SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2023
ORGANIZATION AND MANAGEMENT SERIES NO. 187

INTEGRATION OF AQAP 2110 STANDARD REQUIREMENTS WITH INFORMATION SECURITY REQUIREMENTS ACCORDING TO ISO 27001

Natalia JAGODZIŃSKA

BTCH Systemy Zarządzania; natalia.jagodzinska@outlook.com

Purpose: Presentation of the possibilities of implementing an integrated management system AQAP 2110 and ISO 27001.
Design/methodology/approach: The comparative method presents the common elements and differences of the AQAP 2110 and ISO 27001 standards and the possibility of their integral implementation in the organization.
Findings: During the analysis, information was obtained that, to a significant extent, the requirements of both AQAP 2110 and ISO 27001 standards are consistent and their integration is very beneficial for the organization.
Research limitations/implications: Demonstrated ability to integrate the requirements of AQAP 2110 and ISO 27001 and may be an indication for integration with other systems, e.g. ISO 14001, ISO 45001.
Practical implications: The analysis will simplify the process of implementing ISO 27001 and AQAP management systems, which will reduce implementation costs and shorten implementation time.
Social implications: The analysis is addressed to enterprises and has no impact on the society around us.
Originality/value: The article presents the possibilities of integrating the requirements of the AQAP 2110 and ISO 27001 standards that apply to organizations implementing projects in the military sector.

Keywords: AQAP 2110, ISO 27001, systems integration AQAP 2110 and ISO 27001.

1. Introduction

Many companies carrying out projects for the military are obliged to ensure NATO and information security standards. That is why these companies decide to implement the NATO standard - AQAP 2110 NATO requirements for quality assurance in design, development and production and the ISO 27001 standard - Information Security Management System.

Integrating the requirements of the AQAP 2110 standard with the information security requirements of ISO 27001 is possible because both standards have many elements in common that relate to information security and risk management.

AQAP 2110 is a NATO standard that deals with quality management in defense projects. This standard requires organizations to meet specific requirements for the quality, security, and availability of information. ISO 27001, on the other hand, is an information security management standard that specifies requirements for processes, procedures, and controls related to information protection.

In order to integrate the requirements of the AQAP 2110 standard with the information security requirements of ISO 27001, it is first necessary to identify common areas and set appropriate integration goals. For this purpose, the PDCA (Plan-Do-Check-Act) methodology (Rogala, 2020), used in most ISO standards (most often ISO 9001, ISO 14001, ISO 5000, etc.), can be used, which will allow to ensure continuous improvement of processes related to information security.

The next step is to conduct a risk analysis to identify threats and determine their impact on the achievement of the organization's goals. On this basis, it is possible to determine appropriate controls and procedures that will ensure information security (Skrzypek, 2000) and meet the requirements of AQAP 2110 and ISO 27001 standards.

During the integration of requirements, it is also necessary to take care of documentation that will confirm that the requirements of both standards are met. It is also important to remember about regular reviews and audits to monitor the effectiveness of the solutions used and identify areas for further improvement.

To sum up, the integration of the requirements of the AQAP 2110 standard with the information security requirements of ISO 27001 requires a detailed analysis and determination of appropriate controls and procedures that will ensure information security and compliance with the requirements of both standards. Implementing requirements integration can allow for better control of processes, reduce the risk of information security incidents, and improve the efficiency of the organization's operations.

2. About AQAP 2110 and ISO27001

2.1. AQAP Standard

AQAP 2110 (AQAP 2110, 2016) is a NATO standard for quality management in the design, manufacture and supply of defence products. This standard is designed to ensure high quality and reliability of products and compliance with NATO requirements.

This standard defines the requirements for a quality management system that should be met by suppliers of defense products. It also outlines the procedures and processes to be followed to ensure quality in various areas such as design, manufacturing, quality control, supplier management, and after-sales service.

