Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2021, 8(1):123-128

Research Article ISSN: 2394 - 658X

Examining ISO/IEC 27001 Standard

Mohammed Mustafa Khan

ABSTRACT

The demand for risk analysis and information security of systems by institutions that run an information system is rapidly increasing. The utilization of modern information technology in businesses mandates the introduction of different measures to protect the information and systems that house this information. One of the fundamental aspects that has been recommended to achieve information security is the international standard ISO/IEC 27001. ISO/IEC 27001 was jointly established by ISO (International Organization for Standardization) and IEC (International Electronical Commission). The ISO/IEC 27001 is an international and authoritative standard of information security management systems (ISMS) that has enabled the successful planning and implementation of ISMS. The framework was developed as the definitive worldwide best practice to protect vital intellectual property and information infrastructure. It has played a crucial role as the cornerstone on which other standards have leaned. This has provided worldwide best practices to be known across a conglomeration of digital services and processes in various industrial sectors. The ISO/IEC 27001 has become the key enabler for ensuring confidentiality, integrity and availability of information and information assets in today's increasingly digital world economy. This framework is regularly updated to maintain its stance as the definitive international best practice to reflect on the spike of digitization in organizations and the associated risks and to enhance the management of security controls. Organizations need to adopt this standard to reap the benefits of ISMS ahead of time. The standard will aid various institutions in strengthening information security practices and appropriately dealing with today's ever-evolving threat digital landscape.

Keywords: ISO/IEC 27001, information security, management system, asset.

INTRODUCTION

Over the years, information security was reserved for the technical audience only. However, as cyber threats have evolved and become more sophisticated, the importance of information security has expanded beyond IT departments, now involving business leaders, employees, and even consumers in ensuring the protection of sensitive data and systems. Information is stored in computers, servers, external hard drives, on paper, and even in the minds of those who work for the organization. It is important to preserve and secure this information throughout its entire lifecycle since it has become part and parcel of an organizational heritage [6]. The national and international laws and regulations, cyber threats, and organizational requirements are mounting a lot of pressure on organizations to secure their internal and external information and systems. The onus is on organizations to attain the security requirements and take the necessary steps to implement and satisfy their security objectives.

Arguably, there is no solid evidence that fully provides optimum security and protection of information assets. Nevertheless, there are existing security standards to foster the best practices in the management of information security. It is imperative for organizations to plan and prepare towards information security. The severity of security breach incidents is whooping, and intruders are utilizing sophisticated tactics and techniques to exploit security vulnerabilities [3]. Institutions that still use or implement convectional and outdated approaches in the management of information security are likely to fall victim to cyberattacks.

ISMS, as defined by ISO/IEC 27001, is a global standard that provides requirements to establish, implement, maintain and continuously improve an organization's information security best practices [10]. This standard is an integral component of organizational processes, controls, and information security. This standard can be deployed in any organization regardless of its type, nature, or size, and it consists of a certifiable standard. The ISO/IEC 27001 enables mapping to establish, implement, maintain and continuously enhance ISMS [3]. Organizations that yearn to preserve the confidentiality, integrity and availability of information and systems must strategically decide to adopt this standard. Implementing this international standard creates a conducive environment for an information

security management system. This research paper discusses the information security management systems, the development of ISO/IEC 27001, its structure, the major domains, the certification process and the benefits of ISO/IEC 27001.

UNDERSTANDING ISMS

An ISM constitutes what is referred to as the ISO/IEC 27001 standard. This framework is designed to ensure vital data and digital systems of an organization are preserved and remain protected from data breach incidents and unauthorized access [7]. An ISMS attains this by properly defining procedures, security policies, and controls crafted to secure data and keep it accessible by only specific individuals like IT and security teams. ISMS acts as a roadmap for organizations to secure their data and information systems. Additionally, ISMS encompasses strategies for ensuring employees are informed about the role they can play in enhancing the security posture of an organization. There are a number of factors that determine the establishment and implementation of ISMS that also impact the adoption of ISO/IEC 27001, as listed below;

- Organization's business objectives
- Security requirements
- Internal and external organizational processes
- The organization's size and structure

The continuous improvement process of ISMS utilizes the DEMING model known as PDCA (Plan, Do, Check, and Act) [8].

