ISO 27001: Information Security Management Systems

Ta-Seen Junaid
Faculty of Computer Science and Engineering
Frankfurt University of Applied Sciences
Frankfurt am Main, Germany
taseen.junaid@gmail.com

***Abstract*—To implement an Information Security Management System, ISO 27001 offers a framework to assist enterprises of any size or any industry to protect their information in a methodical and affordable manner which is a part of a set of standards developed to handle information security: the ISO/IEC 27000 series. This article offers a thorough understanding of ISO 27001 in order to assist an organization to adhere to the standards and to earn the ISO 27001 certification. Moreover it provides detailed insight about the changes of the most up to date version of the ISO 27001 which is released in October 2022.**

***Index Terms*—ISO 27001, certificate, security standard, information security management systems**

I. Introduction

In this growing era of digital technologies and its increasing complexity, the management of information security is a critical and challenging task for an organization. Fortunately ISO 27001 [1] standards provides a structured, cost-effective and systematic way to establish, implement, operate, monitor, review, maintain and improve information security through the adoption of an Information Security Management System (ISMS). ISO 27001 is a member of ISO 27000 which has around 63 published standards [3] but only ISO 27001 provides an ISMS certificate. It is a complete framework for ISMS where other standards offer very prescriptive views about how you implement controls to manage information security but what those do not do is to provide you with how to actually implement a framework in place to then implement controls. ISO 27001 is a technologically agnostic and vendor independent framework for ISMS which is fittable for an organization of any size and any type and plugable to every sector of it. This paper provides a detailed insight about ISO 27001 so that an organization will successfully comply with the standards to achieve the ISO 27001 certificate.

II. ISO 27001

The full name of the most recent and most up to date version of ISO 27001 is "ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements". This is a well known international standard of information security management which was jointly published by two renowned organizations, International Organization for Standardization (ISO), in partnership with the International Electrotechnical Commission (IEC). By implementing and adopting the ISO 27001 standards, an organization can achieve a certificate which will be a valid proof that ISO recommendations have been followed.

Thanks to Prof. Dr. Matthias Wagner for his continuous support.

ISMS stands for Information Security Management System which helps an organization to maintain a secure and risk free infrastructure and business. It deals with processes, methods, procedures, policies and tools with specific organizational and technical measures which are continuously monitored with incremental improvement into a controlled environment. To achieve the ultimate security for critical systems, each environmental element like human resources, organization, software, hardware etc needs to be protected against risks and attacks [2].

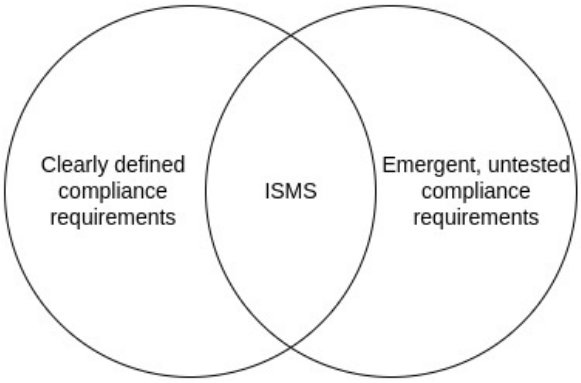

Fig. 1. ISMS coverage [4].

Software system as a whole has emergent properties which means a system may behave differently when it has been made from its individual functions and new characteristics may emerge at that time which may be a reason for an accident for a critical system. To develop a critical software, every code path must be controlled and tested which can be achievable with formal specification and verification. An ISMS not only deals with clearly defined requirements but also puts control on emergent properties likewise "Fig. 1" which will be very crucial for managing critical systems.

