MEST Journal
DOI 10.12709/mest.13.13.01.07

IIA CYBERSECURITY TOPICAL REQUIREMENT AND ISO/IEC 27001

Haris Hamidovic
MKF/MKD EKI Sarajevo, Sarajevo, Bosnia and Herzegovina
https://orcid.org/0000-0002-1296-5008

JEL Category: **K22, M15**

Abstract

Cyber security protects an organization's information assets from unauthorized users, disruption, alteration, or destruction and strengthens the overall control environment to reduce risk. Cyber attacks can lead to direct and indirect effects that are often significant, as computers, networks, programs, data, and sensitive information are critical components of most organizations. Because organizations rely heavily on information technology resources, a clearly defined cybersecurity plan, objectives, inherent risks, and effective controls should be a priority for management. The IIA Cybersecurity Topical Requirement provides a consistent, comprehensive approach to assessing the design and implementation of cybersecurity governance, risk management, and control processes. The IIA's activities on the Cybersecurity Topical Requirement development will certainly contribute to increasing the cyber security level in business organizations. Given that it is possible to map the requirements from the IIA Cybersecurity Topical Requirement with the requirements from the ISO/IEC 27001 standard, it would be more than useful to use the existing good practices and experience related to the use of ISO/IEC 27001 and related standards in terms of practical implementation and assessment of compliance with IIA requirements. In this paper, we present one of the possible ways how the good practices of the international standard ISO/IEC 27001 can be used to assess the level of compliance with the IIA Cybersecurity Topical Requirement.

Keywords: *computers, information, corporate security, management of technology, auditing.*

1 INTRODUCTION

The Institute of Internal Auditors - The IIA after the research conducted at the global level indicates the risk of cyber security as the greatest risk for modern business organizations. A similar situation is expected in the next three years. (IIA, 2024 a)

Address of the author:
Haris Hamidović
haris.hamidovic@eki.ba

Therefore, the IIA launched in 2024 a pilot project for the development of topical audit requirements in the domain of cyber security. Topical requirements provide audit requirements for specific areas and clarify the audit methodology. (IIA, 2024 b)

In the middle of 2024, a draft of topical requirements in the field of cyber security was submitted to the association members for review and comments. For organizations that already use

the ISO/IEC 27001 information security management framework, we find possible appropriate mappings between IIA topical requirements and ISO/IEC 27001 requirements and controls, so we propose a more granular assessment of the degree of compliance for each of the IIA requirements than one stated in the IIA document Appendix B – Tool to Document Conformance with Topical Requirement where conformance level is expressed only as Yes / No / Partial.

2 CHALLENGES OF INFORMATION SECURITY MANAGEMENT

Failure to protect information can be seen mainly as a management failure and cannot be solved by technology alone. ISACA – the International Association of Experts for Auditing and Control of Information Systems – emphasizes that it is necessary to raise consideration of the need for adequate protection of information resources to the level of the highest management bodies of every business organization, as is done for other critical management functions. To achieve a significant improvement in information security, senior management and boards of directors must be responsible for information security management. They must provide the necessary leadership, organizational structure, oversight, resources, and processes to ensure that information security management is an integral and transparent part of governing the organization's business operations. Since information security risk is a business risk and has a direct impact on business goals, the responsibility for establishing an appropriate information security program must be balanced between security professionals and business leaders. (ISACA, 2022)

Those who understand the scope and depth of information risks increasingly say that information, as a critical resource, must be treated with the same care, caution, and prudence as any other for the business organization's survival critical asset.

Previously, the focus of protection was often on the IT systems that process and store the vast majority of information, and not on the information itself. However, today this approach is considered too narrow to achieve the level of integration, process assurance, and overall security that is really needed. Information security takes the broader view that content information and knowledge based on it must be adequately protected, regardless of how it is handled, processed, transmitted, or stored. This protection increasingly includes the need to consider security issues associated with technologies based on cloud computing and other virtual technology platforms. Business organizations exist to create value for their stakeholders. Therefore, every organization - commercial or not - has value creation as a management objective. Creating value means realizing benefits with optimal use of resources and risk optimization. Benefits can take many forms, such as: financial for commercial enterprises and high-quality public service for state entities. (ISACA, 2022)