- **Plan.** The phase entails collecting information needed to discover security vulnerabilities and assess the risks. An organization's security policies and processes are defined based on this factor [8].
- **Do.** This is the preceding step after the plan. As the name suggests, it involves materializing previously developed policies and processes. It clearly states how these processes and policies are applied within an organization [8].
- **Check.** This is the third step, which entails monitoring and measuring the efficacy of the applied processes. The overall idea is to evaluate the processes to determine if they are working as intended.
- **Act.** This marks the last stage of the model. It involves enhancing the underlying processes [8]. The processes can be improved by modifying, eliminating or developing new ones that serve the aforementioned factors like security requirements and business objectives of the organization, just to mention a few.

DEVELOPMENT OF ISO/IEC 27001

The origin of ISO/IEC 27001 dates back to 1995 when the British Standard BS 7799 was initially published as a framework to manage information security focused on various security controls [3]. BS 7799 was crafted by the Department of Trade and Industry (DTI) in collaboration with leading British organizations, and it constituted two parts that are BS 7799 – 1, focused on the code of practice for information security management and BS 7799 -2, focused on specific requirements for ISMS [3]. BS 7799 became so effective in ensuring the safety of the information systems that it extended its adoption beyond the UK. In 2000, BS 7799 – 1 became ISO 17799, was renamed ISO/IEC 27002 in 2007, and in 2005, BS7799 – 2 evolved to ISO/IEC 27001, which was established as the international standard for ISMS. The objective was to establish an entire family of standards for information security. As the years go by, various elements have been added or merged to the ISO/IEC 27001 portfolio to cover technological advancements such as cloud computing, edge computing, the internet of things, and blockchain, among others and their associated risks. For instance, the ISO/IEC 27001:2013 is a set of controls in Annex A containing 114 controls organized into 14 categories, whereas the ISO/IEC 27001:2022, which is the latest version, has reduced the number of controls to 93 and grouped them into four themes including organizational, people, physical, and technological [1]. The core functionality of ISO/IEC 27001 to ensure confidentiality, integrity, and availability of data and information systems remains the same no matter the version of the standard developed.

After introducing the development of ISO/IEC 27001 and describing its evolution process, the structure is described briefly.

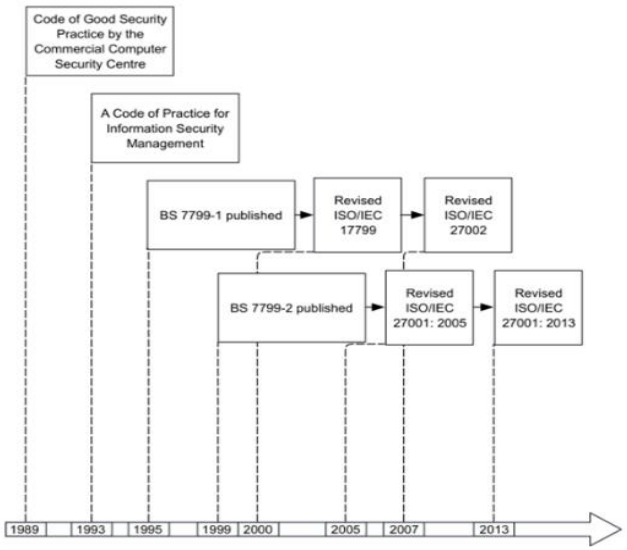

Figure 1: *Showing the Evolution of ISO/IEC 27001*

THE ISO/IEC 27001 STRUCTURE

This standard is divided into two main components. The first component is the definition of requirements, whereas the second component is Annex A security controls. The first component outlines the context of the organization, such as scope, normative references, definition of terms, leadership like policy, planning like risk assessment, and support like resources. Additionally, the first part outlines the operation, performance evaluation, and improvement [10]. In total, the first section consists of 10 clauses. The ten clauses are decomposed into subsections to help organizations clearly understand the context of each and how to tailor each subcomponent to address the ISMS. The second component constitutes Annex A, which involves controls and control domains. The controls grouped under each control objective are high-level and can be categorized based on themes like organizational, people, technological and physical.