A. ISO 27000 Series

ISO 27000 series provides best practice recommendations on ISMS to achieve ISO 27001 certification. This series consists of around 90 standards where some standards have multiple parts and more than 60 of which have already been published [3]. Some of the most common and most useful standards are discussed in this section which will help us to achieve ISO 27001 certification. ISO 27000 provides an introduction and overview about the ISO 27000 family with clear definition and vocabulary. The most supporting standard for ISO 27001 is ISO 27002 which provides a detailed catalog about how to achieve different controls listed in ISO 27001 Annex A. ISO 27005 provides detailed guidelines about risk management, assessment and treatment like reduction, avoidance, transfer or acceptance and is a vital supporting standard as ISO 27001 is a risk centered standard. Cloud computing is gaining more popularity nowadays but it is not safe to store our sensitive data at cloud storage without encryption and without backup. But with the help of Hybrid cloud, it is also possible to manage the control of critical sections by asset owners with load balancing other sections by cloud services. ISO 27017 deals with information security in cloud environments where privacy protection is managed by ISO 27018. Now we are living in the era of internet and digitalization and there are several standards for online security like ISO 27032 deals with cybersecurity, ISO 27033 manages network security and ISO 27034 manages application security where ISO 27033 and ISO 27034 consist of several parts.

B. Security Objectives and Protection Goals

ISO 27001 ensures confidentiality, integrity and availability which are the main security objectives and protection goals of this standard. Confidentiality is intended to ensure that information is only accessible to authorized persons by implementing encryption and access control mechanisms. Integrity

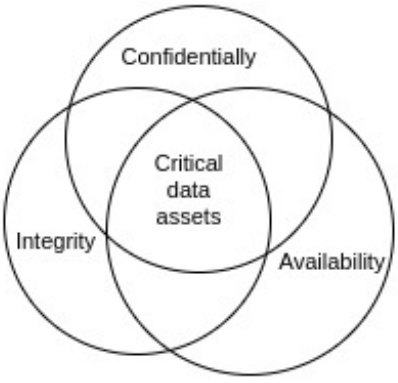

Fig. 2. Security objectives and protection Goals.

ensures that the data is only changed by authorized ways which protects the organization from attackers who try to change the information and also protects from unintentional technical errors. Availability ensures that information is available to the system or to authorized persons whenever it is needed. For critical assets, organizations need protections on all of the three security objectives like "Fig. 2" which will be achievable with the help of ISO 27001 [4].

C. ISO 27001 Structure

The latest version of ISO 27001 was released in October, 2022 which is divided into two parts. The main part contains 11 clauses and the subordinate part which is named as Annex A, contains guidelines of 93 security controls which will act as a safeguards. The 11 clauses numbered from 0 to 10 are introduction, scope, normative References, terms and definitions, context of the organization, leadership, planning, support, operation, performance evaluation, improvement where clauses 0 to 3 (introduction, scope, normative References, terms and definitions) contains introduction, scope, references, terms and definition. The remaining clauses (4 to 10) are mandatory requirements for ISO 27001 and if an organization needs an ISO 27001 certificate, it must fulfill and maintain all those mandatory requirements. Clause 4 is about understanding the context of the organization, organizational needs and expectations and to determine the scope of ISMS to manage it. Clause 5 is all about leadership and its commitment and policy by defining roles and responsibilities of each authority. Next clause is planning which will address the risk and opportunities by assessing the risk and implementing proper treatment. After that the support clause will give guidance about documentation process, communication awareness, resources, competence etc. Clause 8 is indicated as operation for operational planning and control of risk assessment and risk treatment. The next clause is performance evaluation for internal audit, reviews and monitoring the evaluation. An organization always needs improvement and corrective action to comply with the agile environment which is defined in the last clause known as improvement.

The ISO 27001 controls are the best practices guide which need to be implemented to reduce risks to the acceptable levels. The current version of the standard lists 93 controls into Annex A by organizing those into four themes numbered A.5 through A.8. The first theme A.5 deals with 37 organizational controls by defining the behaviors of people, software, hardware and systems. The second theme A.6 is people which has 8 controls so that people can comply with the security standards through proper knowledge, education, skills and experience. The third theme is physical (A.7) which has 14 controls to deal with hardware or devices that have a physical interaction with people and objects. The final theme is technological (A.8) with 34 controls which will be implemented with the help of software and hardware like antivirus software, data backup etc.