The requirements of this standard (AQAP 2110 SRD1, 2016) include, m.in, establishing and documenting policy, process planning and monitoring, configuration control, product identification and traceability, risk management, and ensuring the secure flow of information. Ensuring high quality products is crucial for NATO to ensure that the defence products supplied meet all safety and reliability requirements.

The AQAP 2110 standard is available for suppliers who wish to provide services or products for NATO. Its use allows for the standardization of processes and procedures, which facilitates the exchange of information and cooperation between suppliers and NATO allies.

2.2. ISO 27001 Standard

ISO 27001 is an international standard that specifies the requirements for information security management in an organization. This standard describes the processes, procedures, policies, and practices that should be implemented for effective information risk management.

The main purpose of ISO 27001 is to ensure the confidentiality, integrity and availability of information, as well as to minimize the risk of loss, destruction or unauthorized disclosure of information. This standard assumes that information security management should be managed in a systematic manner and integrated with other processes of the organization.

The ISO 27001 standard covers many areas (ISO 27002, 2023), including: risk assessment, information security policy, management of resources such as human resources, infrastructure and technology, physical security, communication and operations management, information security incident management.

ISO 27001 is flexible and can be adapted to different types of organizations and industries. Its implementation allows for effective information security management and minimization of the risk of cyber threats.

3. AQAP 2110 and ISO 27001 Integration Elements

The integration of the implementation of AQAP 2110 (NATO) with ISO 27001 is aimed at ensuring consistency and comprehensive management of information security in defense-related organizations. The common elements between the AQAP 2110 standard and the ISO 27001 standard are primarily related to issues related to information security and risk management. Here are some of those items:

Risk analysis - both standards require a risk analysis to identify threats to information and determine the actions to be taken to minimize the risk of incidents.

Security Controls – Both AQAP 2110 and ISO 27001 require organizations to apply appropriate security controls to protect information from unauthorized access, loss, damage, or theft.

Incident Management – Both standards require organizations to have appropriate procedures in place for responding to and reporting on information security incidents.

Information Security Policy – Both AQAP 2110 and ISO 27001 require organizations to have a clearly defined information security policy that will provide a framework for information protection activities.

Internal Audit – Both standards require organizations to conduct regular internal audits to assess the effectiveness of information security activities and identify areas for further improvement.

Business continuity – both AQAP 2110 and ISO 27001 require organizations to have adequate follow-up plans in place when incidents such as disasters, natural disasters, or cyber-attacks occur.

Integrating the requirements of the AQAP 2110 standard with the information security requirements of ISO 27001 can allow for more effective risk management and protection of information against various threats.

3.1. Risk analysis

Risk analysis is the process of identifying, assessing, and managing information security risks in an organization. Both the AQAP 2110 standard and the ISO 27001 standard require this analysis to be performed as a core component of an information security management system.

In AQAP 2110, risk analysis is an important part of the process of identifying threats to information related to systems that are designed, developed, or maintained by organizations involved in the defense sector. As part of the risk analysis in AQAP 2110, many factors should be considered, such as the probability of the hazard occurring, its effects, as well as the risks coming from the system itself, its users, applications, or the external context. All of these factors need to be assessed and appropriate countermeasures implemented to reduce the risk to systems and the information associated with them.

On the other hand, in ISO 27001, risk analysis refers to the identification of risks related to information security in the organization, such as threats from cybercriminals, malware attacks, unauthorized access to data, user errors, or hardware and software failures. This process consists of several steps, including asset identification, hazard identification, and risk assessment. Once the risk has been assessed, appropriate security controls should be put in place to help minimize the risk of information security incidents.

In both standards, AQAP 2110 and ISO 27001, the risk analysis process is crucial to ensure an appropriate level of information security and risk management. Conducting this analysis allows you to identify potential threats, determine their effects, and develop appropriate countermeasures to minimize the risk to the information and systems associated with them.

3.2. Security check

Security controls are a key element of information security management in organizations. Both the AQAP 2110 standard and the ISO 27001 standard require the implementation of appropriate security controls to minimize the risk of information security incidents.