Annex A outlines the list of controls that offer an ideal solution for defining basic countermeasures within an organization. Annex A is categorized into groups depending on their objective commonalities, starting from domain A.5, which involves information security policy, up to A.18, which entails compliance [9]. Some of the domains trickle down into subdomains to provide detailed information on the controls. There are different areas of implementation of the domains entailed in Annex A. The ISO/IEC 27001 has 14 domains that cover six major security areas. The next section will discuss the six major security areas for the implementation [12]. The ISO/IEC 27001 consists of the managerial and practical components of security requirements and controls. The managerial and practical components must be integrated to guarantee the practicability of information security policies and procedures to enhance the information security culture.

THE SIX MAJOR SECURITY AREAS OF ISO/IEC 27001

Company Security Policy

Information security has become a major component of organizational responsibilities. The board of management and executives must be involved to ensure comprehensive security governance is properly implemented and that each stakeholder is responsible for ensuring the security of the organizational data and assets. Additionally, the management is responsible for setting aside the budget needed for the acquisition and implementation of ISO/IEC 27001 standards. Company security policy provides a framework for setting objectives, assigning roles to every individual and ensuring continuous improvement of security measures. The company security policy deters employees from engaging in risky activities that endanger data and information systems. It is paramount to outline a security policy that properly aligns security practices with business goals [12].

Asset Management

Asset management involves identifying and classifying information assets, including tangible and intangible assets such as data, hardware, software, and personnel. It is important to maintain an accurate inventory of assets, comprehend their value, and implement protection measures accordingly. Proper asset management aids in the identification of risks, evaluating the consequences of possible risks and ensuring that sensitive information is protected appropriately. Asset management helps the security team to identify any rogue devices that have been

added to the company's network [12]. Additionally, asset management aids in the proper allocation of resources and in risk management strategies.

Physical and Environmental Security

This domain focuses on securing the physical infrastructure that supports information systems like servers, buildings and data centers. Enhancing security is essential to secure critical infrastructure. It is vital to establish solid perimeter security to prevent intruders from physically walking into the critical system, asset or facility. Physical security involves the construction of effective fences and access controls like biometric doors, installing CCTV surveillance at strategic points, and employing security personnel to physically guard critical infrastructure. The effectiveness of CCTV surveillance is that it monitors the environment and can generate an alarm for suspicious motions. Additionally, the footage may be used for future reference in the event of theft, vandalism or burglary. Data centers need environmental security, such as sensors and tools that measure humidity and temperature to provide the optimum conditions required for information systems to operate [12].

Access Control

Access control focuses on regulating access to specific information and systems in an organization. It provides privileges on how the information and systems must be accessed, thus limiting unauthorized access to data and systems. Access controls outline policies for authentication, authorization, and accountability, making sure that only those individuals who have been granted access can interact with data and systems [12]. Data breach incidents and misuse can be reduced or prevented by implementing role-based access controls and managing user privileges by leveraging the access control list. Moreover, access control acts as a formidable audit tool that monitors and keeps track of all logs that can be used for future reference in case of data breach incidents.

Incident Management

Incident management focuses on disaster recovery that ensures there is business continuity in case of disastrous events like ransomware or natural catastrophes like hurricanes. It outlines the procedures to detect, respond and recover from security incidents [12]. Incident management involves setting up an incident response plan, training employees, and escalating security incidents in a timely manner. The incident response plan may involve discovering vulnerabilities, coordinating with relevant teams, and how to enhance cyber resilience from past security incidents.

Regulatory Compliance

Any organization that operates in any country must abide by the federal laws and regulatory and contractual obligations associated with information security [12]. Regulatory compliance emphasizes understanding and conformance to relevant laws like data protection regulations, industry standards, and client agreements. Depending on the nature of the businesses that a company is engaging in, there are different specific regulatory standards that govern organizations. The E-commerce industry and businesses that deal with online payments must comply with the PCC–DSS standards to prevent credit card fraud [13]. Healthcare sectors must protect patient data by ensuring compliance with HIPAA [13]. Research industries need to observe the GDPR act that governs the collection and sharing of personal data among the European member states [5]. Compliance protects the organization from legal penalties and builds trust with stakeholders. Regulatory compliance involves proper documentation, regular audits, and the implementation of controls, among others, that align with the required standards.

