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
©The Author(s) **Publisher: University of Tabriz** **E-ISSN:** 2821-045X

The paper is an open access and licensed under the Creative Commons CC BY NC license.

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

نشریه مطالعات دانش پژوهی

ارزیابی عملکرد مدیریت امنیت اطلاعات در سازمان‌های دولتی با تکیه‌بر ISO/IEC 27002

عادل سلیمانی‌نژاد [۱]، فریبرز درودی [۲*]، معصومه طهماسبی [۳]

۱- دانشیار، بخش علم اطلاعات و دانش‌شناسی، دانشگاه شهید باهنر کرمان، کرمان؛ ایران

۲- استادیار، پژوهشکده علوم اطلاعات، گروه پژوهشی علم‌سنجی و تحلیل‌اطلاعات، پژوهشگاه علوم و فناوری اطلاعات ایران، تهران، ایران. (نویسنده مسئول) doroudi@irandoc.ac.ir

۳- کارشناس ارشد، بخش علم اطلاعات و دانش‌شناسی دانشگاه باهنر کرمان، کرمان، ایران

تاریخ دریافت: ۵ مرداد ۱۴۰۴ **تاریخ بازنگری: ۱۶ مهر ۱۴۰۴**

تاریخ پذیرش : ۲۹ مهر ۱۴۰۴ **تاریخ انتشار: ۱۰ اسفند ۱۴۰۴**

چکیده

هدف: پژوهش حاضر باهدف ارزیابی وضعیت عملکرد مدیریت امنیت اطلاعات در سازمان های دولتی مستقر در شهر کرمان بر اساس استاندارد ایزو/ آی.ای.سی ۲۷۰۰۲ انجام شده است.

روش‌شناسی: روش پژوهش توصیفی- پیمایشی است و به منظور گردآوری اطلاعات از پرسش‌نامه استاندارد مذکور استفاده شده است. برای بررسی سنجش پایایی پژوهش از روش آلفای کرونباخ بهره گرفته شد که میزان آن ۰/۹۸ تعیین شد. جامعه آماری پژوهش شامل، ۱۷۶ نفر از مدیران فناوری اطلاعات و مدیران اصلی و میانی شاغل در سازمان‌های دولتی مستقر در شهر کرمان است. نمونه جامعه آماری با استفاده از فرمول کوکران، شامل ۱۲۰ نفر تعیین شد.

یافته‌ها: یافته‌های حاصل از پژوهش نشان می‌دهد که در اولویت بندی (بر اساس میانگین رتبه‌ای) شاخص‌های مدیریت امنیت اطلاعات در سازمان‌های دولتی کرمان بر اساس آزمون فریدمن به ترتیب: مدیریت امنیت اموال سازمان (۶/۹۵)، مدیریت امنیت اطلاعات سازمان (۶/۴۹)، مدیریت استمرار کسب و کار (۶/۳۱)، مدیریت امنیت عملیات و ارتباطات (۵/۸۶)، مدیریت اکتساب توسعه حفظ و نگهداری (۵/۸۳) و مدیریت تطابق (۴/۶۸) است. نتایج پژوهش حاکی از این است به علت اینکه مقدار p به‌دست آمده از آزمون برابر با ۰/۰۰۰ و کمتر از سطح معناداری تحقیق (۰/۰۵) است در نتیجه می‌توان بیان کرد که میانگین نمره عملکرد مدیریت امنیت اطلاعات در سازمان‌های دولتی مستقر در شهر کرمان بر اساس استاندارد ایزو/ آی. ای. سی. ۲۷۰۰۲ بالاتر از حد انتظار است.

نتیجه‌گیری: نتایج نشان می‌دهند که شایسته است تا سند خط‌مشی امنیت اطلاعات برای سازمان‌ها تدوین شود. مسئولیت‌های عمومی و تخصصی مدیریت امنیت اطلاعات، برای تمامی کارکنان مشخص باشد. گزارش رخدادهای امنیت اطلاعات در تمامی بخش‌های سازمانی تهیه شود. رویه‌ها و خط‌مشی‌های امنیتی سازمان‌های دیگر بررسی و با برنامه‌های سازمانی تطبیق داده شود.

اصالت و ارزش: پژوهش حاضر از منظر ساختاری به مقوله امنیت اطلاعات پرداخته و نتایج آن می‌تواند برای برنامه‌ریزی در سازمان‌ها مورد استفاده قرار گیرد.

کلیدواژه‌ها: ***ارزیابی عملکرد، مدیریت امنیت اطلاعات، ایزو آی. ای. سی.۲۷۰۰۲، سازمان‌های دولتی، شهر کرمان***

چگونه به این مقاله استناد کنیم؟

سلیمانی‌نژاد، عادل؛ درودی، فریبرز و طهماسبی، معصومه. (۱۴۰۵). ارزیابی عملکرد مدیریت امنیت اطلاعات در سازمان‌های دولتی با تکیه بر ISO/IEC 27002 . نشریه *مطالعات دانش‌پژوهی*، ۵ (۱): ۱۱۴-۹۹.

Doi: https://doi.org/10.22034/jkrs.2026.20646

URL: https://jkrs.tabrizu.ac.ir/article_20646.html

نوع مقاله: مقاله پژوهشی

ناشر: دانشگاه تبریز **شاپا الکترونیکی:** 2821-045X

© نویسندگان

این مقاله به‌صورت دسترسی باز و با لایسنس CC BY NC کریتیوکامانز قابل‌استفاده است.