The following are examples of security controls that are recommended under AQAP 2110 and ISO 27001.

- Access controls: restricting access to systems and information to only authorized users.
- Configuration checks: Monitoring and managing the configuration of systems to minimize the risk of information security incidents.
- IT tool management checks: deploy software updates to address vulnerabilities.
- Physical access control controls: control access to buildings, premises, and equipment to minimize the risk of information security incidents.
- Risk management controls: identifying and assessing information security risks and implementing appropriate countermeasures.

In addition, in the ISO 27001 system we have monitoring controls: monitoring systems and information for early detection and response to irregularities, and training and awareness checks: training employees in information security and increasing their awareness of threats.

Security controls in AQAP 2110 and ISO 27001 are essential to ensure an appropriate level of information security and risk management.

3.3. Incident management

Incident management is a key component of information security management in organizations. Both the AQAP 2110 standard and the ISO 27001 standard require the implementation of appropriate incident management procedures and plans to effectively respond to information security threats. Incident response procedures should be developed and implemented to enable a rapid and effective response to any information security incidents. As a result of the monitoring, a contingency plan should be created that should be available and up-to-date to enable rapid action in the event of a system or network failure. The implemented procedures are designed to quickly and effectively recover systems in the event of a disaster. These activities should be supported by procedures for incident reporting, incident handling and security plans.

Incident management in AQAP 2110 and ISO 27001 is essential to ensure effective information protection and minimize the risk of information security incidents.

3.4. System Policy

The Information Security Policy for ISO 27001 or the Quality Policy for AQAP2110 the foundation of the management system. Both the AQAP 2110 standard and the ISO 27001 standard require organizations to have a clearly defined information security policy and Quality Policy, which is the basis for activities related to ensuring security, risk supervision and information protection. Common elements that can be included in an information security and quality policy in accordance with AQAP 2110 and ISO 27001 are:

- Management involvement.
- Compliance with laws and regulations.
- Protecting the confidentiality, integrity and availability of information.
- Management of access rights.
- Employee training.
- Risk management.
- Monitoring and audits.

3.5. Internal audits

Internal audits are an important part of management according to both the AQAP 2110 and ISO 27001 standards. Their purpose is to assess the effectiveness of the management system and to identify areas for improvement. Here, the requirements of both standards are consistent and include:

a) Audit scheduling: Both AQAP 2110 and ISO 27001 require organizations to schedule internal audits on a systematic and regular basis. Audit planning should take into account the importance of individual elements of the information security management system and their criticality for the organization.
b) Conducting an audit: Internal audits should be conducted by individuals who are independent of the areas being audited. In the case of AQAP 2110 and ISO 27001, auditors should have relevant qualifications and experience in the field of information security management.
c) Conformity Assessment: During internal audits, both AQAP 2110 and ISO 27001 require an assessment of compliance with the requirements of the standard and the information security policy. The conformity assessment should take into account both technical and organizational aspects.
d) Identification of corrective actions: Internal audit should identify areas for improvement and corrective actions. In the case of AQAP 2110 and ISO 27001, auditors should identify information security risks and recommend appropriate countermeasures.

e) Reporting audit results: Both AQAP 2110 and ISO 27001 require that the results of internal audits be reported at an appropriate level within the organization. The reports should include information on identified non-conformities, corrective actions and recommendations for the Management Board. Reports should also be made available to the audited areas to enable the implementation of corrective actions.