ISO/IEC 27001 CERTIFICATION PROCESS

The accreditation of this standard is one of the ways to create assurance to clients and interested parties that ISO recommendations have been met. The frequency at which this certification is adopted is increasing annually [1]. For instance, 27536 certificates were issued globally in 2015, a 20% increase compared to the previous year [2]. The summary procedure for obtaining this standard certification is shown in Figure 2. New versions of the ISO/IEC 27001 certification process may come with a different process, so always check on the latest requirements to get the certification for your organization.

Different options for certification

• Organizations can declare compliance by themselves.
• Organizations can request clients to prove their compliance with the standard.
• An independent external auditor validates organizational conformity.

A list of Registered Certification Bodies (RCB) is introduced by the ISO for the purpose of certification procedures as mandated by certification organizations. The RCB aids organizations in evaluating the degree to conform with the standard, and further actions are needed for practical certification, such as examination. Later, the required measures for standard conformity are outlined in a preparation project. The RCB conducts a review of the presented documents, such as the security policy and process description [1]. The primary audit process entails steps such as interviewing all appropriate employees to inspect their comprehension of the security policy. Depending on the outcomes of the interviews, a report is generated by the certification organization indicating the audit results and areas to improve before performing the next audit.

If the overall findings are positive, the company gets an official certificate of ISMS compliance that aligns with ISO/IEC 27001 requirements. Time duration varies during the implementation stage. It may even take up to a year or years, depending on the maturity level of the IT security management within an organization. The validity of ISO/IEC 27001 certification is three years, and the recertification process consumes less effort than the initial one. In case some serious deviations have been discovered in an organization after certification, the RCB can reclaim or suspend the certificate [11].

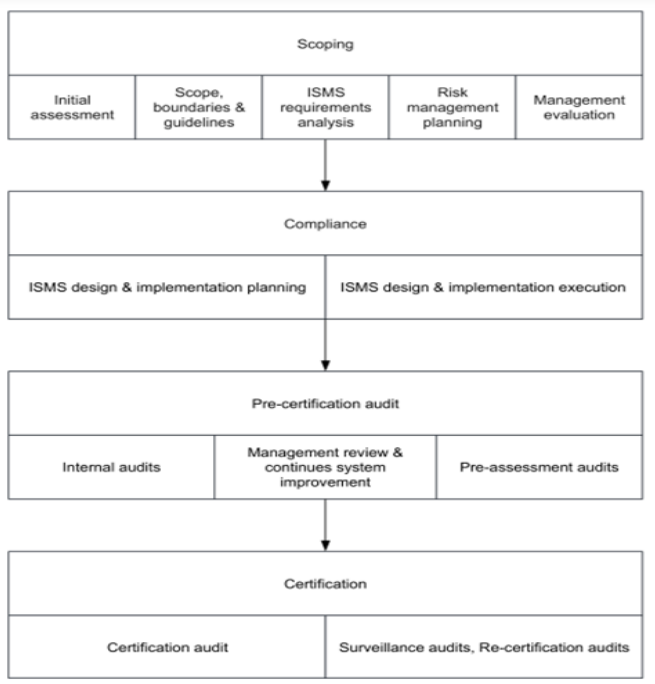

Figure 2: *Showing procedure for acquiring ISO/IEC 27001 certification*

BENEFITS OF ISO/IEC 27001

The ISO/IEC 27001 standards provide a holistic approach to managing risks that exposes the value of the information within an organization by developing, implementing and maintaining an ISM. Organizations that credit this certification show a commitment to accomplishing the information security management system [4]. Additionally, an organization accrues a lot of benefits, both internal and external, such as:

- Increases an organization's resilience to cyber-attacks.
- Reduces or eliminates data breach incidents.
- Enables an organization to meet contractual obligations.
- Enhances organization culture on information security.
- Organizations can respond to emerging security threats on time.
- Eliminates regulatory fines and penalties.
- Provides a competitive advantage since people looking to conduct businesses understand there is less risk of information security failures [4].