۱-مقدمه

در حال حاضر، امنیت اطلاعات تقریباً برای هر کسب‌وکاری به دغدغه‌ای حیاتی تبدیل شده است (ابرو و ویکراماراچی[1]، ۲۰۲۱) و جوامع اطلاعاتی به‌طور مستمر با تهدیدهای امنیتی و آسیب‌پذیری‌های اطلاعاتی مواجه هستند (پروین و همکاران[2]، ۲۰۱۹). از همین‌رو، یکی از مسائل حیاتی در مدیریت سازمان، امنیت اطلاعات است (اولووا سفونمی و همکاران[3]، ۲۰۲۱). هر سازمانی با خطرات مرتبط با اطلاعات مانند: نشت اطلاعات، نقص سیستم و خدمات، نفوذهای غیرمجاز، به خطر انداختن رایانامه‌های تجاری، حملات باج‌خواهی و غیره مواجه است (ناگاتا[4]، ۲۰۲۴). به این دلیل، امنیت اطلاعات به یک نگرانی مبرم برای هر مؤسسه‌ای که وظیفه ارائه خدمات مناسب را برعهده دارد، تبدیل شده است (امانوئل و حمید[5]، ۲۰۲۳). رایج‌ترین مفهوم امنیت اطلاعات، سه‌گانه محرمانگی، یکپارچگی و در دسترس بودن است (بیتزر و همکاران[6]، ۲۰۲۱). همچنین، مفهوم امنیت اطلاعات، پیشگیری از فعالیت کاربران و صاحبان اطلاعاتی است که به‌طور تصادفی یا ناخواسته، ماهیت طبیعی یا مصنوعی داشته و به منابع اطلاعاتی، از جمله آن‌هایی که زیرساخت را پشتیبانی می‌کنند، آسیب می‌رسانند (عثمانوف[7]، ۲۰۲۴). همچنین، بسیاری از سازمان‌هایی که اطلاعات حساس را پردازش و ذخیره می‌کنند، با چالش‌هایی در محافظت از آن در برابر تهدیدات داخلی مواجه می‌شوند(آمارو[8]، ۲۰۲۰). لذا، برای اطمینان از حفاظت جامع اطلاعات، استفاده از ابزارهای مختلف حفاظت از اطلاعات، که بر اساس سطوح و بخش‌های سیستم اطلاعاتی توزیع می‌شوند، ضروری است (سلیفانوف[9]، ۲۰۲۱) و سازمان‌ها تلاش می‌کنند اقداماتی را برای محافظت از اطلاعات خود و حفظ محرمانگی انجام دهند(حسین[10]، ۲۰۲۴).

با پیشرفت فناوری، پیچیدگی جرایم سایبری نیز افزایش می‌یابد، که در نتیجه نیازمند بهبود اقدامات امنیت اطلاعات است(احمد و الحداد[11]، ۲۰۲۱). باید تأکید کرد که توسعه فناوری‌ها ناگزیر تهدیدهای جدیدی را به‌وجود می‌آورد و نیاز به بازنگری رویکردها برای سیستم‌های امنیتی و مدیریت آنها دارد (سلیفانوف و همکاران، ۲۰۲۲). همچنین، تهدیدهای امنیتی سیستم اطلاعاتی هنوز برای بسیاری از سازمان‌ها دغدغه اصلی است. با این حال، اکثر سازمان‌ها در دستیابی به پذیرش و اجرای موفقیت‌آمیز اقدامات امنیتی سیستم‌های اطلاعاتی کوتاهی می‌کنند(حمید و آراچیلاج[12]، ۲۰۲۰). براین‌اساس، سازمان‌ها می‌توانند با حفاظت در عرصه امنیت اطلاعات به‌عنوان دارایی اطلاعاتی و داده‌محور، به

1. Abrew and Wickramarachchi
2. Parvin et al.
3. Oluwasefunmi et al.
4. Nagata
5. Emmanuel and Hamid
6. Bitzer et al.
7. Usmonov
8. Amaro
9. Selifanov et al.
10. Hussein
11. Ahmed and Al-Haddad
12. Hameed and Arachchilage

مزیت راهبردی دست یابند (ما[1]، ۲۰۲۲). علاوه بر آن باید بیان کرد که فنون جرایم سایبری به‌طور فزاینده‌ای پیچیده‌تر می‌شود(لاتولا[2]، ۲۰۲۳). امنیت اطلاعات نقش مهمی در حفاظت از کسب‌وکار سازمان دارد(الغمدی و همکاران[3]، ۲۰۲۰) و امروزه، امنیت اطلاعات سازمانی یک حساسیت حیاتی در دنیای به هم پیوسته و مبتنی بر داده است (آکلو[4]، ۲۰۲۴). براین‌اساس، توجه به ساختار مناسب سیستم‌های اطلاعاتی و بهره‌گیری از فناوری‌های اطلاعاتی برای حفاظت از منابع اطلاعاتی سازمانی یک ضرورت به شمار می‌آید و مدیران در این زمینه، تلاش می‌کنند تا بتوانند سیستم‌های مطلوب و کارآمدی را برای حفاظت از اطلاعات راهبردی خود به کار گیرند.

رعایت پروتکل‌های امنیت اطلاعات، یک ضرورت جدی در سازمان‌هاست که نتایج آن می‌تواند سبب کنترل بهینه فرایندهای کاری نهادهای اجرایی شود. حفاظت از اطلاعات سازمانی، کنترل‌های مدیریتی، وضعیت نیروی انسانی، عوامل فرایندی و مدیریت سازمانی نقش مهمی در حفاظت اطلاعات و رویه‌های سازمانی دارد تا فعالیت‌ها به شیوه امن و مطمئن به انجام رسد. همچنین باید بیان کرد که وضعیت امنیت فضای تبادل اطلاعات در سازمان‌ها، با توجه به برخی از تهدیدهای موجود در ارتباط با نفوذ و خراب‌کاری، به‌ویژه در حوزه دستگاه‌های دولتی، نیازمند عنایت بیشتری است. بررسی وضعیت زیرساخت و عملیات، سیستم‌های اطلاعاتی، ارتباطات، کسب‌وکار، و اموال سازمانی نقش مهمی در بهبود کیفیت فرایندهای حرفه‌ای در سازمان دارد. از این‌رو، پژوهش حاضر، با توجه به اهمیت بررسی زیرساخت‌های اطلاعاتی به سنجش وضعیت ایمن سازی شرایط استفاده از اطلاعات در دستگاه‌های دولتی در شهر کرمان می‌پردازد. براین‌اساس، هدف اصلی پژوهش، ارزیابی وضعیت عملکرد مدیریت امنیت اطلاعات در سازمان‌های دولتی شهر کرمان از ابعاد زیرساختی وعملیاتی بر اساس استاندارد بین‌المللی ایزو ۲۷۰۰۲ است.

فرضیه پژوهش نیز عبارت است از: بین عملکرد سازمان‌های دولتی مستقر در شهر کرمان از نظر مدیریت امنیت اطلاعات تفاوت معناداری وجود دارد. فرضیه‌های فرعی پژوهش(۶ فرضیه) نیز از این قرار است: بین مولفه‌های (مدیریت امنیت اطلاعات سازمان، مدیریت امنیت اموال سازمان، مدیریت امنیت عملیات و ارتباطات، مدیریت اکتساب توسعه حفظ و نگهداری، مدیریت استمرار کسب و کار، و مدیریت تطابق ابعاد زیرساخت و عملیات) در سازمان‌های دولتی مستقر در شهر کرمان از نظر مدیریت امنیت اطلاعات تفاوت معناداری وجود دارد.

