THE STRUCTURE OF THE ISMS DOCUMENTATION IN ACCORDANCE WITH UPDATES TO ISO 27001:2022, 27002:2022

Dmitrii OBUH

Department of Software Engineering and Automation, Information Security, Faculty of computers, Informatics and Microelectronics, Technical University Of Moldova, Chisinau, Republic of Moldova

Corresponding author: Dmitrii OBUH, dmtrii.obuh@isa.utm.md

Tutor/coordinator: Rodica BULAI, university lecturer, in charge of the study program Information Security

Abstract. *Building information security in the modern world is one of the most important aspects of the stable development of any IT business. In order not to reinvent the wheel, it is most logical to use already proven solutions, namely to follow the international standards ISO 27001, ISO 27002. This paper will contain recommendations on the organization of the documentation structure according to the current updates of the above-mentioned standards.*

Keywords: *ISMS, documentation, ISO 27001, ISO 27002.*

Introduction

The ISO/IEC 27001:2022 is a global standard that outlines guidelines for managing information security in a company. This specification enables organizations of any kind to safeguard the security of various types of data, including employee information, financial records, intellectual property, and data shared with third-party entities [1].

The ISO 27001 standard outlines the necessary conditions for creating an Information Security Management System (ISMS) [2]. In contrast, the ISO 27002 provides advice on how to implement each of these conditions [3]. An ISMS involves a complete approach to handling confidential data within an organization, using risk management strategies to maintain security and protection.

An ISMS is designed to mitigate the risk of security breaches and maintain uninterrupted business operations by taking proactive measures to limit the impact of such incidents. It generally focuses not only on data and technology but also on employee behavior and processes [4].

These standards require specific documentation detailing policies and procedures. The disclosure of the topic and recommendations will be in the following chapters.

Contribution: In this paper, I develop an analysis of the most up-to-date standards to make recommendations on the organization of documentation to ensure information security. After studying many sources of information, I came to the conclusion that each organization needs its own set of documents, but nevertheless, it is possible to develop a versatile list that will be relevant and useful for many organizations. However, we should remember that an effective information security management system must be tailored to requirements of an organization [5].

A discussion about additional, but no less important documentation that is not included in the standards completes this paper.

Paper structure: This paper is structured in four sections, the first one being the introduction. In Section 2 I do an overview of the changes that have been made to the 2022 sample standard compared to 2013. Section 3 consists of recommendations on the structure of the documentation. We conclude with Section 4.

Overview of changes in the standards

The ISO 27001:2022 standard contains many useful optimizations. The number of sections in Appendix A has been reduced from 14 to 4 [6]. 57 security controls were merged, 11 new controls appeared. Here are new security controls:

- A.5.7 – Threat intelligence
- A.5.23 – Information security for use of cloud services
- A.5.30 – ICT readiness for business continuity
- A.7.4 – Physical security monitoring
- A.8.9 – Configuration management
- A.8.10 – Information deletion
- A.8.11 – Data masking
- A.8.12 – Data leakage prevention
- A.8.16 – Monitoring activities
- A.8.23 – Web filtering
- A.8.28 – Secure config

It's worth mentioning that the clause "6.2 Information security objectives and planning to achieve them" now states that the objectives should be monitored and also be available in a documented form [7]. Ultimately, if you have an ISMS and you want to update it in accordance with the latest standard, you need to do the following:

- Update the ISMS Management review procedure
- Update information security objectives and the Monitoring, measurement analysis and evaluation procedure
- Align the Risk Treatment Plan with the new structure of controls
- Update the Statement of Applicability
- Update the ISMS Communication Plan
- Update checklists and questionnaires used for audits
- Update other policies if needed

Recommendations on the structure of the documentation

The ISMS Documentation comprises several components, including the following levels:

- Level 0 - Corporate Information System Security Policy: This is the highest-level security policy of a company.
- Level 1 - ISMS Manual: This document outlines the ISO/IEC 27001 standard requirements and explains how the established ISMS satisfies those requirements.
- Level 2 - Supporting Policies and Guidelines: It consists of a complete collection of technical policies and guidelines that correspond to the ISMS scope.
- Level 3 - Procedures and Processes: This level contains the necessary processes and procedures for implementing and supporting the defined policies and guidelines.
- Level 4 - Templates and Forms: These templates and forms are utilized to streamline the operation of ISMS and serve as the foundation for records [8].