The increasing dependence on information and supporting systems and the growing risk of numerous threats force management to make difficult and often expensive decisions about effectively solving the information security problem. In addition, numerous new and existing laws and regulations increasingly require compliance and a higher level of accountability due to governments' efforts to address sophisticated attacks and growing losses that pose an increasing threat to the nation's critical infrastructure. (ISACA, 2022)

3 AREA OF APPLICATION OF INFORMATION SECURITY

Information security deals with all aspects of information in any medium (eg, written, spoken, electronic), regardless of whether the information is created, viewed, transmitted, stored, or destroyed. It differs from IT security, which deals with information security within the boundaries of a technology domain, usually in a custodial capacity. It is significant to pay attention to this difference. The IT department usually does not own most of the information in its systems; instead usually, it just owns devices that process information. Information is under the supervision, control, and custody of the IT, and the IT functions as the custodian of the data owner. (ISACA, 2021)

Professional literature mentions cyber security as a particular topic and concept and as an area of specific concern, significant for the management of overall information security. Although definitions

vary widely, it is commonly believed that cybersecurity is a sub-discipline of information security. Specific areas covered by cyber security include Advanced Persistent Threats (APT), malware, ransomware, identity theft in all its forms, and several other cyber-related threats. It should be remembered that in many areas in recent years there has been a convergence of cyber security and information security. (ISACA, 2021)

In the context of information security management, it is important that the scope and responsibilities of information security are clearly stated in the information security strategy and reflected in the policies. It is also essential that information security is fully supported by senior management and various organizational units. Without clearly defined responsibilities for information security, it is impossible to assign responsibility. (ISACA, 2021)

4 ASSESSMENT AND EVALUATION OF CYBER SECURITY MANAGEMENT

When performing an internal audit engagement that includes cybersecurity objectives in their scope, internal auditors must assess whether the organization's management processes adequately address cybersecurity.

According to the IIA Cybersecurity, Topical Requirements are structured to guide performing internal audit services in three areas: governance, risk management, and control processes. Each area includes (IIA, 2024 b):

- Requirements, which are mandatory and cover essential organizational objectives.
- Considerations, which are not mandatory but serve as best practices for evaluating the design and implementation of organizational objectives.

For example, in the Evaluating and Assessing Cybersecurity Governance domain, it is stated that auditors must assess whether Policies and procedures related to cybersecurity risk management processes are established and periodically updated, including the promotion of practices that strengthen the control environment based on widely adopted frameworks (NIST, COBIT, and others).

Considerations for this Governance Requirement are: To assess how the essential governance processes are applied to cybersecurity objectives, internal auditors may review:

Policies, procedures, and other relevant documentation used by the organization to oversee daily cybersecurity duties including:

1. Documents that are clear, concise, consistent, and regularly updated, particularly as new cybersecurity risks emerge and no less than annually.
2. Procedures concerning the identification, analysis, resolution, and reporting of breaches or other instances of sensitive data loss.
3. Documentation detailing how management ensures those policies and procedures are adequate to uphold cybersecurity operations. (IIA, 2024-b)

In Evaluating and Assessing Cybersecurity Risk Management, we find Requirement: A process is established to identify and manage cybersecurity risks related to third parties. Vendors, suppliers, and other providers of outsourced processes and/or services are contractually required to implement effective cybersecurity controls that adequately protect the confidentiality, integrity, and availability of the organization's systems and data to which third parties have access.

The appropriate considerations are (IIA, 2024 b):

- To assess the required aspects of cybersecurity risk management, internal auditors may review the organization's process for managing third-party cybersecurity risks.
- To verify that vendor cybersecurity controls are applied before starting a business relationship and that contracts build in the right to periodic reviews throughout the relationship.
- To include obtaining and analyzing the third party's service organization controls report and verifying the organization has documented its SOC report review, which should include ensuring user control considerations have been implemented.
- Gain an understanding of management's approach to determining if third parties have an appropriate control environment that is

commensurate with the organization's controls.

When it comes to the area of Evaluating and Assessing Cybersecurity Control Processes, as an example we will cite Requirements: Adequately integrates cybersecurity into the system development life cycle for business applications, including software and acquired or custom-developed applications.

