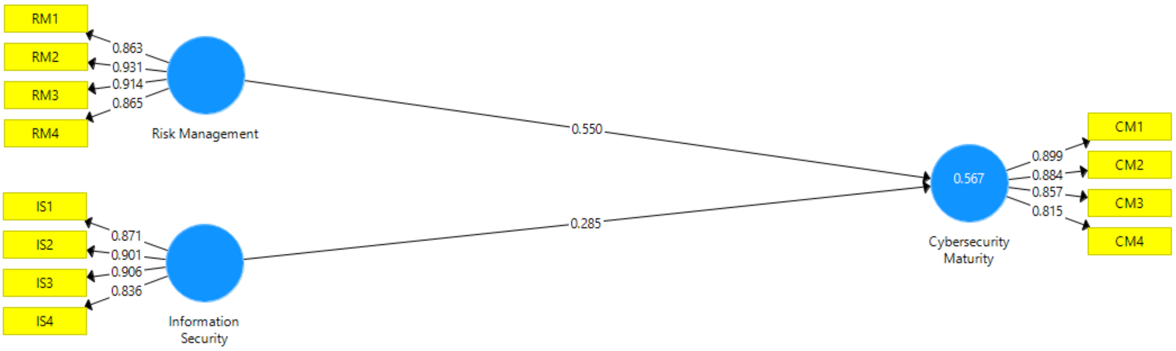

Figure 2. Internal Model Assessment

4.3 Model Fit

Model fit assessment evaluates how well the estimated model fits the observed data. Various fit indices are used to assess the goodness of fit of the model. Below are the fit indices for the Saturated Model and the Estimated Model:

Table 4. Model fit

	Saturated Model	Estimated Model
SRMR	0.057	0.057
d_ULS	0.256	0.256
d_G	0.160	0.160
Chi-Square	114.931	114.931
NFI	0.898	0.898

Source: Data processed by the author (2024)

The fit indices assessment indicates a satisfactory fit of both the Saturated Model and the Estimated Model. The Standardized Root Mean Square Residual (SRMR) values of 0.057 for both models fall below the acceptable threshold of 0.08, signifying a good fit. Furthermore, both models demonstrate d_ULS and d_G values of 0.256 and 0.160, respectively, suggesting a close alignment between the observed and reproduced covariance matrices. The Chi-Square values, although significant due to the large sample size, remain consistent at 114.931 for both models, a common occurrence in Structural Equation Modeling (SEM) and not indicative of a poor fit. Additionally, the Normed Fit Index (NFI) values of 0.898 for both models suggest a favorable fit relative to the null model, with values closer to 1 indicating better fit. These findings collectively indicate that both the Saturated and Estimated Models adequately capture the relationships between variables and provide a satisfactory representation of the observed data.

Table 5. R Square

	R Square	R Square Adjusted
Cybersecurity Maturity	0.567	0.559

Source: Data processed by the author (2024)

The R-Square (Coefficient of Determination) and R-Square Adjusted values offer insights into the proportion of variance in the dependent variable (Cybersecurity Maturity) explained by the independent variables (Risk Management and Information Security) in the SEM-PLS model. The R-Square value of 0.567 suggests that approximately 56.7% of the variance in Cybersecurity Maturity is accounted for by the included independent variables, indicating a substantial portion of the variability in Cybersecurity Maturity is captured by the model. Additionally, the R-Square Adjusted value of 0.559, which adjusts for the number of predictors in the model, provides a more conservative estimate of the explained variance. This value indicates that around 55.9% of the variance in Cybersecurity Maturity is explained by the independent variables after considering the model's complexity. These findings underscore the significant influence of Risk Management and Information Security on Cybersecurity Maturity within the SEM-PLS framework.

4.4 Hypothesis Testing

Hypothesis testing evaluates the significance of the relationships between independent variables (Information Security and Risk Management) and the dependent variable (Cybersecurity Maturity) in the regression model. The results of hypothesis testing are typically assessed using t-statistics and p-values.