۲-پیشینه پژوهش

امنیت اطلاعات شامل فناوری‌ها و فرایندها برای حفاظت از سیستم‌های اطلاعاتی در سازمان‌هاست که در زمان دسترسی، بهره‌برداری و ارائه اطلاعات ارزشمند، به یاری مدیران، کارکنان و سازمان‌ها آمده و هدف آن حفظ محرمانگی، یکپارچگی و در دسترس‌پذیری است. استاندارد

1. Ma
2. Latola
3. AlGhamdi et al.
4. Akello

ISO/IEC 27002 نیز استانداردی بین‌المللی است که چارچوبی برای سیستم مدیریت امنیت اطلاعات تعریف کرده تا سازمان‌ها بتوانند اطلاعات مهم خود را به روش مؤثر حفاظت کنند. از این رو در ادامه پژوهش‌های مهم در حوزه‌های مختلف مرتبط معرفی می‌شوند:

کنترل‌های مدیریتی

پژوهش چیو و تان[1] (۲۰۲۰) حاکی از آن بود که راه‌های شناسایی شده برای درک چگونگی افزایش انطباق کارکنان با سیاست‌های امنیت اطلاعات بیشتر از طریق رعایت مؤلفه‌های سازمانی این حوزه و نیز تعهد اداری آن‌ها به این مقوله است. در کنار آن نتایج نشان داد که ایجاد شغل مناسب می‌تواند تعهد کاری و تعهد سازمانی کارکنان را افزایش داده و شرایط بهتری برای حفاظت ازداده‌های حساس ایجاد شود. نتایج پژوهش داویگا و همکاران[2] (۲۰۲۰) نشان داد که مؤلفه‌های فرهنگ امنیت اطلاعات مطلوب با تکیه بر ویژگی‌های برتر مربوط به جنبه‌هایی مانند نیروی انسانی آگاه و توانمند دارای اثربخشی بیشتری است. در این میان تعهد کاری نسبت به رعایت موازین حفاظتی در بهره‌گیری از داده‌ها نقش مهمی برعهده دارد. این عوامل می‌توانند بر فرهنگ امنیت اطلاعات تأثیر مثبت بگذارند. یافته‌های پژوهش کام، ماتسون و گوئل[3] (۲۰۲۰) نشان داد، با توجه به آن‌که صنایع مختلف دارای هنجارها، قوانین و ارزش‌های مرتبط با امنیت منحصربه‌فردی هستند، شایسته است تا سطوح مختلف تلاش سازمانی را برای بالا بردن آگاهی در زمینهٔ امنیت اطلاعات کارکنان خود را ارتقاء دهند. همچنین نتایج مطالعات کاندو و همکاران[4] (۲۰۲۱) حاکی از آن بود که آگاهی از امنیت اطلاعات کارکنان به یکی از جنبه‌های حیاتی حفاظت در برابر رفتارهای نامطلوب امنیت اطلاعات تبدیل می‌شود و از روش‌ها و عوامل مختلفی برای تقویت این نوع از آگاهی کارکنان در سازمان‌ها استفاده شده و با تکیه بر آن می‌توان به تقویت این حوزه یاری رساند.

عناصر فنی

نتایج پژوهش شچپانیوک و دیگران[5] (۲۰۲۰) نشان داد که در سال‌های ۲۰۱۶-۲۰۱۷، در ادارات دولتی لهستان، مشکلاتی در بعد مدیریت امنیت اطلاعات وجود داشته است که از جمله می‌توان به فقدان سازمان‌دهی سیستم مدیریت امنیت اطلاعات و اسناد ناقص، قدیمی، و یا فقدان آن اشاره کرد. ارائه راهکارهای حفاظتی در بخش نیروی انسانی و اجرای برنامه امنیتی راهکار مهم این مطالعه بوده است. چیس[6] (۲۰۲۱) در پژوهش خود بیان کرد که سازمان‌ها باید اهمیت حفاظت از دارایی‌های اطلاعاتی را در برابر قرار گرفتن در معرض تهدید فزاینده ناشی از اطلاعات درخواستی قابل دسترسی از طریق اینترنت مدنظر قرار داده و برای آن برنامه مدون داشته باشند. او تصریح کرد که این برنامه باید قابلیت اجرا و پذیرش از سوی کارکنان را داشته باشد. یافته‌های پژوهش حسن و

نشریه مطالعات دانش‌پژوهی
صفحه | ۱۰۲
دوره ۵، شماره ۱
پیاپی ۱۵

1. Chiu & Tan
2. Da Veiga et al.
3. Kam, Mattson & Goel
4. Khando et al.
5. Szczepaniuk et al.
6. Chase

همکاران[1] (۲۰۲۱) نشان داد که اهمیت هفت عامل از ۹ عامل مؤثر بر آمادگی امنیت سایبری شناسایی شده در سازمان‌های دولتی بحرین تأیید شده است. علاوه بر آن، آمادگی امنیت سایبری تأثیر مثبتی بر عملکرد امنیت سازمانی دارد که به نوبه خود بر عملکرد مالی و غیر مالی تأثیر مثبت می گذارد. نوویچکا، سیکانوفسکی و میلوسکا[2] (۲۰۲۴) به پژوهش در باره شناسایی و تعیین نقش امنیت اطلاعات در عملکرد سازمانی پرداختند. یافته‌ها حاکی از آن بود که تحلیل امنیت اطلاعات نیازمند یک رویکرد جامع است که هم جنبه‌های فناوری و هم جنبه‌های نظارتی را در نظر بگیرد. علاوه بر این، نیاز و انتظار برای بهبود مستمر شیوه‌ها برای محافظت از داده‌ها و منابع یک سازمان در برابر تهدیدات دیجیتال رو به رشد وجود دارد که شامل داده‌های شخصی، مالی و همچنین داده‌های خاص و استراتژیک، بسته به ماهیت سازمان یا نهاد خاص می شود. کرویتز[3] (۲۰۲۴) به پژوهش در باره تأثیر هوش مصنوعی بر مدیریت امنیت اطلاعات سازمانی در چارچوب ایزو ۲۷۰۰۱ و ۲۷۰۰۲ مبادرت ورزید. نتایج نشان داد که تحلیل نشان داد که سیستم مدیریت امنیت اطلاعات و کنترل‌های امنیتی موجود ISO 27001 برای رسیدگی به چالش‌های امنیتی نوظهور هوش مصنوعی کافی نیستند. پیشنهاد پژوهش برای بهبود این فقدان کنترل‌های امنیتی کافی، شش کنترل امنیتی جدید و ده کنترل امنیتی اصلاح‌شده موجود بود.

