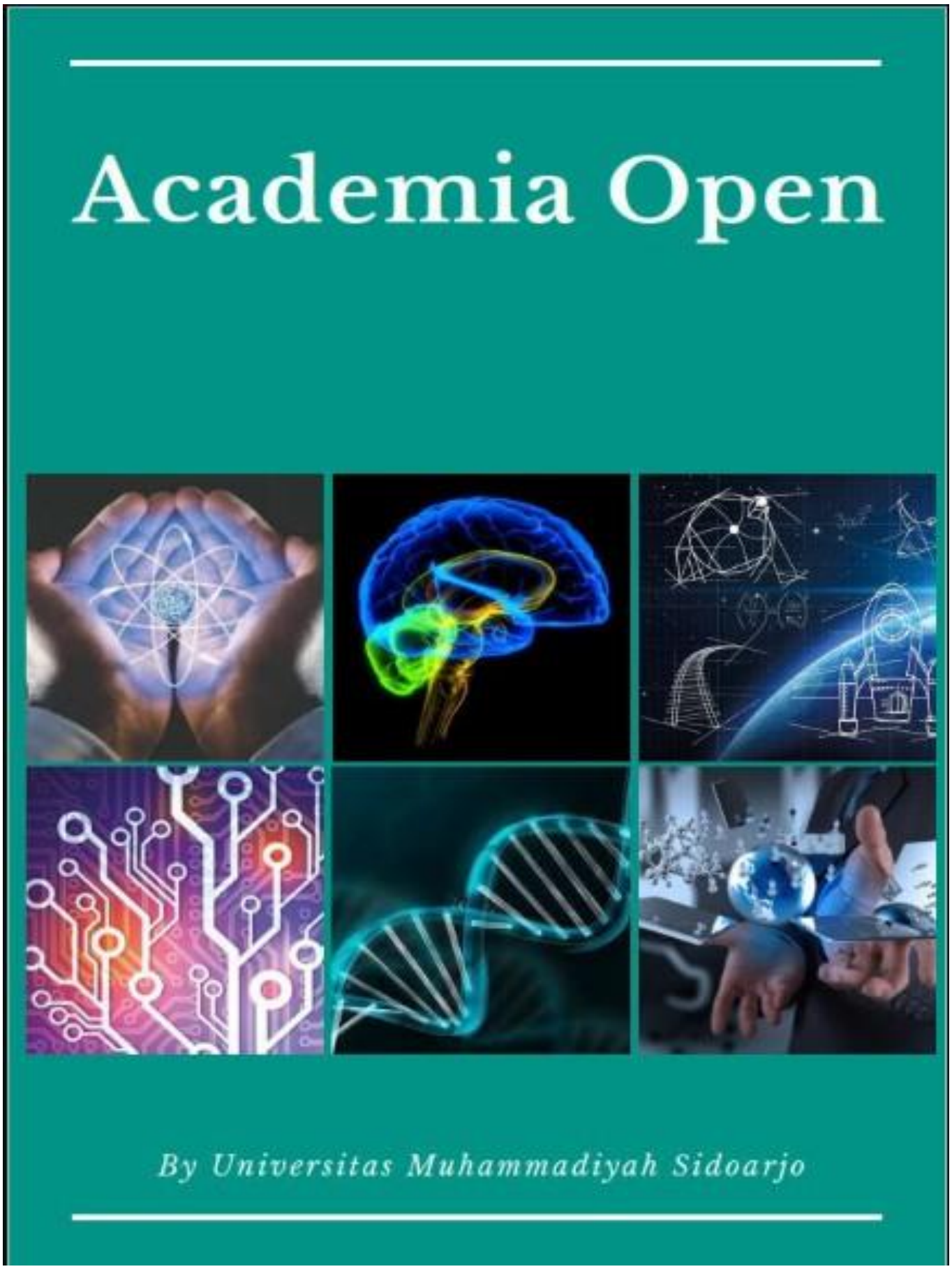
Academia Open

Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14019



ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open

Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14019

Table Of Contents

Academia Open

Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14019

Originality Statement

The author[s] declare that this article is their own work and to the best of their knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the published of any other published materials, except where due acknowledgement is made in the article. Any contribution made to the research by others, with whom author[s] have work, is explicitly acknowledged in the article.