D. ISO 27001 Evolution

Due to the introduction of new technologies and increase in system complexity the ISO 27001 standard has evolved and matured through time. Currently the most recent version of ISO 27001 is ISO/IEC 27001:2022 which is released in October 2022 with a new title written as "ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection —

Information security management systems — Requirements" [1]. The first version of ISO 27001 (ISO/IEC 27001:2005) was published in October 2005, effectively replacing BS7799-2 as an audit standard for determining the maturity and effectiveness of Information Management Systems [8]. The current version is an improvement of the 2nd version (ISO/IEC 27001:2013) which was published in 2013. Different countries have their local version by translating the standard into their own languages, making minor changes that do not affect the content of the international version of the standard. For example BS ISO/IEC 27001 is the British version of the standard, which is distinguishable from the worldwide standard by the addition of additional letters at the beginning. These regional versions of the standard may also include the year and language like BS EN ISO/IEC 27001:2017, which indicates that the British Standards Institution approved ISO/IEC 27001:2013 in 2017.

In the most updating version mandatory clauses 4 to 10 have undergone a number of minor revisions, particularly in clauses 4, 6, 8, and 9 where new content has been imposed. In clause 4, not only the ISMS processes but also their interactions are needed to be identified which will give us a more formal and specific view of the system. It is a common mistake that changes are not documented properly which will create more problems when we need further changes on a changed system. From now on, all changes require documented planning and security objectives must be documented and available for all stakeholders which is the added item in clause 6. An attack on system security may violate safety and other crucial requirements and so the internal audits of clause 9 will assess not only ISO 27001 requirements but must cover all the organizational requirements.

Along with being organized into more useful groups, the controls have been streamlined and are now divided into 4 themes instead of 14 groups with 93 controls instead of 114. The changes are 35 controls have remained the same, 23 controls were renamed, 57 controls were merged into 24 controls, 1 control has been divided into 2 and 11 new controls were added. The newly added controls are for coping up with new trends and technologies. Nowadays we are dealing a lot with cyber space and new controls are needed to secure the overall organization. To protect our online activities we need web filtering, data leakage prevention. There are some web attacks like SQL injection, cross-site scripting which may not be caught with antivirus and firewall and so we need to follow secure coding. Due to the increasing complexity of modern systems, cloud computing is gaining more popularity. But it will not be a good idea to keep our critical data at cloud space without encryption and backup. Many organizations are currently following hybrid cloud approaches where they take the control of critical parts and deploy non critical parts into the cloud. So they added 11 new controls to comply with the current world and those controls are threat intelligence, information security for use of cloud services, ICT readiness for business continuity, physical security monitoring, information deletion, data masking, data leakage prevention, monitoring activities, web filtering, secure coding.

III. Plan, Do, Check, Act Cycle

The ISO 27001 standards can easily be implemented by following the Plan Do Check Act (PDCA) cycle which originated from quality assurance [5].The quality of the ISMS will improve as time passes through the incremental delivery by following the PDCA cycle. "Fig. 3" represents how we can implement ISO 27001 standard with PDCA cycle to increase the agility, clarity, and objectivity of management processes. Mandatory clauses 4, 5, 6 (context of the organization, leadership, planning) will come into the Plan phase with the establishment of the ISMS. The implementation of ISMS will need to be completed into the Do phase which covers mandatory clauses 7 and 8. Check phase will handle the monitoring and reviewing of the ISMS to fulfill the mandatory clause 9 (performance evaluation). The final part of the cycle is Act which deals with the maintenance and improvement of the ISMS by complying with clause 10 (improvement).