عوامل فرایندی

نتایج پژوهش اوتینو[4] (۲۰۲۱) نشان داد که تهدید داخلی برای امنیت اطلاعات به‌طور فزاینده به چالشی برای مدیران امنیت اطلاعات تبدیل می‌شود. از زمره چالش‌های بزرگ این عرصه، فقدان سیاست‌های قوی و مستحکم نیست، بلکه اطمینان از انطباق کامل یا بالاترین میزان با سیاست‌های امنیتی است. یافته‌های مطالعه آفتابی و همکاران[5] (۲۰۲۵) حاکی از آن بود که چارچوب برنامه امنیت اطلاعات ابزاری قوی برای تصمیم‌گیرندگان امنیتی ارائه می‌دهد و سازمان‌ها را قادر می‌سازد تا استراتژی‌های امنیتی خود را با سطح تهدید در حال تحول همسو کرده و تاب‌آوری خود را در برابر حملات سایبری افزایش دهند. شبیه‌سازی دقیق و تحلیل آماری، عناصر تأثیرگذار در سیستم‌های اطلاعاتی را در طول زمان شناسایی می‌کند و تأثیر تعاملات بین تهدیدات داخلی، خارجی و سیستم‌های اطلاعاتی را در محیطی که با عدم قطعیت بالا و رفتارهای تهدیدآمیز متنوع مشخص می‌شود، برجسته می‌کند. لوپز-واسکو و همکاران[6] (۲۰۲۴) به پژوهش در باره کاربرد ISO/IEC 27001 در مؤسسات فناوری آموزش عالی مبادرت ورزیدند. یافته‌ها حاکی از آن بود که مدیریت ریسک راهبردی متناسب با نیازها و ویژگی‌های مؤسسه تدوین و اجرا می‌شود. نتایج نشان دهنده افزایش انطباق با استانداردهای ISO و در نتیجه بهبود قابل توجه امنیت اطلاعات می‌باشند. این

1. Hasan et al.
2. Nowicka, Ciekanowski & Milewska
3. Kreutz
4. Otieno
5. Aftabi et al.
6. López-Vasco et al.

پیشـــرفت نه تنها نشـــان دهنده اثربخشـــی روش اتخاذ شـــده اســـت، بلکه اهمیت مدیریت ریســـک سیستماتیک و ساختارمند در بخش آموزشی را نیز برجسته می‌کند.

عناصر سازمانی و پیکربندی

نتایج پژوهش دیش، پفاف و کرچمار[1] (۲۰۲۰) نشان داد که مؤلفه‌های اصلی مدل جامع عوامل امنیت اطلاعات در ۱۲ حوزه طبقه‌بندی می‌شـوند. این عوامل شـامل: امنیت فیزیکی، آسـیب‌پذیری، زیرساخت، آگاهی، کنترل دسترسی، خطرپذیری، منابع، عوامل سازمانی، مدل استاندارد سی.آی.ای (محرمانگی، یکپارچگی و دسترس‌پذیری)[2]، تداوم، مدیریت امنیت، انطباق و سیاست. پژوهش لوپز[3] و همکاران (۲۰۲۲) در باره تهدید امنیت اطلاعات سـازمانی با اسـتفاده از مهندسـی اجتماعی به انجام رسـید. نتایج نشـان داد که از تحقیقات علوم طراحی به دلیل امکان سـاخت، ارزیابی و اعتبارسـنجی مسـائل امنیتی اسـتفاده می‌شـود. همچنین با تدوین چارچوب مدون امنیت اطلاعات، می‌توان برای جلوگیری از حملات مهندسـی اجتماعی در سـازمان‌ها به منظور نفوذ خرابکاری بهره گرفت. گریگالیوناس و همکاران[4] (۲۰۲۴) به پژوهش در باره چارچوب جامع مدیریت امنیت اطلاعات سازمانی مبادرت ورزیدند. نتایج نشان می‌دهد که چارچوب پیشنهادی که حوزه‌های امنیتی عملیاتی، فنی، انسـانی و فیزیکی را ادغام می‌کند، نه تنها الزامات انطباق را در حوزه‌های امنیتی متعدد برآورده می‌کند، بلکه یک راه‌حل مقیاس‌پذیر برای سـازگاری کارآمد با تهدیدات و مقررات جدید نیز ارائه می‌دهد. همچنین مشخص شد که سازمان‌ها می‌توانند از طریق این چارچوب یکپارچه، وضعیت امنیتی و انطباق قانونی خود را به طور هم‌زمان افزایش دهند. آریانتی[5](۲۰۲۵) به پژوهش در باره تحلیل پیاده‌سـازی سـیسـتم مدیریت امنیت اطلاعات پرداخت. این مطالعه، اثربخشـی پیاده‌سـازی سـیسـتم مدیریت امنیت اطلاعات را با تمرکز بر رعایت اسـتانداردهای بین‌المللی، اسـتراتژی‌های مدیریت ریسـک و تعهد سـازمانی به حفاظت از اطلاعات ارزیابی می‌کند. یافته‌ها، نقش حیاتی تعهد رهبری، ارزیابی‌های جامع ریسـک و ارزیابی‌های منظم سیسـتم را در دسـتیابی به اهداف اسـتاندارد نشـان داد. مشـخص شـد که اسـتاندارد ISO/IEC 27001 در محافظت از اطلاعات حسـاس، تقویت اعتماد و همسویی دارای شرایط مطلوبی است.

مولفه‌های ارزیابی و نظارت

پژوهش ایجیگو، سیپونن و مولونه[6](۲۰۲۱) نشان داد که فرهنگ سازمانی به‌طور قابل‌توجهی بر تبعیت کارکنان بانک‌های اتیوپی از سیاست‌های امنیت اطلاعات تأثیر می‌گذارد. نتایج حاکی از آن بود که برای ارتقای رفتار سـازمانی در رابطه با امنیت اطلاعات، شـرکت‌ها باید فرهنگ سـازمانی خود و چگونگی تأثیر آن بر اثربخشی اجرای سیاست‌های امنیت اطلاعات را بررسی، تحلیل و ارزیابی کنند.

1. Diesch, Pfaff & Krcmar
2. CIA Standards for Confidentiality, Integrity, and Availability
3. Lopes et al.
4. Grigaliūnas et al.
5. Arianty
6. Ejigu, Siponen & Muluneh

دی ویت، پیترز و ون گلدر[1] (۲۰۲۴) که در زمینهٔ ارزیابی خطرپذیری امنیت اطلاعات به مطالعه پرداختند، بیان کردند که متخصصانی که هم در حوزه امنیت فیزیکی و هم در حوزه امنیت سایبری کار می‌کنند باید خطرات امنیتی را ارزیابی و تحلیل کنند. شواهد تجربی در باره درک موقعیت اطلاعات و سطوح اطمینان متخصصان امنیتی، تأثیر اطلاعات دقیق و مغالطه ارتباط، و سطح اختلال در ارزیابی‌های امنیتی حاکی از آن است که این مقوله‌ها می‌تواند خطرپذیری امینت اطلاعات در سازمان را تحت تاثیر قرار دهد. دانگ-فام[2] و همکاران (۲۰۲۵) به مطالعه درباره شیوه‌های امنیت اطلاعات در سایه در سازمان‌ها مبادرت ورزیدند. نتایج نشان داد بر اساس مدل‌سازی معادلات ساختاری هم اضافه بار امنیتی و هم توانمندسازی روانی، قصد اتخاذ اقدامات امنیت سایه را افزایش می‌دهند، در حالی که شفافیت درک‌شده از امنیت سازمانی (از طریق ارتباطات امنیتی) این قصد را کاهش می‌دهد. همچنین نتایج نشان‌دهنده ارتباط میان ساختارها بود و مشخص شد که اضافه بار امنیتی با توانمندسازی روانی از افزایش بیشتری برخوردار خواهد بود.