3.6. Business continuity

Business continuity management is a key element of management for both standards. It ensures that your organization is ready to handle incidents and maintain business continuity in the event of disruptions. According to the AQAP 2110 and ISO 27001 standards, business continuity should be implemented on the basis of the following model:

a) Business continuity analysis: Organizations should conduct a regular business continuity analysis. This analysis should include risk identification and assessment, as well as the determination of critical business processes and their dependencies.
b) Business continuity planning: Based on the business continuity analysis, organizations should develop a business continuity plan that outlines strategies and procedures for dealing with incidents. The plan should include, m.in. defining the role and responsibilities of employees, contingency procedures, and data recovery plans.
c) Implement and test plans: It's important for organizations to implement business continuity plans and test them regularly to assess their effectiveness.
d) Review and update: Standards require organizations to regularly review and update business continuity plans. This review should take into account changes in the organization, changes in the business environment, and the results of plan tests.
e) Awareness and training: Employee awareness of business continuity plans and their role and accountability in the event of incidents is required. Employees should be trained in crisis management and the implementation of business continuity plans.

4. Different in risk and security management requirements in AQAP 2110 and ISO 27001 standards.

AQAP 2110 and ISO 27001 are two different standards related to risk management and information security management, and their approach to managing this area differs in several aspects. The following are some key differences in the approach to management in both standards:

a) Scope and purpose: AQAP 2110 is a standard for the defense sector, while ISO 27001 is a general standard that can be used in various sectors. AQAP 2110 focuses on specific information security threats and requirements in the defense sector, and ISO 27001 in all business areas.
b) Documentation: AQAP 2110 requires detailed documentation, including information security-related plans and procedures, while ISO 27001 focuses on the performance and performance of an information security management system, allowing for greater flexibility and customization to meet the specific needs of an organization.
c) Importance of risk: AQAP 2110 assumes that risk assessment is a key element of project management (including information security) and requires organizations to conduct regular risk analysis and implement appropriate preventive measures. ISO 27001 also requires a risk assessment especially for information assets, but the approach to it is more formal and factual and depends on the individual needs and context of the organization.
d) Segregation of responsibilities: AQAP 2110 assumes that responsibility for information security rests with the entire organization, not just a dedicated team or department. ISO 27001, on the other hand, requires that all persons in the organization be responsible for security and requires the appointment of a person responsible for the information security management system.
e) Regulatory requirements: AQAP 2110 requires organizations to comply with legal requirements and regulations related to information security in the defense sector, and ISO 27001 focuses on complying with general information security-related regulations that apply to all organizations.

In conclusion, AQAP 2110 and ISO 27001 have similar objectives, i.e., ensuring information security in an organization, but their approach and requirements vary depending on the sector in which the organization operates and the individual needs and context of the organization.

5. Different in risk and security management requirements in AQAP 2110 and ISO 27001 standards.

Integrating the requirements of AQAP 2110 and ISO 27001 can face some difficulties and challenges. Here are some of the most important difficulties:

a) Differences in scope of application: AQAP 2110 is a specific industry standard for the defense sector, while ISO 27001 is a general standard used in all sectors. This means that AQAP 2110 requires less specific and specific safety requirements, and some of these requirements may not have equivalents in ISO 27001. Therefore, integrating the

requirements of AQAP 2110 and ISO 27001 may require a thoughtful approach and alignment of requirements with the specific needs of the organization.

b) Differences in language and terminology: AQAP 2110 and ISO 27001 use different terms and language, which can introduce confusion and make it difficult to integrate requirements. In the case of requirements integration, it may be necessary to define and explain terms precisely and to provide clear definitions for key concepts.
c) Complicated certification procedure: Both AQAP 2110 and ISO 27001 require a certification procedure to confirm an organization's compliance with the requirements of the standards. These procedures are complex and time-consuming, which can be challenging for organizations looking to achieve certification against both standards.
d) Need to adapt to changing requirements: Both standards require organizations to constantly adapt to changing information security requirements. This means that organizations must monitor and update their security procedures and controls to meet the requirements of both standards.
e) Required management involvement: The integration of AQAP 2110 and ISO 27001 requirements requires the involvement of the organization's leadership to ensure that the organization is adequately prepared and has adequate resources to implement the requirements of both standards. Management must also be aware of the benefits of requirements integration and the difficulties and challenges that may arise.

