Journal of Knowledge-Research Studies

Assessment of Information Security Management Performance in Government Organizations Based on ISO/IEC 27002

Adel Soleimani Nezhad[1], Fariborz Doroudi[2]*, Masoomeh Tahmasbi [3]

Received: July, 27, 2025; Revised: October, 8, 2025
Accepted: October, 21, 2025; Published: March, 1, 2025

Abstract

Purpose: This study aimed to evaluate the performance of information security management in government organizations in Kerman city based on the ISO/IEC 27002 standard.

Methodology: The research employed a descriptive-survey design. Data were collected using a standardized questionnaire. Reliability was assessed using Cronbach's alpha coefficient, which yielded a value of 0.98, indicating high internal consistency. The statistical population consisted of 176 information technology managers as well as senior and middle managers working in government organizations in Kerman. Using Cochran's formula, a sample size of 120 participants was determined.

Findings: The results indicate that the components of information security management in the studied organizations were prioritized based on mean rank as follows: Organizational Asset Security Management (6.95), Organizational Information Security Management (6.49), Business Continuity Management (6.31), Operations and Communications Security Management (5.86), Acquisition, Development, and Maintenance Management (5.83), and Compliance Management (4.68). Furthermore, statistical analysis showed that the overall mean score of information security management performance in these organizations was significantly higher than the expected level according to the ISO/IEC 27002 standard ($p = 0.000 < 0.05$).

Conclusion: The findings highlight the importance of developing comprehensive information security policy documents within organizations. Clearly defining both general and specialized responsibilities related to information security for all employees is essential. Additionally, organizations should establish systematic reporting mechanisms for security incidents across departments and review security procedures and policies adopted by other organizations to improve their own security programs.

Value: By examining information security from a structural and managerial perspective, this study provides insights that can support strategic planning and policy development in public sector organizations.

Keywords: ***Performance Evaluation, Information Security Management, ISO/IEC 27002, Government Organizations, Kerman City***

How to Cite:
Soleimani Nezhad, A., Doroudi, F., & Tahmasbi, M. (2026). Assessment of Information Security Management Performance in Government Organizations Based on ISO/IEC 27002. *Journal of Knowledge-Research Studies*, 5 (1), 99-114.
Doi: https://doi.org/10.22034/jkrs.2026.20646
URL: https://jkrs.tabrizu.ac.ir/article_20646.html?lang=en
Article Type: Original Article
 Publisher: University of Tabriz **E-ISSN:** 2821-045X

1. Associate Professor, Department of Knowledge and Information Science, Shahid Bahonar University of Kerman, Kerman, Iran.
2. Assistant Professor, Iranian Research Institute for Information Science & Technology (IranDoc); Tehran, Iran (Corresponding Author) doroudi@irandoc.ac.ir
3. M.S.c. in Knowledge and Information Science; Kerman, Iran.

Journal of Knowledge-Research Studies (JKRS)

Vol 5

Issue 1

Serial Number 15

Extended Abstract

Introduction: Information security (InfoSec) is a set of security procedures and tools that broadly protect sensitive enterprise information from misuse or unauthorized access, while also keeping all forms of information safe. Additionally, InfoSec safeguards sensitive information from unauthorized activities such as destruction, recording, and disruption. Organizations implement information security for a variety of reasons, with the main objectives typically revolving around ensuring the confidentiality, integrity, and availability of company information. Information security is crucial for protecting valuable information assets from various threats, whether they are stored digitally or in other forms such as paper documents. This management system is essential for reducing risks, maintaining stakeholder trust, and complying with regulations. The goal of InfoSec is to minimize risk and ensure business continuity by proactively limiting the impact of security breaches. Many organizations develop a formal, documented process for managing InfoSec, often referred to as Information Security Management (ISM). The objectives of information security management include ensuring that information is available and ready to use when needed, that systems providing information can resist attacks and recover from failures, that information is visible only to those with necessary authorization, that information remains complete and accurate with protection against unauthorized modification, and that business transactions and the exchange of information between enterprises or partners are trustworthy.

Purpose:ISO/IEC 27002 is an international standard for information security and the establishment of an Information Security Management (ISM) system. Jointly published by ISO/IEC, the standard does not mandate specific actions but provides recommendations for documentation, internal audits, continual improvement, and corrective and preventive action. To become ISO 27002 certified, an organization needs an ISM that identifies organizational assets and protects them. This study assessed status of information security management in government agencies located in Kerman according to ISO/IEC 27002. The research method used in this study was a descriptive survey, and a questionnaire was used to collect information.