The appropriate considerations are: How the organization addresses cybersecurity within its system development life cycle, including the following control aspects:

1. Planning: Cybersecurity has been identified as a key component when assessing risks and analyzing potential vulnerabilities. The scope and objectives of the software implementation should be included as the organization evaluates cybersecurity controls during the planning phase.
2. Gathering requirements: Cybersecurity requirements are a component when defining functional requirements, which should also include complying with all applicable legal and regulatory requirements.
3. Design: Cybersecurity considerations are included as an integral part of the detailed processing requirements. Controls should be identified in all design aspects as the organization more formally defines the needs of the system architecture design (such as platforms, user interfaces, databases, and others).
4. Development: The organization has established a secure environment and formally defined a development process that minimizes cyber vulnerabilities (for example, limited user access to development code, appropriate segregation from the production environment, the use of approved tools, the existence of audit trails to track development activities, specific cybersecurity requirements for vendor-developed software, and others).
5. Testing: The organization includes the review and assessment of cybersecurity during the testing phase (for example, automated testing, penetration testing, and vulnerability assessment). The organization should be able to quickly be alerted to and address any cyber vulnerabilities identified through testing, which includes a detailed description of the vulnerability and what code changes or mitigating controls were established in response.
6. Deployment: As new software is moved into production, the organization should carefully monitor potential cybersecurity threats, including ensuring end-users have been trained to use the software in a way that minimizes cybersecurity risks. The organization should ensure that events and errors are logged and analyzed related to potential cybersecurity events.
7. Maintenance: The organization should ensure that all security-related software releases are applied promptly and should have open communication with software vendors to ensure emerging risks and threats are properly controlled and that end-users are informed of any known vulnerabilities. (IIA, 2024 b)

5 MAPPING WITH REQUIREMENTS FROM ISO/IEC 27001

By analyzing each of the IIA Cybersecurity Topical Requirements, we find a corresponding mapping to one or more controls and processes from the international standard ISO/IEC 27001. (ISO/IEC, 2022 a)

For example, for the IIA Cybersecurity Topical Requirement:

“Internal auditors must assess if the organization has implemented appropriate physical security controls to protect high-risk information centers (such as data centers, network operations centers, and security operations centers) from attacks”

we find the following possible mappings with ISO/IEC 27001 controls:

7.1. Physical controls
7.2. Physical security perimeters
7.3. Physical entry
7.4. Securing offices, rooms, and facilities
7.5. Physical security monitoring
7.6. Protecting against physical and environmental threats

For each of the controls in the international standard ISO/IEC 27002, we can find

recommendations regarding their implementation. (ISO/IEC, 2022 b)

So, for example, for 7.6 Protecting against physical and environmental threats, the control description is stated: Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to the infrastructure should be designed and implemented. The purpose of control is to prevent or reduce the consequences of events originating from physical and environmental threats. The guidance for implementation is risk assessment to identify the potential consequences of physical and environmental threats. It should be performed at a physical site before beginning critical operations and at regular intervals. Necessary safeguards should be implemented and changes to threats should be monitored. Specialist's advice should be obtained on how to manage risks arising from physical and environmental threats such as fire, flood, earthquake, explosion, civil unrest, toxic waste, environmental emissions, and other forms of natural disasters or disasters caused by human beings…(ISO/IEC, 2022 b)

When it comes to assessing the level of implementation, the following scale, which can be found in professional literature, can be useful (ISO27k Forum, 2022):

1. Nonexistent - Complete lack of recognizable policy, procedure, control, etc.
2. Initial - Development has barely started and will require significant work to fulfill the requirements
3. Limited - Progressing nicely but not yet complete
4. Defined - Development is more or less complete although detail is lacking and/or it is not yet implemented, enforced, and actively supported by top management
5. Managed - Development is complete, the process/control has been implemented, and recently started operating
6. Optimized - The requirement is fully satisfied, is operating fully as expected, is being actively monitored and improved, and there is substantial evidence to prove all that to the auditors

The levels of implementation can further be expressed in the form of a scale from 0 to 5, and the level of implementation could be more clearly displayed on a scale from 0 to 1 - for example in Figure 1.