6. Summary

The combined requirements of AQAP 2110 and ISO 27001 are used in organizations that are engaged in the production, supply, or operation of systems and services related to national defense and security. For example, companies that provide military equipment, IT services for military services, software providers or telecommunications services for government institutions dealing with security. The requirements of both standards are used together in such organizations to provide a comprehensive approach to information security management that takes into account the specific requirements related to the defense and national security sector, as well as the general requirements related to information security management. This allows organizations to better secure their systems and data, protecting them from threats such as cyberattacks and computer crime.

The integration of AQAP 2110 and ISO 27001 requirements has many benefits for organizations that use these standards, such as:

- Comprehensive approach to information security management: Requirements integration enables organizations to develop a comprehensive approach to information security management that takes into account both defense-specific requirements and general information security requirements.
- Improve security: Integration of requirements allows you to improve the security of your systems and data by identifying and assessing threats, managing risks, and applying appropriate security controls.
- Increase trust: The use of standards allows organizations to increase the trust of customers, business partners, and government institutions in their services and products by ensuring that their systems and data are adequately secured.
- Resource optimization: Implementing an integrated system allows you to optimize the use of resources such as time, people, and money by ensuring that security efforts are thoughtful, efficient, and effective.
- Compliance with legal requirements: The use of standards allows organizations to meet legal requirements related to information security and data protection, which in turn can minimize the risk of unpleasant legal and financial consequences.

The integration of AQAP 2110 with ISO 27001 allows for coordinated implementation and management of information security in all areas of the organization. ISO 27001 is an international standard for information security management that provides a general framework and requirements for identifying, managing, and minimizing information security risks.

The integration of these two standards allows for the establishment of consistent and coordinated procedures, policies and controls related to information security, both in the context of NATO and in the organisation in general. This enables the organization to more effectively manage information security risks, minimize risks, and ensure data confidentiality, integrity, and availability.

7. Notes in the main text

Standardization trend in quality management (Rogala, 2020).

Quality and Efficiency (Skrzypek, 2000).

AQAP 2110 SRD.1 Edition A, Version 1, 2016 Guidelines for the Transition Period and Implementation.

AQAP 2110 Edition D, Version 1, 2016 NATO Requirements for Quality Assurance in Design, Development and Manufacturing.

PN-ISO/IEC 27001:2022 Information security management systems. Requirements. Information security management systems. Requirements.

PN-EN ISO/IEC 27002:2023-01 Information security, cybersecurity and privacy protection – Securing information.

References

1. AQAP 2110 Edition D, Version 1 (2016). NATO Requirements for Quality Assurance in Design, Development and Manufacturing.
2. AQAP 2110 SRD.1 Edition A, Version 1 (2016). Guidelines for the Transition Period and Implementation.
3. Głowacka, M., Fertach, M. (2004). *Zarządzanie produkcją.* Poznań: Wyższa Szkoła Logistyki, p. 16.
4. Grajewski, P. (2003). *Koncepcja struktury organizacji procesowej*. Toruń: TNOiK, p. 48.
5. Kitler, W., Stepnowska, M., Nowak, D. (2017). *Prawo wojskowe*. Warszawa: Wolters Kluwer Polska, p. 51.
6. PN-EN ISO/IEC 27002:2023-01 Information security, cybersecurity and privacy protection – Securing information.
7. PN-ISO/ IEC 27001:2022 Information security management systems. Requirements. Information security management systems. Requirements.
8. Pszczółkowski, K. (2018). *Metodyka zarządzania ryzykiem w ochronie danych osobowych. Prawa własności.* Warszawa: Fundacja Bezpieczeństwa Informacji Polska (FBI Polska), p. 50.
9. Rogala, P. (2020). Research trends in quality management in years 2000-2019. *International Journal of Quality and Service Sciences, Vol. 12, No. 4*, p. 3.
10. Skrzypek, E. (2000). *Quality and Efficiency*. Lublin: Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, p. 14.