Methodology: The statistical population of the research includes 176 information technology managers, as well as senior and middle managers working in government organizations based in Kerman. The sample size was determined using the Cochran formula and consisted of 120 participants from educational organizations, the Kerman governorate, tax affairs, agricultural jihad, and industries and mines, who were selected to provide the required statistics and information. Data analysis was conducted using both descriptive and inferential statistics in SPSS statistical software. To analyze the research data and examine the information related to research questions and hypothesis, the Kolmogorov-Smirnov test was performed to confirm the normality of the data. Assuming equality of variances in the investigated groups, the analysis of variance (ANOVA) test was used, and the Friedman test was applied for ranking. A researcher-made questionnaire was used to collect the data required for the study. This questionnaire was developed in accordance with the components of the ISO/IEC 27002 standard. Considering the scope of the present study, which focuses on infrastructure and operations components, six components were selected and addressed in the research questions. These components include: (1) Information security management (2 components); (2) Organizational asset security management (2 components); (3) Operations and communication security management (10

components); (4) Acquisition, development, maintenance, and upkeep of information systems (6 components); (5) Business continuity management (1 component); and (6) Compliance management (3 components). A five-point Likert scale was used for respondents to answer each question. The validity of the research instrument was examined using the content validity method, with a value of 0.93. Additionally, Cronbach's alpha was used to examine the internal consistency of the instrument, yielding a reliability coefficient of 0.98.

Findings: The results of the independent t-test for the research sub-hypotheses, aimed at determining the expected level in the organizations under study, are presented in Table 1.

Journal of Knowledge-Research Studies (JKRS)

Vol 5

Issue 1

Serial Number 15

Table 1. T-test results, hypothesis testing

Hypotheses	T-test	DF	Significance	Confidence interval		Average
				Lower limit	Upper limit	
Organizational Information Security Management	3.021	120	0.001	1.672	2.234	14.087
Organizational Asset Security Management	3.432	120	0.004	1.871	2.543	14.153
Operations & Communications Security Management	3.003	120	0.001	1.542	2.787	14.003
Development and Maintenance Management	4.201	120	0.000	2.437	3.679	14.674
Business Continuity Management	3.965	120	0.002	3.645	4.212	14.342
Infrastructure and Operations Compliance Management	4.870	120	0.002	3.567	3.363	14.754

Based on the data in Table 6, all research sub-hypotheses have a significance level (p-value) of less than 0.05, indicating that the tests of these hypotheses are statistically significant. This suggests that the performance of these components in government organizations in Kerman city is higher than the expected level based on the desired standard.

Based on the results presented in Table 2, the findings indicate that, according to the average ranks obtained from Friedman's test, the prioritization of information security management indicators in government organizations in Kerman is as follows: asset security management (6.9), organization of information security (6.49), business continuity management (6.31), operations and communications management (5.86), information system acquisition, development, and maintenance (5.83), and compliance (3.14). The p-value obtained from the test is 0.000, which is lower than the significance level of 0.05. This result indicates that the average performance score of information security management in government organizations in Kerman, based on ISO/IEC 27002, is higher than the expected level.

Table 2. Average Rankings of the Friedman Test

Infrastructure and Operations Security Management Indicators	Rank averag	No.	Chi-Square	DF	Significance
Organizational Asset Security Management	6.95	120	190.86	10	**<0/001**
Organizational Information Security Management	6.49				
Business Continuity Management	6.31				
Operations and Communications Security Management	5.86				
Development and Maintenance Management	5.83				
Infrastructure and Operations Compliance Management	**4.68**				

Journal of Knowledge-Research Studies (JKRS)

Vol 5

Issue 1

Serial Number 15

The comparison of government organizations in Kerman city in terms of infrastructure and operations security management performance, based on the ANOVA test calculations, yielded a p-value of 0.089. Since this value is greater than the significance level of 0.05, the null hypothesis is accepted. Therefore, it can be concluded that there is no significant difference in the performance of government organizations in Kerman city regarding infrastructure and operations security management.