نتایج بررسی پیشینه پژوهش نشان داد که تدوین سیاست‌های امنیت اطلاعات برای کارکنان، فرهنگ امنیت اطلاعات، آگاهی تخصصی کارکنان از امنیت اطلاعات، ایجاد زمینهٔ زیرساختی برای امنیت اطلاعات، شناسایی انواع تهدیدهای داخلی و خارجی، شکاف میان آموزش آگاهی امنیتی و نگرش کاربر نهایی، ارزیابی آمادگی امنیت سایبری سازمان‌ها، کاربردپذیری خط‌مشی امنیت اطلاعات و ارزیابی خطرپذیری امنیت اطلاعات نقش مهمی در مطالعات انجام شده دارد. تمامی موضوع‌های ذکر شده از ابعاد مختلف به این مقوله مهم توجه کرده‌اند، ولی در زمینهٔ زیرساخت‌ها و ابعاد عملیاتی امنیت اطلاعات کمتر فعالیت مطالعاتی انجام گرفته است. لذا این پژوهش به این جنبه از موضوع امنیت اطلاعات می‌پردازد.

۳-روش‌شناسی پژوهش

روش پژوهش حاضر پیمایشی-توصیفی است. جامعه آماری پژوهش تمامی کارشناسان حوزه فناوری اطلاعات، مسئولان حراست، مدیران اصلی و میانی سازمان‌های دولتی مستقر در شهر کرمان هستند که زیر نظر دولت اداره می‌شوند و دارای بودجه دولتی هستند. بر اساس آمار دفتر منابع انسانی استانداری این سازمان‌ها مشتمل بر ۸۹ دستگاه اجرایی در سطح استان بودند. با عنایت به محدودیت‌های زمان و هزینه، تعداد ۵ سازمان از طریق نمونه‌گیری با هدف دسترسی به آمار و اطلاعات انتخاب شدند که شامل اداره کل آموزش‌وپرورش، استانداری کرمان، امور مالیاتی، جهاد کشاورزی و سازمان صنایع و معادن استان می‌شوند. منطق انتخاب این سازمان‌ها بر اساس نقش آن‌ها در فعالیت‌های مهم تخصصی و مدیریت کلان‌شهری، یعنی حوزه‌های آموزشی، حکمرانی و سیاست‌گذاری، اقتصادی و مالی، کشاورزی و ترویجی، نیز حوزه صنعت و معدن در نظر گرفته شد. جامعه آماری شامل مدیران در سطوح مختلف مرتبط با زمینه امنیت اطلاعات بودند. دراین‌ارتباط با بررسی انجام‌گرفته، تعداد ۱۷۶

1. De Wit, Pieters & van Gelder
2. Dang-Pham et al.

نفر در سمت‌های نامبرده شناسایی شدند. با استفاده از فرمول کوکران نمونه‌گیری این جامعه آماری انجام شد. با استفاده از روش نمونه‌گیری طبقه‌ای متناسب با حجم جامعه و با استفاده از فرمول کوکران و با حداکثر خطای برآورد قابل‌قبول برای تعیین نمونه معادل ۰/۰۵، حجم نمونه ۱۲۰ نفر تعیین شد. پس از تعیین حجم نمونه در هر طبقه، از روش تصادفی ساده برای انتخاب واحد نمونه‌گیری استفاده شد. به این معنا که هر سازمان به‌عنوان یک طبقه در نظر گرفته‌شده و به نسبت جمعیت، تعدادی به‌عنوان حجم نمونه، با استفاده از نمونه‌گیری تصادفی ساده انتخاب و پرسش‌نامه بین آن‌ها توزیع شد.

در جدول ۱، حجم نمونه موردبررسی به تفکیک سازمان، تعداد کل و نمونه انجام‌شده بیان شده است.

جدول ۱. جامعه آماری و تعداد نمونه پژوهش

سازمان	تعداد کل	تعداد نمونه
آموزش‌وپرورش	۳۸	۲۶
استانداری کرمان	۶۸	۴۶
امور مالیاتی	۳۳	۲۳
جهاد کشاورزی	۲۱	۱۴
صنایع و معادن	۱۶	۱۱
جمع کل	۱۷۶	۱۲۰

نشریه مطالعات دانش‌پژوهی

صفحه | ۱۰۶

دوره ۵، شماره ۱

پیاپی ۱۵

برای گردآوری داده‌های موردنیاز پژوهش از پرسش‌نامه محقق ساخته استفاده شده است. این پرسش‌نامه مطابق با مؤلفه‌های استاندارد ایزو/ آی. ای. سی. ۲۷۰۰۲ تدوین شد. با عنایت به حیطه پژوهش حاضر، یعنی بررسی مؤلفه‌های زیرساخت و عملیات، تعداد ۶ مؤلفه این حوزه انتخاب و در پرسش‌ها مطرح شد که شامل: ۱) مدیریت امنیت اطلاعات (۲ مؤلفه)؛ ۲) مدیریت امنیت اموال سازمان (۲ مؤلفه)؛ ۳) مدیریت امنیت عملیات و ارتباطات (۱۰ مؤلفه)؛ ۴)اکتساب، توسعه، حفظ و نگهداری سیستم‌های اطلاعاتی (۶ مؤلفه)؛ ۵) مدیریت استمرار کسب‌وکار (۱ مؤلفه)؛ و ۶) مدیریت تطابق (۳ مؤلفه) می‌شود. برای پاسخگویی به هر سؤال برای پاسخ‌دهنده، از طیف ۵ گزینه‌ای در مقیاس لیکرت استفاده شد. روایی ابزار پژوهش به روش محتوایی موردبرر سی قرار گرفت که میزان آن ۰/۹۳ تعیین شد. همچنین، برای بررسی همسانی درونی سنجش پایایی پژوهش از روش آلفای کرونباخ بهره گرفته شد.