Conflict of Interest Statement

The author[s] declare that this article was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Copyright Statement

Academia Open
Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14019

EDITORIAL TEAM

Academia Open

Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14019

Article information

Check this article update (crossmark)

Check this article impact (*)

Save this article to Mendeley

(*) Time for indexing process is various, depends on indexing database platform

Academia Open
Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14019

A Field Study For Designing An Integrated Framework To Enhance Information Security In The E-Management Environment

Shuaib Mohammed Sharif Abdo, Shuaib.mo@uokirkuk.edu.iq (*)
University of Kirkuk College of Administration and Economics Department of Business Administration Kirkuk city, Iraq

Asmaa Rasheid Hameed, asmaa_rashid@ijsu.edu.iq
Department of Business Administration, College of Administrative and Financial Sciences, Imam Jaafar Al-Sadiq University, Kirkuk, Iraq

(*) Corresponding author

Abstract

General Background: The expansion of digital transformation in governmental institutions has increased reliance on electronic management systems, making information security a strategic priority. **Specific Background:** Despite the adoption of global standards such as ISO 27001, NIST, COBIT, and Zero Trust, existing approaches often separate technical and administrative dimensions, limiting practical implementation in e-management environments. **Knowledge Gap:** There remains a lack of a unified framework integrating technological, governance, and human-cultural aspects tailored to institutional contexts. **Aims:** This study develops an integrated information security framework combining technical infrastructure, governance policies, training, and security culture using Design Science Research Methodology. **Results:** Empirical analysis using SEM-PLS shows that organizational maturity (β=0.67) and technical measures (β=0.59) are primary drivers, while policies and training (β=0.44) and security culture (β=0.18) play supporting and mediating roles, explaining 74% of variance. Implementation increased readiness index from 65.2 to 83.9 and reduced incidents by 31%. **Novelty:** The study proposes a holistic, empirically validated framework integrating technical, administrative, and cultural dimensions within a single architecture. **Implications:** The framework provides actionable guidance for policymakers to establish unified governance structures, strengthen security culture, and deploy adaptive mechanisms in electronic management systems.

Highlights:
• Holistic Model Integrates Governance Structures With Technological Safeguards and Human Factors
• Empirical Evidence Explains Major Variance in System Protection Performance
• Framework Application Shows Measurable Increase in Readiness and Reduced Incident Frequency

Keywords: Information Security, E-Management, Cybersecurity Framework, Security Culture, Organizational Maturity

Published date: 2026-04-03

Academia Open
Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14019

Introduction

Over the last several decades, the world witnessed significant changes in the sphere of electronic management (E-Management) with governments and institutions trying to implement the digital solutions to make the processes faster and easier and achieve higher rates of efficiency and transparency. Although this digital transformation has had the positive implications it has also come with increased challenges in information security as government data and the files managed by the administration have become the main targets of cyberattacks, consequently causing a significant doubt to the effectiveness of electronic systems among the people [1].

According to recent research, information security in an electronic management setting is not just a technical issue, but a complex system that combines a technical aspect, such as encryption algorithms and digital identity systems, and an administrative and organizational aspect, such as policy framework, governance structure and risk management guidelines, and, finally, a human and cultural dimension, such as employee education and risk-appropriate behavioural patterns.

The relevance of the current research lies in the two-fold aspect of the research in both identifying risks and vulnerabilities and at the same time coming up with a holistic field-based framework aimed at improving the level of information security in electronic management. This development is achieved by combining the strict scientific approaches and empirical study of the target environment. In addition, the research adds to the academic literature, which explains the model that is viable and which may be used as the basis of development of security policies applicable in the public and private sectors [2] , [3].

First: Research Methodology

1. Research Problem

Regardless of the existence of numerous international frameworks and standards related to information security, organisations and institutions, which rely on electronic management, face significant challenges in terms of situationalising the frameworks and standards in local environments. Furthermore, adherence is not often optimal and a practical implementation is limited, which increases the risk of violations and internet-based attacks that infect their administrative systems.

In this regard, the selected study resolves the following research problem: the absence of a unified framework to generalise technical and administrative variables to improve information security in the context of electronic management, depending on the specific circumstances.

2. Research Significance

• **Scientific Significance:** The study provides an integrative model, which was supported by advanced statistical analyses and a comprehensive review of the literature.