Conclusion: Information security management in government organizations in Kerman city has been strong. When comparing the average information security management of each organization to the expected level, it can be seen that, with the exception of Jihad Keshavarzi, all five organizations have higher levels of information security management than expected. The governorate and education sectors have the highest levels, while Jihad Keshavarzi has the lowest compared to the other organizations studied. By accepting organizational responsibility in this field, efficient information security management can strengthen this crucial factor. It has been determined that by establishing different levels of senior managers, middle managers, operational managers, and experts, implementing active monitoring tools at the entry and exit points of systems, using control software to prevent hacking and infiltration; and employing hardware, software, and Internet-control equipment and technologies, the level of information security can improve. Having a comprehensive program and utilizing artificial intelligence capabilities in this area is also significant. If environmental security issues arise that may lead to physical damage, these considerations should be incorporated. Therefore, supervision by responsible institutions at the governance level is important. Furthermore, modern information systems must align with emerging threats and their evolution. This requires continuous review and examination of security processes through relevant technologies. Adhering to the aforementioned approach enables organizations to maintain their stability in today's challenging environment. The results indicate that developing an information security policy document for organizations is necessary. It is important for all employees to understand both general and specialized responsibilities related to information security management. Incident reports should

be prepared in all organizational departments. Security procedures and policies from other organizations should be reviewed and adjusted to match organizational plans. The information security policy should be periodically reviewed. A written document detailing the history of security incidents, threats, and problems should also be prepared and presented to senior management.

Value: The present study focuses on information security from a structural perspective, and its results can be utilized for organizational planning.

Keywords: ***Performance Evaluation, Information Security Management, ISO/IEC 27002, Government Organizations, Kerman City***

Journal of Knowledge-Research Studies (JKRS)

Vol 5

Issue 1

Serial Number 15

References

Abrew, K. M. N. D., & Wickramarachchi, R. (2021). A review on organizational factors affecting the effectiveness of information security management systems in IT sector organizations in Sri Lanka. In *Proceedings of the International Conference on Advanced Marketing (ICAM4): Business, Law, and Management (BLM2)*.

Aftabi, N., Moradi, N., Mahroo, F., & Kianfar, F. (2025). SD-ABM-ISM: An integrated system dynamics and agent-based modeling framework for information security management in complex information systems with multi-actor threat dynamics. *Expert Systems with Applications, 263*, 125681. https://doi.org/10.1016/j.eswa.2024.125681

Ahmed, V., & Al-Haddad, S. (2021). The use of social engineering to change organizational behavior toward information security in an educational institution. *Journal of Information System Security, 17*(2), 103–124.

Akello, B. O. (2024). Organizational information security threats: Status and challenges. *World Journal of Advanced Engineering Technology and Sciences, 11*(1), 148–162. https://doi.org/10.30574/wjaets.2024.11.1.0047

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & Security, 99*, 102030. https://doi.org/10.1016/j.cose.2020.102030

Amaro, F. (2020). *Organizational challenges in adopting a security baseline to protect federal information from insider threats* (Doctoral dissertation, Capella University).

Arianty, K. P. (2025). Analysis of information security management system implementation at BSN. *Jurnal Informatika: Jurnal Pengembangan IT, 10*(1), 119–129.

Bitzer, M., Brinz, N., & Ollig, P. (2021). Disentangling the concept of information security properties: Enabling effective information security governance. In *Proceedings of the European Conference on Information Systems (ECIS)*.

Chase, J. L. (2021). *Examining the effect of organizational culture on end-user attitude towards information security awareness* (Doctoral dissertation, Colorado Technical University).

Chiu, C.-M., & Tan, C. M. (2020). Enhancing employees' intention to comply with information security policies: The roles of job crafting and organizational commitment.

da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture: Perspectives from academia and industry. *Computers & Security, 92*, 101713. https://doi.org/10.1016/j.cose.2020.101713

Dang-Pham, D., Thompson, N., Ahmad, A., & Maynard, S. (2025). Shadow information security practices in organizations: The role of information security transparency, overload, and psychological empowerment. *Computers & Security, 156*, 104538. https://doi.org/10.1016/j.cose.2025.104538

de Wit, J., Pieters, W., & van Gelder, P. (2024). Bias and noise in security risk assessments: An empirical study on the information position and confidence of security professionals. *Security Journal, 37*(1), 170–191. https://doi.org/10.1057/s41284-023-00376-1

Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security, 92*, 101747. https://doi.org/10.1016/j.cose.2020.101747

Ejigu, K., Siponen, M., & Muluneh, T. (2021). Influence of organizational culture on employees' information security policy compliance in Ethiopian companies. In *Proceedings of the Pacific Asia Conference on Information Systems (PACIS)*.

Emmanuel, K., & Hamid, T. (2023). A qualitative study of the effects of socio-organizational factors on the information security culture of employees in a financial institution. In *Proceedings of the International Conference on Advances in Communication Technology and Computer Engineering (ICACTCE)*. Springer.