جدول ۲. سنجش پایایی پرسش‌نامه بر اساس آلفای کرونباخ

پرسش‌نامه	آلفای کرونباخ	تعداد سؤالات	تعداد آزمودنی‌ها
مدیریت امنیت اطلاعات	۰/۹۸	۳۹	۱۲۰

برای تحلیل داده‌های پژوهش به‌منظور بررسی اطلاعات مربوط به فرضیه پژوهش، پس از انجام آزمون کلموگروف-اسمیرنوف و تأیید نر مال بودن داده ها، با فرض برابری وار یانس ها در گروه های موردبررسی از آزمون تحلیل واریانس (ANOVA) و برای رتبه‌بندی از آزمون فریدمن برای بررسی

فرضیه پژوهش استفاده شده است. برای تجزیه‌وتحلیل داده‌ها از نرم‌افزار اس.پی.اس.اس.، ویراست ۲۲ استفاده شد و سطح معنی‌داری ۰/۰۵ برای آن در نظر گرفته شد.

٤-یافته‌ها

بر اساس تحلیل یافته‌های پژوهش در ابتدا قبل از بررسی فرضیه‌های پژوهش باید نرمال بودن متغیرهای پژوهش توسط آزمون کولموگروف-اسمیرنوف یک نمونه‌ای بررسی شود. بر این اساس گزاره‌های زیر موردبررسی قرار گرفت و نتایج بررسی نشان داد:

H_0 : متغیر موردبررسی توزیع نرمال دارد.

H_1 : متغیر موردبررسی توزیع نرمال ندارد.

جدول ۳ . آزمون کلمگروف-اسمیرنوف برای متغیر امنیت اطلاعات و شاخص‌های آن در سازمان‌های دولتی شهر کرمان

مؤلفه‌ها / آزمون آماری	امنیت اطلاعات	امنیت اموال سازمان	امنیت عملیات و ارتباطات	نگهداری سیستم‌های اطلاعاتی	استمرار کسب‌وکار	تطابق زیرساخت و عملیات
کلمگروف-اسمیرنوف	۱/۰۶۹	۱/۲۸۰	۰/۹۳۴	۱/۶۶۲	۱/۸۰	۱/۷۸
معنی‌داری	۰/۲۰۳	۰/۲۹۸	۰/۳۴۷	۰/۱۱۲	۰/۰۹۹	۰/۱۳
نتیجه‌گیری	نرمال	نرمال	نرمال	نرمال	نرمال	نرمال

بر اساس نتایج جدول۳، آزمون کولموگوروف-اسمیرنوف و معنی‌داری به‌دست‌آمده، به دلیل آن‌که معنی‌داری به‌دست‌آمده بیشتر از ۰/۰۵ (سطح معنی‌داری پژوهش) است لذا فرض نرمال بودن برای متغیرهای تحقیق مورد تأیید قرار می‌گیرد. یعنی با ۰/۹۵ درصد اطمینان (در سطح معنی‌داری ۰/۰۵) فرض نرمال بودن پذیرفته می‌شود.

سنجش فرضیه اصلی پژوهش

فرضیه اصلی پژوهش: بین عملکرد سازمان‌های دولتی مستقر در شهر کرمان ازنظر عملکرد مدیریت امنیت زیرساخت و عملیات تفاوت معناداری وجود دارد.

H_0 : بین عملکرد سازمان‌های دولتی مستقر در شهر کرمان ازنظر عملکرد مدیریت امنیت زیرساخت و عملیات تفاوت معناداری وجود ندارد.

H_1 : بین عملکرد سازمان‌های دولتی مستقر در شهر کرمان ازنظر عملکرد مدیریت امنیت زیرساخت و عملیات تفاوت معناداری وجود دارد.

جهت بررسی فرضیه اصلی پژوهش، عملکرد مدیریت امنیت زیرساخت و عملیات در سازمان‌های دولتی شهر کرمان از آزمون ANOVA استفاده شد تا مقایسه میانگین اثرات یک یا چند متغیر مستقل بر روی یک متغیر وابسته مشخص شود (جدول ۴).

جدول ٤. آماره‌های آزمون Anova برای مقایسه عملکرد مدیریت امنیت زیرساخت و عملیات سازمان‌های دولتی کرمان

متغیرها / عملکرد	عملکرد مدیریت امنیت زیرساخت و عملیات			
–	تعداد	میانگین	انحراف معیار	–
نامطلوب	۲۸	۳/۸۸	۰/۶۲۲	
نسبتاً مطلوب	۴۷	۴/۱۲	۰/۷۰۴	
مطلوب	۴۴	۴/۰۸	۰/۶۸۸	
کل	۱۲۰			
–	منابع تغییر	مجموع مربعات	میانگین مربعات	درجه آزادی
	بین گروهی	۷/۸۲۰	۶/۵۸	۴
	درون‌گروهی	۱۲/۵۵۰	۸/۰۹	۱۱۶
	کل	۲۰/۳۷۰	–	۱۲۰
آماره	۱۵/۷۶			–
معنی‌داری	۰/۰۸۹			

نشریه مطالعات دانش‌پژوهی
صفحه | ۱۰۸
دوره ۵، شماره ۱
پیاپی ۱۵

با توجه به نتایج جدول۴، مقایسه عملکرد سازمان‌های دولتی شهر کرمان در عملکرد مدیریت امنیت زیر ساخت و عملیات بر ا ساس محا سبات از طریق آزمون ANOVA به‌د ست‌آمده و مقدار P (معنی‌داری) متغیر فوق در سطوح مختلف عملکرد مدیریت امنیت زیرساخت و عملیات برابر با ۰/۰۸۹ و بیشتر از سطح معنی‌داری ۰/۰۵ است. لذا در این سطح فرض صفر پذیرفته می‌شود و درنتیجه می‌توان گفت بین عملکرد سازمان‌های دولتی مستقر در شهر کرمان در عملکرد مدیریت امنیت زیرساخت و عملیات تفاوت معناداری وجود ندارد.

فرضیه‌های فرعی پژوهش

نتایج آزمون تی مستقل فرضیه‌های فرعی پژوهش جهت تعیین حد انتظار در سازمان‌های مورد پژوهش در جدول ۵ آورده شده است.