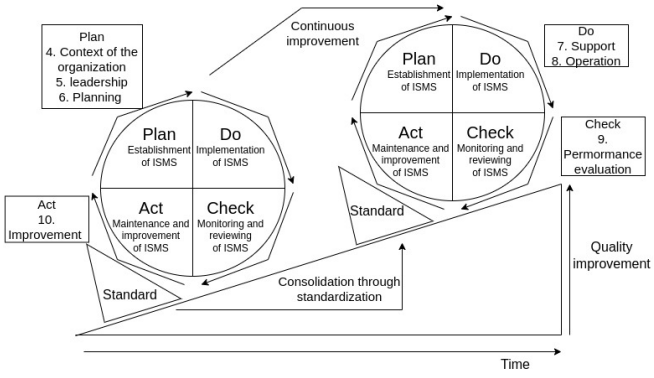

Fig. 3. PDCA cycle.

IV. ISO 27001 Certification Process

ISO 27001 certificate has huge economical and reputational benefits which not only reduce the economical and reputational damage caused by security attacks but also reassure clients, partners, customers, shareholders that protective actions have been taken to save the assets of the organization in the event of a security attack. The certificate will improve the overall structure of an organization, will help to avoid regulatory fines and will reduce the need for frequent audits.

Only authorized certification organizations can issue valid ISO 27001 certificates and ISO has a list of Registered Certification Bodies (RCB) from which an organization can achieve the certificate. "Fig. 4" [6] shows the process of achieving and holding an ISO 27001 certificate. First of all, an organization needs to define the scope of ISMS with initial assessment, scope, boundaries and guidelines, requirement analysis, risk management planning, management evaluation etc. The next part is the compliance phase where not only design and implementation planning is completed but also execution of those planning should comply with standards. Before achieving the certificate, the organization will go through a

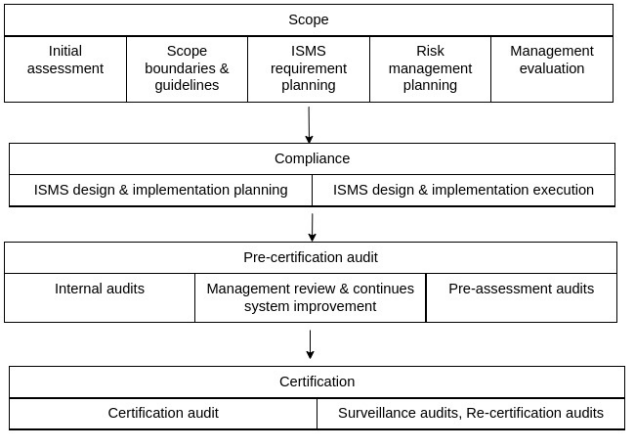

Fig. 4. Getting an ISO 27001 certificate [6].

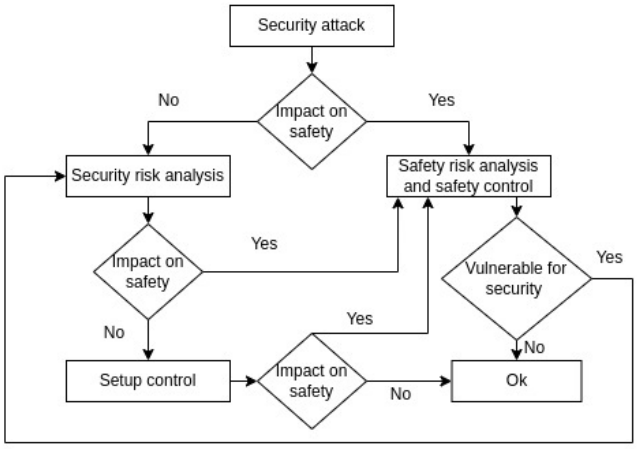

Fig. 5. Security risk management with safety.

pre-certification audit and assessment which will be helpful to know about which processes comply with standards and which processes need improvement to comply with standards. Finally the organization will receive an official certificate of ISO 27001 for ISMS which has a validity period for three years. After the expiration of the certificate, the organization can apply for recertification which will be achieved with less auditory process. The RCB will continuously monitor the organization and the RCB has the power to withdraw the certificate if they find any flaw in maintaining and managing the standards.