CONCLUSION

In conclusion, the ISO/IEC 27001 standard provides a comprehensive framework for managing information security and addressing the evolving cyber threats in today's digital landscape. It outlines essential policies and controls to protect organizational assets and ensure information and information systems' confidentiality, integrity, and availability. Implementing this standard strengthens an organization's defence against cyberattacks and helps ensure compliance with regulations, improving stakeholder confidence. The certification process offers a structured pathway to achieving compliance, positioning organizations to mitigate risks and secure competitive advantages in the marketplace.

REFERENCE:

[1]. B. Shojaie, "Implementation of Information Security Management Systems based on the ISO/IEC 27001 Standard in different cultures," Feb. 2018. Available: https://ediss.sub.uni-hamburg.de/bitstream/ediss/7572/1/Dissertation.pdf

[2]. B. Barafort, A.-L. Mesquida, and A. Mas, "Integrating risk management in IT settings from ISO standards and management systems perspectives," Computer Standards & Interfaces, vol. 54, pp. 176–185, Nov. 2017, doi: https://doi.org/10.1016/j.csi.2016.11.010.

[3]. Shojaie, Bahareh, H. Federrath, and I. Saberi, "Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016)," Google Books, Sep. 2016. https://books.google.com/books?hl=en&lr=&id=zRqqDAAAQBAJ&oi=fnd&pg=PA88&dq=advantages+of+ISO/IEC+27001&ots=lv-Q40AqQG&sig=6J1_fyCabBrJCN9QfuweMCzJ1lQ

[4]. Diamantopoulou, Vasiliki, A. Tsohou, and M. Karyda, "From ISO/IEC27001:2013 and ISO/IEC27002:2013 to GDPR compliance controls," Mar. 25, 2020. https://www.emerald.com/insight/content/doi/10.1108/ICS-01-2020-0004/full/html

[5]. Z. A. Soomro, M. H. Shah, and J. Ahmed, "Information security management needs more holistic approach: A literature review," International Journal of Information Management, vol. 36, no. 2, pp. 215–225, Apr. 2016, doi: https://doi.org/10.1016/j.ijinfomgt.2015.11.009.

[6]. D. Ganji, C. Kalloniatis, and H. Mouratidis, "Approaches to Develop and Implement ISO/IEC 27001 Standard - Information Security Management Systems: A Systematic Literature Review," Jun. 2019. https://www.researchgate.net/profile/Lea-Daling/publication/340886820_Media_Comparison_for_Instruction-based_AR_Usage_in_Collaborative_Assembly/links/5ea2b5d092851c87d1b105aa/Media-Comparison-for-Instruction-based-AR-Usage-in-Collaborative-Assembly.pdf#page=49

[7]. Majernik, Milan, et al, "Design of integrated management systems according to the revised ISO standards," Bibliotekanauki.pl, Jun. 2017. https://bibliotekanauki.pl/articles/405346.pdf

[8]. Hamdi, Zaidatulnajla, A. Anir Norman, F. Hassandoust, and N. Molok, "A comparative review of ISMS implementation based on ISO 27000 series in organizations of different business sectors," Dec. 2019. https://iopscience.iop.org/article/10.1088/1742-6596/1339/1/012103/meta

[9]. Gallotti and Cesare, "Information security: risk assessment, management systems, the ISO/IEC 27001 standard," Google Books, Jan. 2019. https://books.google.com/books?hl=en&lr=&id=40mFDwAAQBAJ&oi=fnd&pg=PR9&dq=ISO/IEC+27001+scope

[10]. C. Hsu, T. Wang, and A. Lu, "The Impact of ISO 27001 Certification on Firm Performance," 2016 49th Hawaii International Conference on System Sciences (HICSS), Jan. 2016, doi: https://doi.org/10.1109/hicss.2016.600.

[11]. EC-Council Global Services, "All About ISO 27001 Global Standard | ISO 27001 Advisory | EGS," EC-Council Global Services (EGS), Dec. 2020. https://egs.eccouncil.org/what-do-you-know-about-iso-27001/

[12]. M. Schertler and J. Bronfman, "US cybersecurity and privacy regulations," CRC Press eBooks, pp. 273–294, Oct. 2018, doi: https://doi.org/10.1201/b22142-14.