Table 6. Hypothesis Testing

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values
Information Security -> Cybersecurity Maturity	0.285	0.297	0.088	3.248	0.001
Risk Management -> Cybersecurity Maturity	0.550	0.542	0.093	5.888	0.000

Source: Data processed by the author (2024)

The results of hypothesis testing provide strong evidence to support the relationships between Information Security and Cybersecurity Maturity, as well as Risk

Management and Cybersecurity Maturity. For Information Security -> Cybersecurity Maturity, the original sample coefficient (O) is 0.285, with a sample mean (M) coefficient of 0.297 and a standard deviation (STDEV) of 0.088, resulting in a t-statistic (|O/STDEV|) of 3.248 and a p-value of 0.001, indicating statistical significance. This signifies those improvements in Information Security practices are associated with higher levels of Cybersecurity Maturity. Similarly, for Risk Management -> Cybersecurity Maturity, the original sample coefficient (O) is 0.550, with a sample mean (M) coefficient of 0.542 and a standard deviation (STDEV) of 0.093, resulting in a t-statistic (|O/STDEV|) of 5.888 and a p-value of 0.000, indicating high statistical significance. This highlights the critical role of proactive risk management strategies in bolstering organizational cyber resilience.

DISCUSSION

The discussion section explores and interprets the findings of the study, focusing on the relationships between risk management, information security, and cyber security maturity within ABC Institute's data management application. This section does not delve into mediation or moderation effects but rather provides an in-depth analysis of the direct associations between the variables.

Influence of Risk Management on Cyber Security Maturity

The study findings reveal a significant positive relationship between risk management practices and cyber security maturity. Organizations that prioritize risk management strategies demonstrate higher levels of cyber security maturity, indicating that a proactive approach to identifying, assessing, and mitigating risks contributes to overall cyber resilience. The importance of risk management in strengthening an organization's defences against cyber threats is well documented [15], [24]–[27]. Implementing a robust risk management framework and process enables organizations to anticipate and mitigate potential cyber risks effectively, thereby improving the overall cybersecurity posture. By integrating structured language models and entity frameworks, organizations can unify systems and processes to automate cybersecurity functions at different operational levels, ensuring a holistic approach to risk management. In addition, understanding and controlling risks specific to autonomous intelligent cyber agents (AICA) is critical to preventing unintended consequences and increasing confidence in cyber defence mechanisms. Alignment of risk management strategies with security testing tools and mobile security frameworks helps detect vulnerabilities and defects during the software development stage, contributing to the overall security of the software system.

Impact of Information Security on Cyber Security Maturity

Similarly, the study findings indicate a significant positive relationship between information security measures and cyber security maturity. Organizations that invest in information security technologies and practices exhibit higher levels of cyber security maturity, underscoring the importance of safeguarding data assets against unauthorized access, manipulation, and disclosure. Effective information security measures, including access control, encryption and intrusion detection systems, are essential to mitigate cyber risks and maintain the confidentiality, integrity and availability of organisational data [28], [29]. Previous research highlights the importance of information security in improving overall cyber resilience [30]. Organisations face a myriad of cyber threats, which necessitates the implementation of strong security controls to protect sensitive information and ensure compliance with legal frameworks [31]. Measures such as user education, authentication and encryption are essential components of a comprehensive security strategy to combat evolving cyber threats and improve data protection. Developing effective information security policies and procedures is critical to protecting information assets and mitigating security threats. By adopting these measures, organisations can proactively defend themselves against cyberattacks and strengthen their resilience in the face of increasing cybersecurity challenges.

Practical Implications

The findings of this study have several practical implications for organizations aiming to enhance their cyber security posture. Firstly, organizations should prioritize the implementation of robust risk management frameworks and processes to proactively identify and mitigate potential cyber risks. This includes conducting regular risk assessments, developing incident response plans, and fostering a culture of risk awareness among employees. Secondly, organizations should invest in information security technologies and practices to safeguard their data assets against cyber threats. This may involve deploying encryption protocols, implementing access controls, and conducting regular security audits to detect and mitigate vulnerabilities.