V. Security and Safety

Safety and security are coherent to each other, security breach will open the door for safety violation. The violation of safety due to security is very common, one recent example is the cyberattack on a critical water treatment plant in Oldsmar, Florida [7] [9]. In that attack, a hacker gained remote access to the computer system at the water treatment plant to poison the water. According to the investigation, the cyber actors most likely gained access to the system by taking advantage of cybersecurity flaws, including faulty password security and an out-of-date Windows 7 operating system, to breach the software used to remotely manage water treatment. The actor most likely achieved illegal access to the system by using the desktop sharing program TeamViewer. The plant's operator observed that the mouse was roaming around the screen to access various systems that regulate the water being treated. By changing sodium hydroxide levels from 100 parts per million to 11,100 parts per million, the hacker attempted to toxicate the supply. The attack was quickly stopped because the plant operator saw what was happening.

"Fig. 5" shows a proposed way to manage the safety and security [10] by integrating safety requirements with security threats. The idea is to verify the effect of each security control or measure on safety requirements before it is implemented, based on the analysis of the interferences between security and safety.

VI. Conclusion

It can be difficult for organizations to align with the security requirements with increasing complexity and emerging technologies. The ISO 27000 family of standards provide best practice recommendations and guidelines to implement an ISMS by analyzing risk and implementing secure guards with security controls. The normative standard of the aforementioned series, ISO 27001, offers an ISMS certificate in addition to the standard specifications for an ISMS. Moreover ISO 27001 is a technologically agnostic and vendor independent framework for ISMS which is fittable for an organization of any size and any type and plugable to every sector of it.

References

[1] "ISO/IEC 27001:2022," ISO, 25-Oct-2022. [Online]. Available: https://www.iso.org/standard/82875.html. [Accessed: 03-Jan-2023].
[2] T. Humphreys and A. Plate, Measuring the effectiveness of your ISMS implementations based on ISO/IEC 27001. London: BSi Business Information, 2006.
[3] "About the ISO27K standards - iso27001security.com." [Online]. Available: https://www.iso27001security.com/html/iso27000.html. [Accessed: 03-Jan-2023].
[4] A. Calder and J. van Bon, Implementing information security based on ISO 27001/ISO 27002: A management guide. 's-Hertogenbosch: Van Haren Publishing, 2017.
[5] C. Carvalho and E. Marques, "Adapting ISO 27001 to a public institution," 2019 14th Iberian Conference on Information Systems and Technologies (CISTI), 2019.
[6] B. Shojaie, "Implementation of information security management systems based on the ISOIEC 27001 standard in different cultures", Staats- und Universitätsbibliothek Hamburg Carl von Ossietzky, 2018.
[7] A. E. Montalbano and E. Montalbano, "Hacker tries to poison water supply of Florida town," Threatpost English Global threatpostcom. [Online]. Available: https://threatpost.com/hacker-tries-to-poison-water-supply-of-florida-town/163761/. [Accessed: 06-Jan-2023].
[8] L. Cook, "The evolution of ISO 27001," Cyjax, 22-Jul-2022. [Online]. Available: https://www.cyjax.com/2022/07/22/the-evolution-of-iso-27001/. [Accessed: 07-Jan-2023].
[9] ABC News. [Online]. Available: https://abcnews.go.com/US/outdated-computer-system-exploited-florida-water-treatment-plant/story?id=75805550. [Accessed: 07-Jan-2023].
[10] O. El Idrissi, A. Mezrioui, and A. Belmekki, "Interactions between cyber security and safety in the ICS context", Journal of Information Assurance Security, vol. 16, no. 2, 2021.