There are no specific rules regarding the format or quantity of documents required for an ISMS. Nevertheless, the information specified below must be recorded in written form [9]:

- Scope of the ISMS
- Risk assessment and risk treatment methodology
- Risk assessment and risk treatment report [10]
- Risk treatment plan
- Information security policy and objectives
- Statement of Applicability
- Acceptable use of assets
- Inventory of assets
- Definition of security roles and responsibilities
- Operating procedures for IT management
- Access control policy
- Supplier security policy

- Secure system engineering principles
- Incident management procedure
- Legal, regulatory and contractual requirements
- Business continuity procedures [11]

To satisfy the standards for continuous enhancement and offer substantiated proof of your ongoing initiatives, organizations should maintain written records of the following:

- Results of the management review
- Records of training, skills, experience and qualifications
- Internal audit program
- Results of internal audits [12]
- Monitoring and measurement results
- Logs of user activities, exceptions and security events
- Results of corrective actions

Presented below is a roster of guidelines that are necessary to adhere to the ISO 27001 Annex A. It is an essential addition to your documentations [13]:

- Mobile Device Policy
- Backup Policy
- Clear Screen and Clear Desk Policy
- Secure Development Policy
- Remote Work Policy
- Cryptographic Controls Policy
- Key Management Policy
- Information Transfer Policies (and Procedures)

The number and nature of extra documents required may vary depending on the organization's type and size. However, the subsequent records, which are beneficial for almost all organizations, should be kept:

- A policy outlining the classification of documented information
- A procedure for internal audit that is recorded
- A written procedure governing document control

A possible list of security policies that meet the requirements of ISO 27001 and ISO 27002 that will suit most companies may be the following:

- Human Resources Security Policy
- Incident Response Policy
- Project & Resource Management Policy
- Third-Party Management Policy
- Security & Privacy Governance Policy
- Vulnerability & Patch Management Policy
- Antivirus policy
- Secure Engineering & Architecture Policy
- Identification & Authentication Policy
- Network Security Policy
- Data Classification & Handling Policy
- Asset Management Policy
- Security Operations Policy
- Security Awareness & Training Policy
- Continuous Monitoring Policy
- Change Management Policy
- Compliance Policy
- Physical & Environmental Security Policy
- Information Exchange Security Management Policy

- Capacity & Performance Planning Policy
- Configuration Management Policy
- Business Continuity & Disaster Recovery Policy [14]
- Endpoint Security Policy
- Maintenance Policy
- Privacy Policy
- Technology Development & Acquisition Policy

Additional documents frequently used in the implementation of ISO 27001 [15]:

- Documentation management procedure
- Password Policy
- Rules for working in safe zones
- Business Impact Analysis
- Maintenance and inspection plan
- Disposal and Destruction Policy

The documentation for operations needs to comprise comprehensive directives pertaining to:

- Restarting and recovering the system
- Handling and processing of information
- Procedures for disaster recovery
- Management of changes, including scheduled maintenance and interrelationships between components
- Date of the last review and update
- Handling of audits and system logs
- Document classification
- Procedures for handling exceptions, along with a record of any exceptions
- Contacts for operations, technical support, emergency, and business purposes
- Managing output and media, including the secure disposal or destruction of sensitive data
- Back-up and recovery, encompassing on-site and off-site storage options
- Computer room management and safety protocols

It is also advisable to document other common activities, such as:

- The creation of a Risk Treatment Plan by the Risk Committee
- Scheduling and reports from Internal Audits
- Reviews of the Information Security Management System by Management
- Assessments of non-conformities or reported incidents by the Information Security Team

Conclusions

Following the ISO 27001, ISO 27002 industrial standards, it is possible to organize the structure of the ISMS documentation most effectively.