Limitations and Future Research Directions

Despite the contributions of this study, several limitations should be acknowledged. Firstly, the findings are based on data collected from a single organization, limiting the generalizability of the results. Future research could replicate the study in diverse organizational contexts to validate the findings. Additionally, the study focused on direct relationships between variables and did not explore potential mediation or moderation effects. Future research could investigate these relationships to provide a more comprehensive understanding of the mechanisms through which risk management and information security influence cybersecurity maturity.

5. CONCLUSION

In summary, this study elucidates the pivotal role of risk management and information security in enhancing the cyber security maturity of ABC Institute's data management application. The empirical evidence underscores the importance of proactive risk management practices and stringent information security measures in safeguarding organizational assets against cyber threats. By effectively managing risks and implementing robust security controls, organizations can bolster their cyber resilience and mitigate the likelihood and impact of cyber incidents. The insights gleaned from this research offer valuable guidance for organizations seeking to strengthen their security posture in an increasingly digitized environment. Moving forward, continued research in this domain is essential to further refine our understanding of cyber security dynamics and inform the development of targeted strategies to combat emerging cyber threats.

REFERENCES

[1] A. Yeboah-Ofori and F. A. Opoku-Boateng, "Mitigating cybercrimes in an evolving organizational landscape," *Contin. Resil. Rev.*, vol. 5, no. 1, pp. 53–78, 2023.

[2] S. Hore, F. Moomtaheen, A. Shah, and X. Ou, "Towards optimal triage and mitigation of context-sensitive cyber vulnerabilities," *IEEE Trans. Dependable Secur. Comput.*, vol. 20, no. 2, pp. 1270–1285, 2022.

[3] C. B. Silaule, L. M. Makhubele, and S. P. Mamorobela, "A model to reduce insider cybersecurity threats in a South African telecommunications company," *South African J. Inf. Manag.*, vol. 24, no. 1, pp. 1–8, 2022.

[4] N. Chaudhry, M. M. Yousaf, and M. T. Khan, "Security assessment of data management systems for cyber physical system applications," *J. Softw. Evol. Process*, vol. 32, no. 2, p. e2241, 2020.

[5] B. Diène, J. J. P. C. Rodrigues, O. Diallo, E. L. H. M. Ndoye, and V. V Korotaev, "Data management techniques for Internet of Things," *Mech. Syst. Signal Process.*, vol. 138, p. 106564, 2020.

[6] A. Nikiforova, "Data security as a top priority in the digital world: preserve data value by being proactive and thinking security first," in *The International Research & Innovation Forum*, Springer, 2022, pp. 3–15.

[7] M. Y. Jung and J. W. Jang, "Data management and searching system and method to provide increased security for IoT platform," in *2017 International conference on information and communication technology convergence (ICTC)*, IEEE, 2017, pp. 873–878.

[8] G. Alam, S. Mahmood, M. Alshayeb, M. Niazi, and S. Zafar, "Maturity model for secure software testing," *J. Softw. Evol. Process*, 2023.

[9] V. E. Kulugh, U. M. Mbanaso, and G. Chukwudebe, "Cybersecurity Resilience Maturity Assessment Model for Critical National Information Infrastructure," *SN Comput. Sci.*, vol. 3, no. 3, p. 217, 2022.

[10] O. Kuzmenko, H. Yarovenko, and L. Perkhun, “Assessing the maturity of the current global system for combating financial and cyber fraud,” *Stat. Transit. new Ser.*, vol. 24, no. 1, pp. 229–258, 2023.

[11] D. P. F. Möller, “Cybersecurity Maturity Models and SWOT Analysis,” in *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices*, Springer, 2023, pp. 305–346.

[12] S. Chockalingam, E. Nystad, and C. Esnoul, “Capability Maturity Models for Targeted Cyber Security Training,” in *International Conference on Human-Computer Interaction*, Springer, 2023, pp. 576–590.

[13] M.-E. Paté-Cornell and M. A. Kuypers, “A probabilistic analysis of cyber risks,” *IEEE Trans. Eng. Manag.*, vol. 70, no. 1, pp. 3–13, 2021.