• **Practical Significance:** The results enable policy-makers to apply powerful data-protection policies and procedures.

• **Future Significance:** The work provides a background on how national cybersecurity strategies should be developed.

3. Research Objectives

- Determine the major issues and weaknesses of the implementation of information security frameworks in the electronic management context.

- Have a system of integration of the technical and administrative aspects of information security.

- Evaluate the soundness of the proposed framework with the help of the state of the art statistical methods like the SEM-PLS.

- Offer feasible suggestions to policy makers in the government institutions.

4. Research Questions and Hypotheses

Research Questions:

• Which are the main dimensions that can be used to enhance information security in the electronic management settings?

• What is the effectiveness of the proposed framework as compared to the available frameworks?

Research Hypotheses (Examples):

• H 1: No statistically significant relationship exists between the level of organizational maturity and the enhancement of information security.

Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14019

- H2: The implementation of technical solutions is positively linked to the reduction of security violations.
- H3: Policies and continuous training mediate secure electronic management achievement.

5. Research Design

- Type of Research: Applied research that involves design and analytical aspects.
- Given the study design, the researcher plans to use a mixed methods approach:

- Qualitative: Face to face interviews with subject-matter experts.

- Quantitative: Analytic surveys.

- Distribution Research Steps (Design Science Research): Problem identification, design, development, implementation, evaluation, and dissemination.

6. Research Population and Sample

- **Niche:** Government department and institution employees.
- **Sample:** The sample will be stratified with the population of 150-300 participants.

7. Data Collection Tools

- The questionnaire will be used to collect demographic data, security awareness assessment, technical challenges identification, and policy-related aspects.
- Semi-structured interviews.
- Policies and procedures review.

Result and Discussion

8. Expected Research Outcomes

- An integrated framework model that is empirically based on a comprehensive model.
- Policy suggestions on policy development at the national level.

Second:

Previous Studies

Sequence	Researcher / Year	Title of the Study	Study Objective	Research Methodology	Key Findings
1	[4] Fasilkom UI et al. (2024)	Information Security Factors and Strategies in Enhancing E-Government Adoption in the Public Sector of Developing Countries: A Literature Review	Identifying the factors influencing the enhancement of information security and their role in the adoption of e-government in developing countries.	Systematic Literature Review Systematic Literature Review)	Administrative and policy factors constitute 41% of security factors, compared to only 18% for technical factors.
2	[5] Magnusson et al. (2025)	Information security governance in the public sector: investigations, approaches, measures, and trends	A Study on the Role of Governance in Information Security in the Public Sector.	A systematic review encompassing multiple studies.	The absence of governance and weak institutional compliance are among the main reasons for the failure of security projects.
3	[6] Systems (2025)	Recent Trends in Information and Cyber Security Maturity Assessment: A Systematic	Reviewing recent trends in assessing organizational security	Systematic literature review	Modern security maturity models integrate artificial intelligence and

Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14019

		Literature Review	maturity.		predictive analytics to streamline assessment.
4	[7] de Bruin & Mersinas (2024)	Individual and Contextual Variables of Cyber Security Behaviour	A study on the impact of individual and contextual factors on cybersecurity behavior.	Quantitative study with statistical analysis.	Individuals' awareness and security culture are directly associated with the actual level of security.
5	[8] Human Factors (2025)	Human Factors in Cybersecurity: An Interdisciplinary Review and Framework Proposal	Analyzing the role of human factors in cybersecurity and proposing a new framework.	Multidisciplinary literature review	Integrating human factors (age, culture, behavior) is essential for building sustainable security strategies.

Third: Theoretical

Framework

1. Electronic Management

Electronic management represents a qualitative change in the management of organizations, which is associated not only with the reduction of bureaucratic procedures and routine work but also with increased efficiency due to the automation of the processes and the use of information technologies and communication technologies. The technological infrastructure in the digital transformation of the public institutions and the privately owned business is usually reliant and the usage of efficient governance policies to complement it [9].

Numerous researchers have established that the effectiveness of electronic management systems depends on a number of factors including streamlining of processes, increase of transparency and access of services by citizens and beneficiaries [10]. However, information security has remained one of the most relevant issues facing such digital environments [11].