جدول ۵. نتایج آزمون تی، مقایسه میانگین‌ها

فرضیه‌ها	T مستقل	درجه آزادی	سطح معناداری	فاصله اطمینان		میانگین
				حد پائین	حد بالا	
مدیریت امنیت اطلاعات سازمان	۳/۰۲۱	۱۲۰	۰/۰۰۱	۱/۶۷۲	۲/۲۳۴	۱۴/۰۸۷
مدیریت امنیت اموال سازمان	۳/۴۳۲	۱۲۰	۰/۰۰۴	۱/۸۷۱	۲/۵۴۳	۱۴/۱۵۳
مدیریت امنیت عملیات و ارتباطات	۳/۰۰۳	۱۲۰	۰/۰۰۱	۱/۵۴۲	۲/۷۸۷	۱۴/۰۰۳

فرضیه‌ها	T مستقل	درجه آزادی	سطح معناداری	فاصله اطمینان		میانگین
				حد پائین	حد بالا	
مدیریت اکتساب توسعه حفظ و نگهداری	۴/۲۰۱	۱۲۰	۰/۰۰۰	۲/۴۳۷	۳/۶۷۹	۱۴/۶۷۴
مدیریت استمرار کسب‌وکار	۳/۹۶۵	۱۲۰	۰/۰۰۲	۳/۶۴۵	۴/۲۱۲	۱۴/۳۴۲
مدیریت تطابق ابعاد زیرساخت و عملیات	۴/۸۷۰	۱۲۰	۰/۰۰۲	۲/۵۶۷	۳/۳۶۳	۱۴/۷۵۴

با توجه به داده‌های جدول ۵، تمام فرضیه‌های فرعی پژوهش با سطح معنی‌داری(p_value) کمتر از ($p < ۰/۰۵$) می‌باشند که درنتیجه آزمون این فرضیه‌ها معنادار است و فعالیت این مؤلفه در سازمان‌های دولتی شهر کرمان بر اساس استاندارد موردنظر، بیشتر از حد انتظار می‌باشد.

جهت مقایسه میانگین رتبه‌های بین گروه‌های متغیر وابسته از آزمون رتبه‌بندی فریدمن استفاده شد تا مشخص می‌شود، آیا تفاوت معنی‌داری بین گروه‌ها وجود دارد یا خیر؟

جدول ٦. میانگین رتبه‌ای فریدمن

شاخص‌های عملکرد مدیریت امنیت زیرساخت و عملیات	میانگین رتبه‌ای	تعداد	کای دو	درجه آزادی	معنی‌داری
مدیریت امنیت اموال سازمان	۶/۹۵	۱۲۰	۱۹۰/۸۶	۱۰	<۰/۰۰۱
مدیریت امنیت اطلاعات سازمان	۶/۴۹				
مدیریت استمرار کسب‌وکار	۶/۳۱				
مدیریت امنیت عملیات و ارتباطات	۵/۸۶				
مدیریت اکتساب توسعه حفظ و نگهداری	۵/۸۳				
مدیریت تطابق ابعاد زیرساخت و عملیات	۴/۶۸				

در جدول۶ متوسط رتبه‌های مربوط به شاخص‌های عملکرد مدیریت امنیت زیرساخت و عملیات سازمان‌های دولتی مستقر در شهر کرمان نشان داده شده است. با توجه به یافته‌های این جدول مشخص گردید به ترتیب مدیریت امنیت اموال سازمان با میانگین(۶/۹۵)، مدیریت امنیت اطلاعات سازمان با میانگین (۶/۴۹)، مدیریت ا ستمرار کسب‌وکار با میانگین (۶/۳۱)، مدیریت امنیت عملیات و ارتباطات با میانگین (۵/۸۶)، مدیریت اکتساب توسعه حفظ و نگهداری با میانگین (۵/۸۳) و درنهایت مدیریت تطابق ابعاد زیر ساخت و عملیات با میانگین(۴/۶۸) بیشترین تأثیر گذاری را بر عملکرد مدیریت امنیت زیرساخت و عملیات سازمان‌های دولتی مستقر در شهر کرمان داشته‌اند.

۵-بحث و نتیجه‌گیری

نتایج پژوهش نشان داد که پذیرش مسئولیت سازمانی، تدوین برنامه اجرایی امنیت اطلاعات، توجه به ساختار سازمانی، نوع اطلاعات، و عنایت به الزامات امنیتی می‌تواند سازمان‌ها را تقویت کند. همچنین فعالیت‌های حرفه‌ای در سازمان باید بر اساس رعایت خط‌مشی‌های امنیتی و حفاظت از اطلاعات صورت گیرد. این یافته با نتایج پژوهش چیو و تان (۲۰۲۰)، داویگا و همکاران (۲۰۲۰)، کاندو و

همکاران (۲۰۲۱) و ایجیگو، سیپونن و مولونه (۲۰۲۱) و در خصوص سیاست‌گذاری امنیت اطلاعات و رعایت آن دارای هم‌سویی است. لذا، پیشنهاد می‌شود تا سند خط‌مشی امنیت اطلاعات، توسط مدیریت سازمان‌های موردبررسی، بر اساس استاندارد ایزو/ آی. ای. سی. ۲۷۰۰۲ تصویب شده و به اطلاع همه کارکنان و اشخاص مرتبط بیرونی برسد. علاوه بر آن، درزمینهٔ نظارت و ارزیابی مؤلفه‌های امنیت اطلاعات ضرورت دارد تا برنامه‌ها به صورت دوره‌ای بررسی و مورد ارزیابی دقیق قرار گیرد تا نقاط قوت و ضعف آن مشخص شده و مشکلات احتمالی بر اساس راه‌حل‌های کاربردی تقویت شود. نتایج پژوهش دی ویت، پیترز و ون گلدر (۲۰۲۴) و دانگ-فام و همکاران (۲۰۲۵) در این زمینه با یافته‌های پژوهش حاضر دارای هم‌سویی است. بر همین اساس، شایسته است تا مسئولیت‌های عمومی و تخصصی مدیریت امنیت اطلاعات، برای تمامی کارکنان در سطوح عالی مدیریتی، مدیریت میانی، مدیریت عملیاتی و نیز کارشناسان مشخص و تعیین شود.

همچنین، مشخص شد چنانچه سطوح مختلف مدیران ارشد، مدیران میانی، مدیران عملیاتی و کار شنا سان تعیین شود، ابزارهای نظارتی در زمان ورود و خروج به برنامه فعال با شد، و نرم‌افزارهای کنترلی برای جلوگیری از هک و نفوذ، به‌کارگیری تجهیزات و فناوری‌های سخت‌افزاری، نرم‌افزاری و کنترل اینترنت مورد بهره‌برداری قرار گیرد، زمینه ایمن‌سازی برنامه امنیت اطلاعات بهبود خواهد یافت. داشتن برنامه جامع و بهره‌گیری از امکانات هوش مصنوعی در این حوزه قابل‌اعتناست. نتایج پژوهش نوویچکا، سیکانوفسکی و میلوسکا (۲۰۲۴) درزمینهٔ برنامه کلان فناوری و امنیت اطلاعات و نیز مطالعه علمی کرویتز (۲۰۲۴) در ارتباط با امکانات هوش مصنوعی با نتایج پژوهش حاضر دارای هم سویی ا ست. بر مبنای این یافته، پیشنهاد می شود تا گزارش رخدادهای امنیت اطلاعات در تمامی بخش‌های سازمانی به‌صورت دوره‌ای ارائه و مورد تحلیل و ارزیابی قرار گیرد.