[14] E. J. Wibowo and K. Ramli, “Impact of Implementation of Information Security Risk Management and Security Controls on Cyber Security Maturity (A Case Study at Data Management Applications of XYZ Institute),” *J. Sist. Inf.*, vol. 18, no. 2, pp. 1–17, 2022.

[15] K. Jakimoski, A. Bennett, and A. Holliday, “Positioning Cyber Security Risk Management Within a Consolidated Security Platform,” in *Building Cyber Resilience against Hybrid Threats*, IOS Press, 2022, pp. 134–144.

[16] H. I. Kure and A. O. Nwajana, “Protection of critical infrastructure using an Integrated Cybersecurity Risk Management (i-CSRM) framework,” in *5G Internet of Things and Changing Standards for Computing and Electronic Systems*, IGI Global, 2022, pp. 94–133.

[17] R. R. Asaad and V. A. Saeed, “A Cyber Security Threats, Vulnerability, Challenges and Proposed Solution,” *Appl. Comput. J.*, pp. 227–244, 2022.

[18] K. I. Jones and R. Suchithra, “Information Security: A Coordinated Strategy to Guarantee Data Security in Cloud Computing,” *Int. J. Data Informatics Intell. Comput.*, vol. 2, no. 1, pp. 11–31, 2023.

[19] L. Huiyuan, “The The importance of information security as an integral part of the cyber security program,” *«Вестник ВИСВ»*, no. 53, pp. 35–43, 2023.

[20] L. A. Alexei and A. Alexei, “The difference between cyber security vs information security,” *J. Eng. Sci.*, no. 4, pp. 72–83, 2022.

[21] J. Marquez-Tejon, M. Jimenez-Partearroyo, and D. Benito-Osorio, “Integrated security management model: a proposal applied to organisational resilience,” *Secur. J.*, pp. 1–24, 2023.

[22] L. A. Sincorá, M. P. V. de Oliveira, H. Zanquetto-Filho, and M. Z. Alvarenga, “Developing organizational resilience from business process management maturity,” *Innov. Manag. Rev.*, vol. 20, no. 2, pp. 147–161, 2023.

[23] A. S. C. Junior and C. H. Arima, “Cyber risk management and iso 27005 applied in organizations: A systematic literature review,” *Rev. FOCO*, vol. 16, no. 02, pp. e1188–e1188, 2023.

[24] M. H. Zahedi, A. R. Kashanaki, and E. Farahani, “Risk management framework in Agile software development methodology.,” *Int. J. Electr. Comput. Eng.*, vol. 13, no. 4, 2023.

[25] H. Zafar, “Critical Success Factors for an Effective Security Risk Management Program,” *Int. J. Syst. Softw. Secur. Prot.*, vol. 13, no. 1, pp. 1–26, 2022.

[26] E. S. Mandrakov, D. A. Dudina, V. A. Vasiliev, and M. N. Aleksandrov, “Risk Management Process in the Digital Environment,” in *2022 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, IEEE, 2022, pp. 108–111.

[27] S. Alghaithi, A. Alkaabi, H. Al Hamadi, N. A. Al-Dmour, and T. M. Ghazal, “A study of risk management frameworks and security testing for secure software systems,” in *2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, IEEE, 2022, pp. 1–4.

[28] C. L. Smith, “Security technology in the protection of assets,” *Handb. Secur.*, pp. 656–682, 2014.

[29] M. N. Masrek, T. Soesantari, A. Khan, and A. K. Dermawan, “Examining the relationship between information security effectiveness and information security threats,” *Int. J. Bus. Soc.*, vol. 21, no. 3, pp. 1203–1214, 2020.

[30] A. Al Mehairi, R. Zgheib, T. M. Abdellatif, and E. Conchon, “Cyber Security Strategies While Safeguarding Information Systems in Public/Private Sectors,” in *International Conference on Electronic Governance with Emerging Technologies*, Springer, 2022, pp. 49–63.

[31] B. Kör and B. Metin, “Understanding human aspects for an effective information security management implementation,” *Int. J. Appl. Decis. Sci.*, vol. 14, no. 2, pp. 105–122, 2021.