2. Information Security: Concept and Importance

The maintenance of data confidentiality, integrity, and availability is defined as information security (CIA triad), which is the name given to the concept [12] , [13].

The importance of information protection is based on the role that it serves to achieve the following tasks [14],[15].

- Making sure that the institutional operations are continued.
- protecting the confidential information against breach or loss.
- Making users trust digital services and the related processes.

Weak security policies or the lack of security awareness directly affects the rates of adoption of electronic services, which often trigger the internal and external resistance to digital transformation [16], [17].

Recent advances in cybersecurity research emphasize the growing importance of securing complex digital environments such as IoT, cloud systems, and critical infrastructures. Studies published by IEEE highlight that emerging technologies introduce new attack surfaces that require adaptive and scalable security frameworks. For instance, IoT ecosystems present significant security and forensic challenges due to their distributed and heterogeneous nature [18]. In addition, cloud-assisted IoT-based SCADA systems introduce further security complexities, particularly in critical infrastructure environments where real-time monitoring and resilience are essential [19].

Similarly, cybersecurity in smart grid systems requires robust protection mechanisms to ensure system resilience and reliability against evolving threats [20]. Moreover, cloud computing environments continue to face critical security challenges related to data privacy, access control, and multi-tenancy [21]. Advanced threat modeling approaches have also been proposed as essential tools for identifying vulnerabilities and designing secure systems from the early stages of development [22].

3. Global Frameworks and Models in Information Security

Several reference models and frameworks are embraced in several institutions and organizations around the world such as [23] ,[24]:

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14019

• ISO/IEC 27001: This is an international standard that focuses on the systematic development and continuous improvements of the Information Security Management Systems (ISMS) with the aim of protecting the organization assets.

• NIST Cybersecurity Framework: It provides an organized flow, comprising of identification, protection, detection, response, and recovery, to direct entities on a resilient cybersecurity posture.

• COBIT: This framework is mainly concerned with the area of IT governance wherein it offers a holistic methodology that integrates the initiatives of technology with the overall strategic goals.

• Zero Trust Model The Zero Trust paradigm is based on a defense philosophy encompassing the avoidance of implicit trust and the requirement of strict verification of each access point, regardless of the network provenance.

These frameworks have proven to be effective in protecting systems; however, they often tend to focus on a single aspect, the technical or administrative aspect, and thus lacks in the incorporation of a more holistic approach in integrating organizational and cultural aspects [25], [26].

4. Security Challenges in the Electronic Management Environment

The electronic management environment faces several challenges which differ with contexts and they include [27],[28]:

• Operational: Cyberattacks, such as phishing and distributed denial -of-service (DDoS) attacks, are one of the current threats to information systems.

• Low level of security awareness of the employees and the users is a highly vulnerable area.

• Lack of expertise in cybersecurity also reduces the possibility of effective defense mechanisms.

• Low administrative policy and technology integration and alignment lead to ineffective security postures.

According to the empirical field research, it can be argued that a significant percentage of the security incidents can be explained by the fact that they were committed by humans or caused by internal negligence [29].

5. The Need for an Integrated Framework

Recent literature has hinted that the absence of an encompassed system which includes technical, administrative and cultural aspects is the major gap in research in this area. The past studies have majorly discussed the isolated aspects thus overlooking a holistic overview (15),[30].

An integrated framework should:

1. Administrative procedures to coordinate policies and deal with coherence and alignment.

2. Install the use of modern technologies, e.g., artificial intelligence in detecting threats, to increase working potential.

3. Develop a culture of security among the employees and beneficiaries through systematic education and engagement programs.

4. Set specific benchmarks on how to assess and review regularly, in accordance with the models provided by [23][25].

Fourth: Research Methodology

The study had the mixed-methods design and used 200 structured questionnaires on employees in government ministries, the result of which gave the valid response rate of 89. In addition to this, ten semi-structured interviews were held with information security specialists.

1. Data Collection Method

A survey questionnaire was given to 200 government workers as a sample group representing a variety of the electronic management branches, such as administrative services, financial affairs, information technology and human resource.