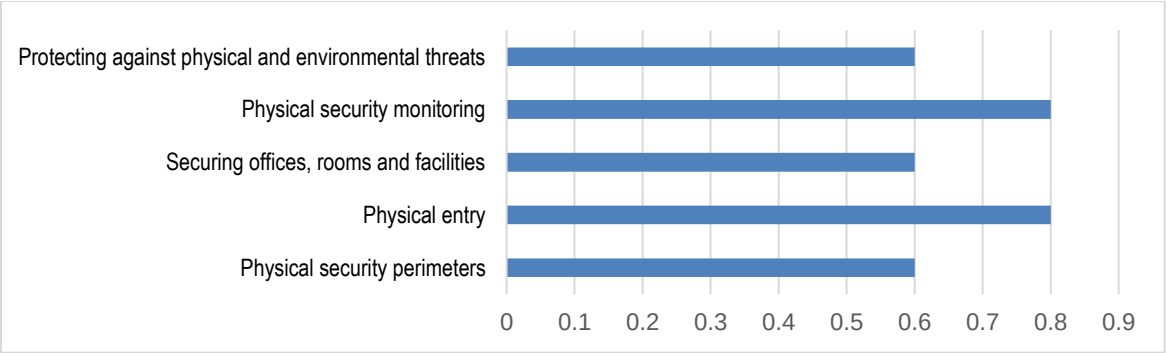

Fig. 1 An example of the achieved level of implementation

6 CONCLUSIONS

IIA's activities on the Cybersecurity Topical Requirement development will certainly contribute to increasing the cyber security level in business organizations. Given that it is possible to map the requirements from the IIA Cybersecurity Topical Requirement with the requirements from the ISO/IEC 27001 standard, we think that it is necessary to use the existing good practices related to the use of this and related standards in terms of compliance with the IIA requirements. The example of the level of compliance presented in the paper, which consists of 5 levels, can give auditors and security managers a more realistic picture of the level of compliance achieved, and areas where more efforts need to be made to overcome the discrepancy between the existing and the desired state.

WORKS CITED

ISACA. (2021, Mar 31). *Cybersecurity Fundamentals Study Guide*, 3rd Edition. ISBN 978-1604207514. Isaca

ISACA. (2022, Feb 28). *CISM Review Manual, 16th Edition*. ISBN 978-1604209013. Isaca

IIA. (2024a). *Risk in Focus 2024 Global Summary*. Retrieved from The Institute of Internal Auditors, https://www.theiia.org/en/internal-audit-foundation/latest-research-and-products/risk-in-focus/

IIA. (2024b). *Cybersecurity Topical Requirement.* Retrieved from The Institute of Internal Auditors, https://www.theiia.org/globalassets/site/standards/editable-versions/cybersecurity-topical-requirement-english.pdf

ISO/IEC. (2022a). ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Retrieved from ISO, https://www.iso.org/standard/27001

ISO/IEC. (2022b). ISO/IEC 27002:2022, Information security, cybersecurity, and privacy protection — Information security controls. Retrieved from ISO, https://www.iso.org/standard/75652.html

ISO27k Forum. (2022). ISO/IEC 27001:2022 ISMS Status, Statement of Applicability (SoA), and Controls Status (gap analysis) workbook. Retrieved from ISO, https://www.iso27001security.com/ISO27k_ISMS_6.1_SoA_2022.xlsx

Received for publication: 05.08.2024
Revision received: 17.08.2024
Accepted for publication: 08.01.2025.

How to cite this article?

Style – **APA** *Sixth Edition:*

Hamidovic, H. (2025, 01 15). IIA Cybersecurity Topical Requirement and ISO/IEC 27001. (Z. Cekerevac, Ed.) *MEST Journal, 13*(1), 76-81. doi:10.12709/mest.13.13.01.07

Style – **Chicago** *Sixteenth Edition:*

Hamidovic, Haris. "IIA Cybersecurity Topical Requirement and ISO/IEC 27001." Edited by Zoran Cekerevac. *MEST Journal* (MESTE) 13, no. 1 (01 2025): 76-81.

Style – **GOST** *Name Sort:*

Hamidovic Haris IIA Cybersecurity Topical Requirement and ISO/IEC 27001 [Journal] // MEST Journal / ed. Cekerevac Zoran. - Belgrade – Toronto : MESTE, 01 15, 2025. - 1 : Vol. 13. - pp. 76-81.

Style – **Harvard** *Anglia:*

Hamidovic, H., 2025. IIA Cybersecurity Topical Requirement and ISO/IEC 27001. *MEST Journal,* 15 01, 13(1), pp. 76-81.

Style – **ISO 690** *Numerical Reference:*

IIA Cybersecurity Topical Requirement and ISO/IEC 27001. **Hamidovic, Haris.** [ed.] Zoran Cekerevac. 1, Belgrade – Toronto : MESTE, 01 15, 2025, MEST Journal, Vol. 13, pp. 76-81.