There are organizations that do not pay due attention to the elaboration of documents declaring the goals and objectives of information security, a set of measures to improve and modernize the information security of the enterprise. Negligent attitude to the creation of the ISMS documentation can subsequently lead to large time costs in the event of information security incidents, to an increase in cases of unintentional damage to the organization by employees due to insufficient awareness of the basic provisions and principles of information security.

In this paper, I talked about ISO standards, conducted a comparative analysis of the most current versions of 2022 with the versions of 2013, pointed out what you should pay attention to in order to update the company's documentation in accordance with the latest version of the standard, being certified according to the previous version, and also made recommendations on the organization of the structure of the ISMS documentation, which suitable for most organizations.

References

1. QUSEF, A., ALKILANI, H. The effect of ISO/IEC 27001 standard over open-source intelligence. In: *PeerJ. Ltd*, 2022.
2. BRENNER, J. ISO 27001 risk management and compliance. In: *Sabinet Online*, 2007.
3. EVANS, L. Protecting information assets using ISO/IEC security standards. In: *Association of Records Managers & Administrators (ARMA)*, 2016.
4. YASAR, K. What is Information Security Management (ISMS). [online]. 2022. [accessed 25.10.2022]. Available: https://www.techtarget.com/whatis/definition/information-security-management-system-ISMS#:~:text=The%20goal%20of%20an%20ISMS,well%20as%20data%20and%20technology
5. SALKIC, A. ISO 27001: What documentation is required for certification. [online]. 2021. [accessed 04.11.2022]. Available: https://sec-consult.com/blog/detail/iso-27001-what-documentation-is-required-for-certification/
6. KOSUTIC, D. ISO 27001 2013 vs. 2022 revision – What has changed. [online]. 2022. [accessed 29.10.2022]. Available: https://advisera.com/27001academy/blog/2022/02/09/iso-27001-iso-27002/
7. PROZOROV, A. ISO 27001:2022. What has changed. [online]. 2022. [accessed 01.11.2022]. Available: https://www.securitylab.ru/blog/personal/80na20/352401.php
8. BISWAS, P. ISO 27001:2013 ISMS Manual. [online]. 2020. [accessed 02.11.2022]. Available: https://preteshbiswas.com/2020/01/08/iso-270012013-isms-manual/
9. ISO 27001 and ISO 27002 Compliance, ImmuniWeb. [online]. [accessed 02.11.2022]. Available: https://www.immuniweb.com/compliance/iso27001-compliance-audit-checklist/
10. BISCOE, C. ISO 27001 Documentation Checklist. [online]. 2017. [accessed 03.11.2022]. Available: https://www.vigilantsoftware.co.uk/blog/iso-27001-documentation-checklist
11. TALIB, M.A., KHELEFI, A., BARACHI, M.E., ORMANDJIEVA, O. Guide to ISO 27001: UAE case study. In: *Informing Science Institute*, 2012.
12. MAUS, B. ISO 27001 Certification – What to Consider. [online]. 2022. [accessed 05.11.2022]. Available: https://otrs.com/otrsmag/iso-iec-27001-certification/
13. ISO 27001 Checklist: The Documentation Required, Risk Crew. [online]. [accessed 28.10.2022]. Available: https://www.riskcrew.com/2022/07/iso-27001-documentation-whats-required-and-whats-optional/
14. ISO 27001 & 27002 Based Security Documentation, ComplianceForge. [online]. [accessed 03.11.2022]. Available: https://www.complianceforge.com/product/iso-27001-27002-policies-standards-cdpp/
15. Documentatsiya pod ISO 27001:2013. Skolko yeyo dolzhno byt i kakoy? [Documentation for ISO 27001:2013. How much should it be and what?], Export center. [online]. [accessed 05.11.2022]. Available: https://export-center.by/blogpost/documents-27001