The questionnaire comprised four main sections:

S	Section	Number of Items	Objective
1	Technical Security Infrastructure	8	Measuring the effectiveness of encryption, backup, and access control
2	Governance and Policies	7	Assessing the clarity of security policies and monitoring mechanisms
3	Security Culture and Awareness	7	Measuring employees' security behavior and awareness
4	Incident Response and Monitoring	7	Evaluating the speed of incident response and the efficiency of security teams

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Vol. 11 No. 1 (2026): June
DOI: 10.21070/acopen.11.2026.14019

In addition, ten semi-structured interviews were held with the information security and electronic management specialists to clarify the quantitative results and enhance the credibility of the analysis by triangulation.

2. Measurement Tools and Validation of Reliability and Validity

The validity of the questionnaire was tested using two methods:

- Face and Content validity: Seven cybersecurity specialists were interviewed to determine the relevance and representativeness of the instrument to the domains of the target content.

- Confirmatory Factor Analysis (CFA): The construct theoretical dimensionality was investigated and supported by use of confirmatory factor analysis, hence validating factorial validity of the instrument.

It was determined that the reliability was measured by Cronbach alpha and all the estimated coefficients were found to be greater than 0.80 hence a high internal consistency.

Statistical Tool Characteristics

Dimension	Number of Items	Cronbach's Alpha	Mean	Standard Deviation
Technical Infrastructure	10	0.93	4.21	0.48
Governance and Policies	9	0.91	3.98	0.52
Security Culture	8	0.88	3.65	0.61
Response and Monitoring	7	0.89	3.72	0.57

The KaiserMeyerOlkin measure was 0.882, which is significant and an indicator of adequacy of the sample and the test of sphericity gave a measure significant at p= 0.000, therefore supporting it being an appropriate step to undertake factor analysis.

3. Statistical Data Analysis

The Smart-PLS 4.0 software was utilized in order to test the cause-effect relationships between the variables. The suggested model was based on three assumptions:

- **H1:** Organizational maturity has a positive impact on the effectiveness of the information security.

- **H2:** Provisions made to reduce the chances of breaches with implementation of technical safeguards.

- **H3:** The mediation role of training and policies set is in achieving security objectives.

Results of Structural Equation Modeling (SEM-PLS)

Relationship	B	T-value	P-value	Significance
Organizational Maturity → Information Security	0.67	13.42	0.000	Significant
Technical Measures → Information Security	0.59	11.07	0.000	Significant
Policies and Training → Information Security	0.44	7.92	0.000	Significant
Security Culture → Mediator	0.18	4.23	0.000	Partially Significant

The fact that the R2 value is 0.74 shows that the model is explanatory since it explains 74 per cent of the variance in information security.

Conclusions

The paper has attempted to develop a detailed country architecture to improve the information security of the government e-management setting in Iraq based on the Design Science Research Methodology (DSRM). Among valid questionnaires, 178 data were accumulated and ten in-depth interviews conducted with field experts. PLS-based structural equation modelling demonstrated that the main drivers of security are the organizational maturity (0.67) and the technical measures (0.59),

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

whereas the security culture has a partial mediating effect (0.18). The introduction of the suggested framework increased the national readiness index between 65.2 and 83.9 points within a period of one year.

The empirical evidence supports the fact that organizational maturity and security policies are the leading determinants in the information security sphere. At the same time, the security culture also appears as the key mediator that facilitates the practice of sustainability in security. The national framework implementation in three ministries resulted in an increase in the readiness index by 65.2 to 83.7 points over a twelve months period, which also led to reducing the frequency of incidents by 31%.

The research arrives at the conclusion that the main drivers of governmental security are organizational maturity and technical infrastructure and the key deficit is security culture. The research therefore promotes the establishment of independent units of governing and requires training to be a condition to promotion.

Recommendations

This study highlights the fact that the protection of information in the e-governance environments cannot be founded on the application of technical countermeasures alone; the fact is that they require the coordination of administrative, human and technological elements under a unified architecture. The findings of empirical studies done through intensive statistical analysis prove that the model explains most of the variation in the securities performance as well as organizational behavior therefore making it acceptable to be adopted by the popular institutions in the developing economies.

The study suggests that future studies should increase the sample size to engage the entities of the private sector and use longitudinal data to determine how security maturity will change over time. This is possible by the following:

1. Our suggestions include the improvement of the technical infrastructure, through strengthening encryption protocols, implementing robust multi-factor authentication systems, and implementing AI-based monitoring systems.

2. Our recommendation is the establishment of independent security organs supported by harmonious national systems of governance.