Folorunso, A., Mohammed, V., Wada, I., & Samuel, B.(2024). The impact of ISO security standards on enhancing cybersecurity posture in organizations. *World Journal of Advanced Research and Reviews, 24*(1), 2582–2595. https://doi.org/10.30574/wjarr.2024.24.1.3344

Grigaliūnas, Š., Schmidt, M., Brūzgienė, R., Smyrli, P., Andreou, S., & Lopata, A. (2024). Holistic information security management and compliance framework. *Electronics, 13*(19), 1–31. https://doi.org/10.3390/electronics13193862

Hameed, M. A., & Arachchilage, N. A. G. (2020). A conceptual model for the organizational adoption of information system security innovations. In *Security, privacy, and forensics issues in big data* (pp. 317–339). IGI Global.

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications, 58*, 102726. https://doi.org/10.1016/j.jisa.2020.102726

Hussein, H. A. (2024). Organizational factors that influence information security in SMEs: A case study of Mogadishu, Somalia. *International Journal of Innovative Science and Research Technology, 9*(6), 1373–1382.

Kam, H. J., Mattson, T., & Goel, S. (2020). A cross-industry study of institutional pressures on organizational effort to raise information security awareness. *Information Systems Frontiers, 22*(5), 1241–1264. https://doi.org/10.1007/s10796-019-09941-6

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees' information security awareness in private and public organisations: A systematic literature review. *Computers & Security, 106*, 102267. https://doi.org/10.1016/j.cose.2021.102267

Kreutz, H., & Jahankhani, H. (2024). Impact of artificial intelligence on enterprise information security management in the context of ISO 27001 and 27002: A tertiary systematic review and comparative analysis. In *Cybersecurity and artificial intelligence: Transformational strategies and disruptive innovation* (pp. 1–34).

Latola, S. (2023). Positive organizational behavior in information security compliance management: A literature review.

Lopes, A., Reis, L., São Mamede, H., & Santos, A. (2022). Information security threat assessment using social engineering in the organizational context: Literature review. In *Information systems and technologies*. Springer.

López-Vasco, F., Angulo-Alvarez, M., Zuñiga, D. I. S., Moromenacho, E. P., & Ortiz, N. (2024). Application of ISO/IEC 27001 in higher education technological institutes: Case-control study. In *Multidisciplinary International Conference of Research Applied to Defense and Security*. Springer.

Ma, X. (2022). IS professionals' information security behaviors in Chinese IT organizations for information security protection. *Information Processing & Management, 59*(1), 102744. https://doi.org/10.1016/j.ipm.2021.102744

Nagata, K. (2024). Establishing information security policy as an organizational risk management. IntechOpen.

Journal of Knowledge-Research Studies (JKRS)

Vol 5

Issue 1

Serial Number 15

Nowicka, J., Ciekanowski, Z., & Milewska, A. (2024). Information security management as the basis for the functioning of an organization. *European Research Studies Journal, 27*(3), 128–141.

Oluwasefunmi, A., Folashade, M., Oluwafolake, O., Yetunde, A. C., & Igbe, T. (2021). Critical factors affecting the efficiency of information security risk management in business organizations: An empirical study. *Covenant Journal of Informatics and Communication Technology, 9*(1), 1–18.

Otieno, E. O. (2021). *The impact of organizational culture on information security compliance culture: A case of Kenyan universities* (Master's thesis, University of Nairobi).

Parvin, S., Sadoughi, F., Karimi, A., Mohammadi, M., & Aminpour, F. (2019). Information security from a scientometric perspective. *Webology, 16*(1), 196–209.

Selifanov, V. V., Doroshenko, I. E., Troeglazova, A. V., & Maksudov, M. M. (2021). Acceptable variants formation methods of organizational structure and the automated information security management system structure. In *2021 XV International Scientific-Technical Conference on Actual Problems of Electronic Instrument Engineering (APEIE)*. IEEE.

Selifanov, V. V., Maksudov, M. M., Doroshenko, I. E., & Titov, D. N. (2022). Methodology for the synthesis of acceptable options for organizational functional structure of the security management system of a significant object of critical information infrastructure. In *2022 IEEE 23rd International Conference of Young Professionals in Electron Devices and Materials (EDM)*. IEEE.

Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T., & Klepacki, B. (2020). Information security assessment in public administration. *Computers & Security, 90,* 101709. https://doi.org/10.1016/j.cose.2019.101709

Usmonov, M. (2024). Basic concepts of information security. *Indexing, 1*(1), 81–85.

Journal of Knowledge-Research Studies (JKRS)

Vol 5

Issue 1

Serial Number 15