چنانچه رعایت مسائل امنیت محیطی برای پیشگیری از هرگونه خطرهای مرتبط با آسیب‌های فیزیکی در این مقوله قرار می‌گیرد. لذا نظارت نهادهای مسئول در سطح حاکمیتی در ارتباط با موارد مطرح‌شده حائز اهمیت است. این یافته با نتایج پژوهش دیش، پفاف و کرچمار (۲۰۲۰) دارای اشتراک است. یکی از مسائل مهم بهره‌گیری از سیستم‌های اطلاعاتی امنیت اطلاعات است. استاندارد ISO/IEC 27002 محور اساسی برای به‌کارگیری سیستم مدیریت امنیت اطلاعات است که راهنمایی‌های دقیق برای مستندسازی، پایش و بهبود مستمر را ایجاد می‌کند. در این زمینه یافته‌های پژوهش آریانتی (۲۰۲۵) با نتایج پژوهش حاضر دارای هم‌سویی است. علاوه بر آن، اعمال مدیریت ریسک سیستماتیک و ساختارمند ضرورتی مهم در سازمان به‌حساب می‌آید. ازاین‌رو، بررسی و شنا سایی عوامل خطرآفرین که معمولاً می‌تواند در بیرون از سازمان اتفاق بیافتد نیز باید موردعنایت قرار گیرد. نتایج پژوهش لوپز-واسکو و همکاران (۲۰۲۴) درزمینهٔ مدیریت ریسک با یافته‌های پژوهش حاضر دارای هم‌سویی است. با عنایت به یافته مطرح‌شده، پیشنهاد می‌شود تا رویه‌ها و خط‌مشی‌های امنیتی سازمان‌های دیگر بررسی و تطابق آن با برنامه‌های سازمانی انجام گیرد.

علاوه بر آن، سیستم‌های اطلاعاتی نوین باید با تهدیدهای پیشرو و تغییرهای آن‌ها هم‌سو باشند. این امر مستلزم بازبینی و بررسی مستمر فرایندهای امنیتی در قالب فناوری‌های مرتبط باشد. رعایت روش یادشده سبب می‌شود تا سازمان‌ها، در محیط پر چالش امروزی شرایط تثبیت خود را حفظ کنند. نتایج پژوهش شچپانیوک و دیگران (۲۰۲۰) و نیز اوتینو (۲۰۲۱) در خصوص نقش و امنیت سیستم‌های اطلاعاتی با یافته‌های این پژوهش دارای هم‌سویی است. از سوی دیگر، نتایج مطالعه دی ویت، پیترز و ون گلدر (۲۰۲۴) نیز درزمینهٔ تأثیر عوامل خطرپذیری سازمانی با نتایج پژوهش حاضر دارای اشتراک است. شایسته است تا سابقه‌ای رخدادهای امنیتی، تهدیدها و مشکلات پیش‌آمده در قالب یک سند مدون تهیه شده و در موارد مختلف موردبررسی قرار گرفته و با ارائه پیشنهادها و راهکارهای جدید پشتیبانی شود.

نتایج نشان می‌دهد که سازمان‌های دولتی درزمینهٔ مدیریت امکانات و دارایی‌های خود به‌خوبی عمل کرده‌اند. لذا، باید تأکید کرد که به‌کارگیری ابزارهای رایانشی و اپلیکیشن‌های تخصصی به صورت مناسبی انجام گرفته است. همچنین، در ارتباط با تأمین انرژی مناسب در زمان لازم و جلوگیری از وقفه در مؤلفه‌های حفاظتی عملکرد مطلوبی ارائه داده‌اند. در این میان باید تأکید کرد که سازمان‌دهی اطلاعات در بستر فناوری در این سازمان‌ها در حد خوب ارزیابی شده است. پژوهش شچپانیوک و دیگران (۲۰۲۰) و کام، ماتسون و گوئل (۲۰۲۰) در این زمینه با نتایج پژوهش حاضر هم‌سویی دارد.

نتایج نشان داد که در تمامی این پنج سازمان مدیریت عملیات و ارتباطات بالاتر از حد انتظار است. در این زمینه انواع برنامه‌های کاربردی، نرم‌افزارها، ابزارهای فناورانه، تجهیزات، سخت‌افزارهای عملیاتی، نظام‌های خودکارسازی شده، شرایط مطلوبی داشته‌اند؛ به‌گونه‌ای که برنامه‌ریزی مناسب برای تحول در ساختار امنیتی و تحلیل مؤلفه‌های آن در این سازمان‌ها انجام گرفته است. این نتایج با یافته‌های پژوهش دیش، پفاف و کرچمار (۲۰۲۰) و چیس (۲۰۲۱) در ارتباط با مؤلفه‌های زیرساخت و عملیات دارای اشتراک است. پیشنهاد می شود تا خط‌مشی دارای یک مالک باشد که رعایت تمامی ابعاد و مؤلفه‌های حفاظتی توسط ایشان رصد شده و مشکلات شناسایی و در رفع آن راهکار ارائه شود.

بررسی و تحلیل شاخص استمرار کسب‌وکار، نیز با توجه به میانگین نمره محاسبه شده (۴/۱۰)، نشان می‌دهد که رعایت این شاخص در سازمان‌های دولتی شهر کرمان به میزان زیاد بوده است و می‌توان نتیجه گرفت که در تمامی این پنج سازمان استمرار کسب‌وکار بالاتر از حد انتظار است. شناخت مناسب از مؤلفه خطرپذیری در سازمان، سبب طراحی خط‌مشی مناسب در زمان کار با ابزارهای فناورانه می‌شود. در این رابطه، شناسایی ویژگی‌های تجهیزات فناوری اطلاعات، در نظر گرفتن مسائل مالی و نیز مقررات اداری می‌تواند نقش مهمی در کنترل دسترسی‌ها و به‌تبع آن، حفاظت از اطلاعات سازمانی داشته باشد. یکی از راهکارهای مهم در عرصه امنیت اطلاعات بحث بیمه و پشتیبانی قوانین آن است که تا حد زیادی سبب رعایت الزامات سازمانی بیمه خواهد شد و لذا، از مشکلات بعدی جلوگیری خواهد کرد. بر همین اساس، پیشنهاد می شود تا بازبینی خط‌مشی تدوین شده برای رعایت ابعاد مختلف امنیتی به‌منظور حفاظت از اطلاعات سازمانی در دستور کار قرار گیرد.

٦-سپاسگزاری

نویسندگان از مدیران و کارکنان سازمان‌های دولتی شهر کرمان به دلیل همکاری در گردآوری اطلاعات این پژوهش سپاسگزاری می‌کنند.

۷-منابع و مآخذ

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.

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.