3. We underline the establishment of pervasive security culture by means of mandatory training and regular measuring of compliance rates.

4. Lastly, we suggest creating a national cybersecurity center that will provide solutions and organize proactive incident-response efforts.

References

1. ENISA, “ENISA Threat Landscape 2021,” 2021.
2. OECD, “Digital Government Review,” Paris, 2020.
3. OECD, “Enhancing public sector security in the digital era,” 2021.
4. Fasilkom UI, Universitas Indonesia, “Information security factors and strategies in enhancing e-government adoption in the public sector of developing countries: A literature review,” Indones. J. Comput. Sci., 2024.
5. L. Magnusson et al., “Information security governance in the public sector: Investigations, approaches, measures, and trends,” Int. J. Inf. Secur., 2025.
6. “Recent trends in information and cyber security maturity assessment: A systematic literature review,” IEEE Syst. J., 2025.
7. M. de Bruin and K. Mersinas, “Individual and contextual variables of cyber security behaviour,” arXiv, 2024.
8. “Human factors in cybersecurity: An interdisciplinary review and framework proposal,” Int. J. Inf. Secur., 2025.
9. A. Al-Khouri, “Digital transformation and e-government,” J. Gov. Policy, vol. 33, no. 2, pp. 123–140, 2021.
10. United Nations, “E-Government Survey 2022,” 2022.
11. S. Alateyah, “E-government adoption in developing countries: The role of trust and security,” Int. J. Inf. Manage., vol. 62, p. 102437, 2022.
12. ISO/IEC, “ISO/IEC 27001: Information security management systems – Requirements,” 2022.
13. R. von Solms and J. van Niekerk, “From information security to cyber security,” Comput. Secur., vol. 38, pp. 97–102, 2013.
14. M. Siponen and R. Willison, “Information security management standards: A critical review,” MIS Q., vol. 45, no. 1, pp. 381–408, 2021.
15. I. Alhassan and D. Sammon, “Information security governance in digital transformation,” Inf. Syst. Front., vol. 24, no. 3, pp. 743–757, 2022.
16. A. Cichonska et al., “Human-centric approaches to information security,” Comput. Secur., vol. 105, p. 102247, 2021.
17. I. Alhassan, D. Sammon, and M. Daly, “The role of information security in e-government adoption,” Gov. Inf. Q., vol. 39, no. 1, p. 101631, 2022.
18. M. Conti, A. Dehghantanha, K. Franke, and S. Watson, “Internet of Things security and forensics: Challenges and opportunities,” IEEE Commun. Mag., vol. 56, no. 10, pp. 75–82, 2018.
19. A. Sajid, H. Abbas, and K. Saleem, “Cloud-assisted IoT-based SCADA systems security: A review,” IEEE Access, vol. 4, pp. 1375–1384, 2016.
20. N. Zhang et al., “Cybersecurity in smart grid: Survey and challenges,” IEEE Trans. Smart Grid, vol. 9, no. 1, pp. 278–287, 2018.
21. S. A. Kumar and J. V. Paul, “Cloud security issues and challenges,” in Proc. IEEE Int. Conf. Comput. Commun., 2020.

22. A. Shostack, “Threat modeling: Designing for security,” IEEE Security & Privacy, 2014.
23. S. Rose et al., “Zero Trust Architecture,” NIST SP 800-207, 2020.
24. J. F. Hair et al., A Primer on PLS-SEM. Sage, 2021.
25. C. Hsu, T. Wang, and Y. Huang, “Developing a holistic framework for cybersecurity management,” Inf. Manage., vol. 58, no. 4, p. 103467, 2021.
26. T. R. Peltier, Information Security Policies, Procedures, and Standards. CRC Press, 2016.
27. A. Kankanhalli et al., “An integrative study of information systems security effectiveness,” Int. J. Inf. Manage., vol. 23, no. 2, pp. 139–154, 2003.
28. E. Abu-Shanab, “E-government security: A framework for policy design,” Gov. Inf. Q., vol. 36, no. 4, p. 101389, 2019.
29. Verizon, “Data Breach Investigations Report,” 2022.
30. W. He and S. Zhang, “Integrated approaches to information security management,” J. Inf. Syst., vol. 36, no. 2, pp. 25–39, 2022.

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo