Comparative Analysis of ISO27001 and NIST CSF

Ahmed Alghamdi

Cyber Security Department, College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia. ahmedg@uj.edu.sa

Abstract: Recent developments in Information and Communication Technology (ICT) have had a significant impact on commercial organizations in achieving their goals and objectives. However, the introduction of ICT introduced new cyber risks and threats as well. To mitigate cyber threats, various cybersecurity frameworks and standards are available e.g., ISO/IEC27001 and NIST Cybersecurity Framework (CSF). These frameworks can be used to measure/ audit the maturity level of an organization's cybersecurity status. In this study, we have compared the ISO 27001 and NIST CSF and map these frameworks with each other.

Keywords: ISO 27001, NIST CSF

1. INTRODUCTION

Cyber-attacks are the real threat to organizations now a days [1]. Organizations spent a huge budget on protecting their IT infrastructure and critical data. Cyber security strategies and initiatives become an integral component of an organization's overall IT strategy. Different organizations have different security requirements; therefore, it is important to understand security needs and then implement the required controls to protect information systems. With the passage of time and changes in the IT infrastructure of the organization, the security needs are changing as well. Changes in IT infrastructure can introduce new risks which may lead to a successful cyberattack. Therefore, risk assessment is a continuous process [2] to identify risks and come up with appropriate countermeasures (controls) to mitigate the risks completely or up to acceptable level. Vulnerabilities exist in applications, hardware, operating systems, and network devices. Vulnerability assessment needs to be carried out regularly to protect systems from threat agent penetration.

Different cybersecurity standards and frameworks are available, which can be adopted by organizations to safeguard their information systems[3]. Cybersecurity standards are technical specifications and guidelines that aim to ensure confidentiality, integrity, and availability of information systems. Cybersecurity standards are categorized in two ways, i.e., information security standards and information security governance standards. The information security standards and frameworks focus on security controls such as ISO/IEC27000 series and NIST series frameworks. The selection of appropriate cybersecurity standards plays an important role in the protection of organizational information assets [4]. These frameworks have a comprehensive list of controls which can be used as benchmark to protect information systems. Organizations can choose cybersecurity framework depending on their requirements.

In this study, we have compared two well-known cybersecurity frameworks i.e., ISO/IEC27001 and NIST CSF. ISO/IEC 27001 is a standard developed by the International Organization for Standardization. It deals with having an Information Security Management System (ISMS) which means it's a lot of concerning the broader processes and principles of managing IT security than the measures. The key purpose of ISO 27001 is to introduce a scientific approach to maintaining security by creating an ISMS. The idea is that the ISMS can create commonplace follow across an organization to regulate and mitigate IT security risks, rather than hoping on a piecemeal approach. On the other hand, the US National Institute of Standards and Technology (NIST) Cybersecurity Framework is a voluntary, risk based cyber security standard. It was developed by thousands of participants from government, academia, and industry. The first release was in 2014 which provided for the purpose of improving critical infrastructure. The updated v1.1 release was in April 2018 which enhances and clarifies the cybersecurity framework based on comments from across all industry sectors.

Following introduction section, section II describes the structure of ISO/IEC27001 and NIST CSF. In Section III, we explain the similarities and differences between both frameworks and section IV concludes the paper.

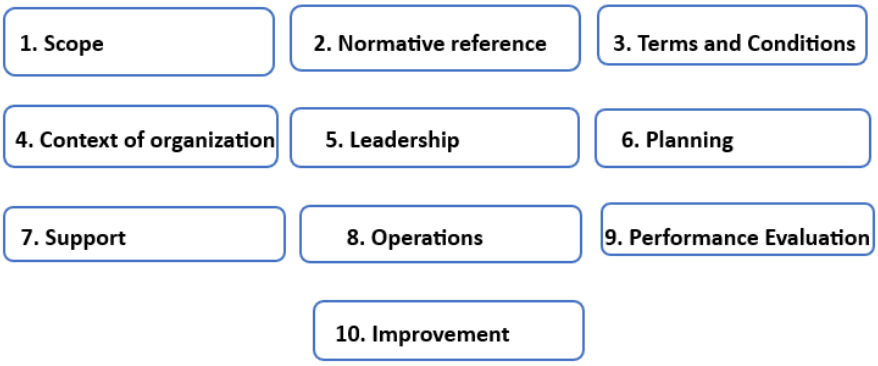

Fig. 1: ISO 27001 Clauses

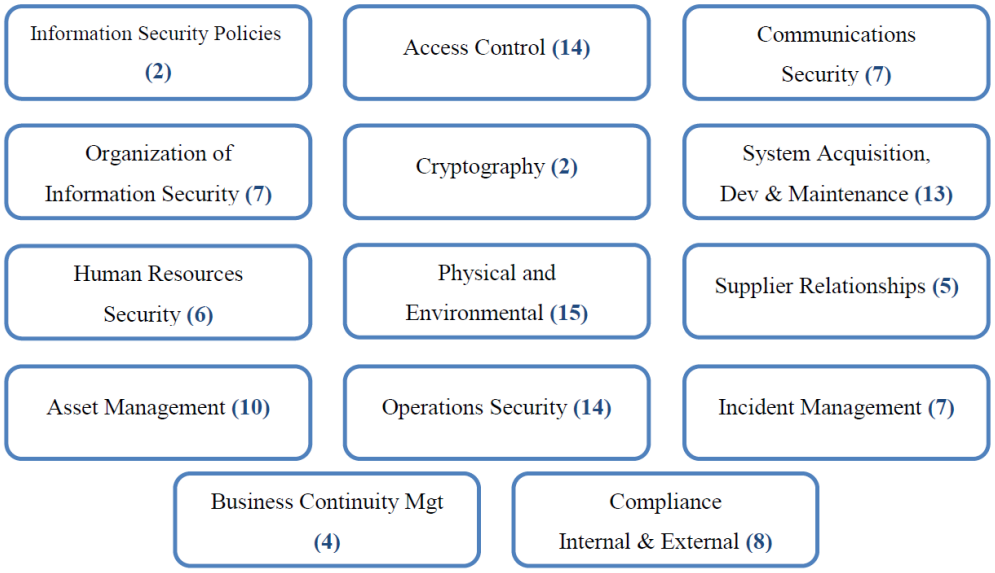

Figure 2: ISO27001 Security Domains

2. BACKGROUND

A. ISO/IEC 27001 Standard

The ISO/IEC27001 is an international standard developed by ISO in 2005. It belongs to the ISO 27000 family of standards. The ISO/IEC27001 standard provides specification for Information Security Management Systems (ISMS). According to the ISO/IEC 27001, ISMS is “a management system that carries out the establishment, operation, maintenance, monitor, and continuous improvement of information security” [5]. ISMS is a strategic decision for an organization which preserves confidentiality, integrity, and availability of information by applying a risk management process [6]. This will help the stakeholders by boosting their confidence that the level risk is appropriately managed. ISO 27001 standard has ten management clauses along with Annex A, which outline 114 security controls for supporting the implementation and maintenance of an ISMS. The ten clauses are given in Figure 1.

The second part of the ISO 27001 document is Annex A. It outlines 14 security controls that an organization should consider, these controls are divided across 14 security domains and 35 control objectives as summarized in Figure 2.

B. The ISO 27001 implementation Process

As a strategic decision, the objective of the ISO 27001 standard is to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an ISMS [7]. In addition, designing and implementing ISMS depends on the organization security requirements and objectives, the process employed and the organization size and structure. By applying the Plan-Do-Check-Act (PDCA) model (Figure 3) to structure the processes, the implementation of ISO 27001 is conducted [8].

C. NIST CSF

The US National Institute of Standards and Technology (NIST) Cybersecurity Framework is a voluntary, risk based cyber security standard [9]. It was developed by thousands of participants from government, academia, and industry. The first release was in 2014 which provided for the purpose of improving critical infrastructure. The updated v1.1 release was in April 2018 which enhances and clarifies the cybersecurity framework based on comments from across all industry sectors. (Evan, 2016).

The NIST framework uses five overarching functions to permit organizations to customize their cybersecurity measures to best meet their goals and distinctive challenges that they face in their environments. The functions are as follows:

1. Identify (ID): Developing an understanding and managing of organizations cybersecurity risks to systems, people, assets, data, and capabilities.
2. Protect (PR): Ensuring the delivery of critical services by developing and implementing appropriate safeguards.
3. Detect (DE): Identifying the occurrence of cybersecurity events by developing and implementing appropriate activities.
4. Respond (RS): Taking action regarding a detected cybersecurity incident by developing and implementing appropriate activities.
5. Recover (RC): Maintaining plans for resilience by developing and implementing appropriate activities.

The framework fundamentals give a detailed description of the major functions that an information security system employs in its' operations. These functions are shown in Figure 4.

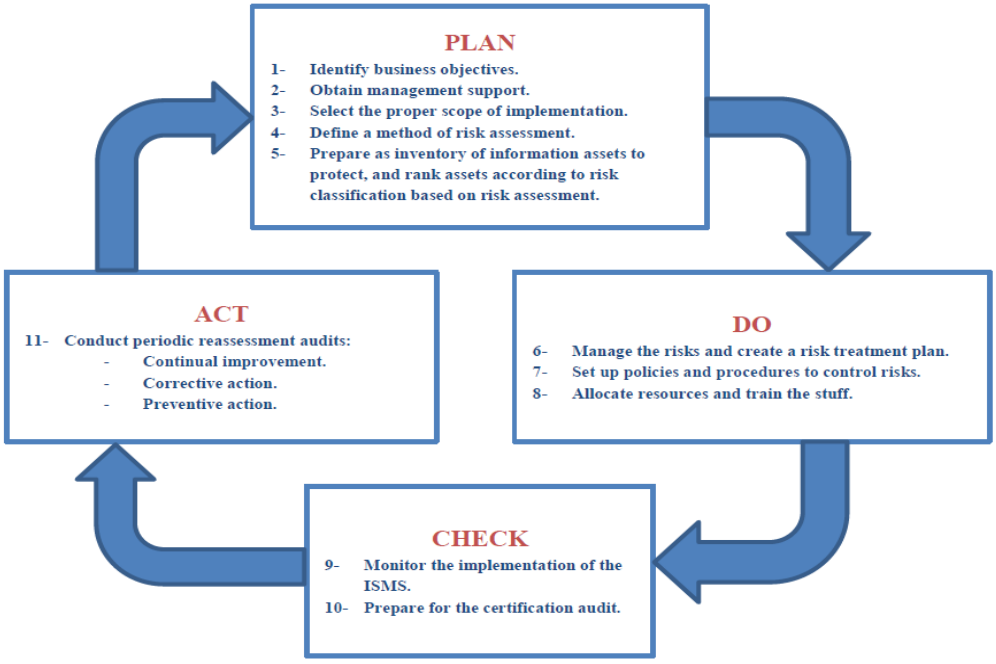

Fig. 3: PDCA Model

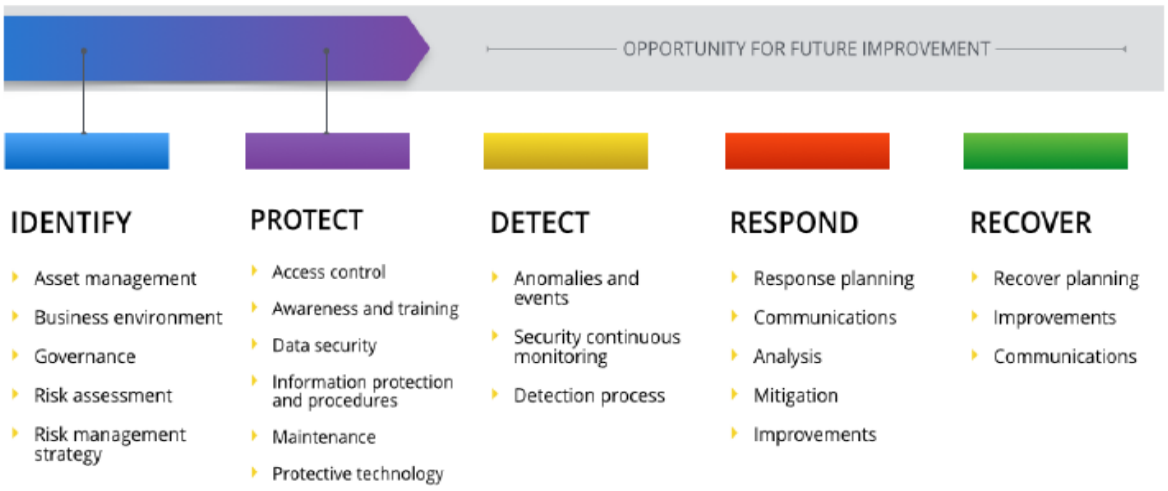

Fig. 4: NIST CSF Functions

NIST CSF control families are shown in Figure 5. Figure 6 is the illustrations of how organizations can use the framework to create a new cybersecurity program or improve the existing one if they already have. The steps are repeatable for improvement continuity.

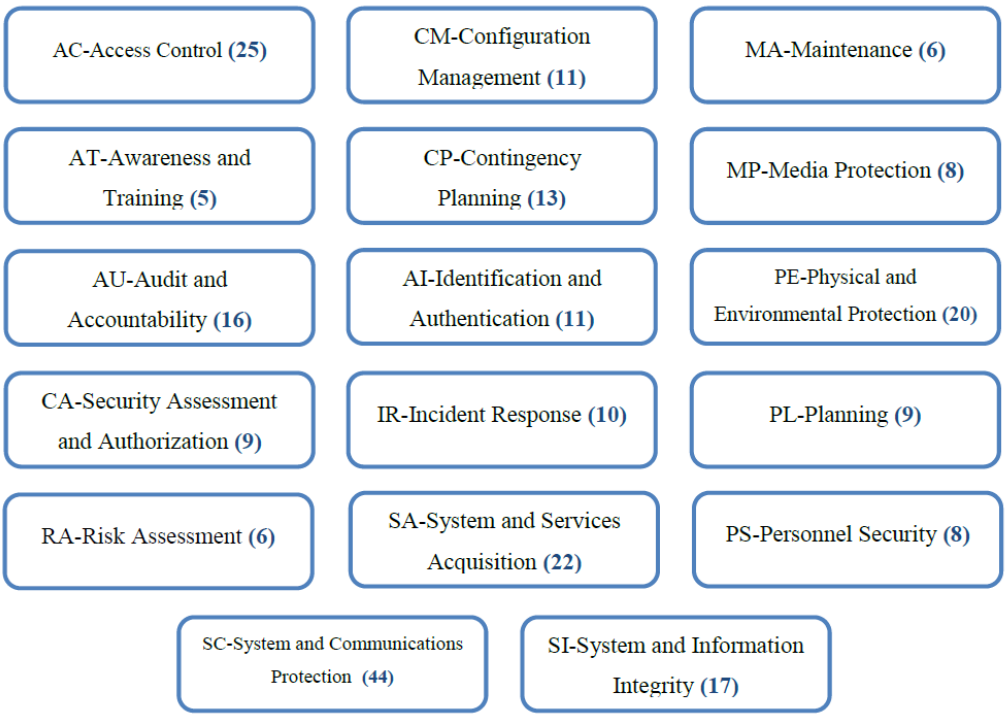

Figure 5: NIST CSF control families

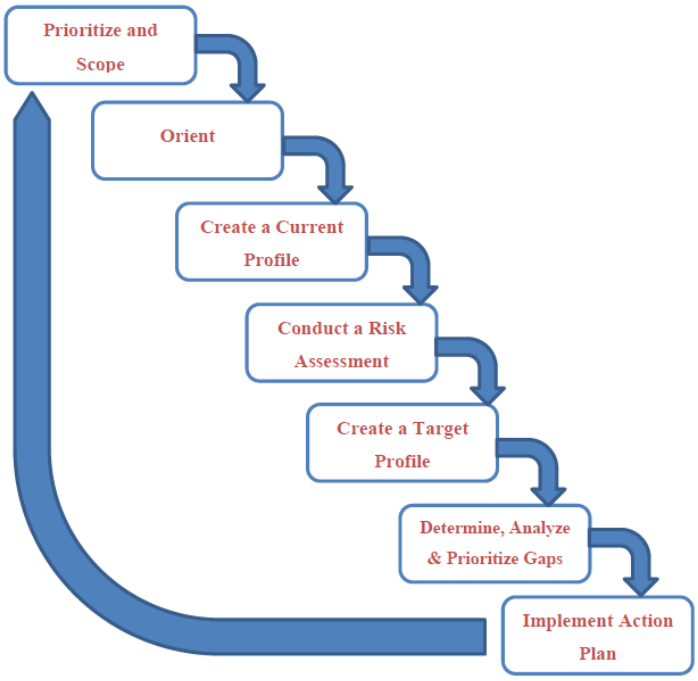

Fig. 6: NIST CSF implementation Steps

3. SIMILARITIES BETWEEN ISO27001 AND NIST CSF

NIST CSF and ISO 27001, both frameworks provide comprehensive techniques to deal with cyber threats and breaches [10]. Any of these frameworks, if implemented in its true spirit, will provide excellent security (CIA) and improve the overall status of the organization's security posture. ISO 27001 and NITS CSF, both are technology and platform independent frameworks, therefore these can be adopted by any organization wanting to improve their security posture.

However, ISO27001 standard is more suitable and adopted by commercial organizations because it has two rigorous documentations i.e., mandatory documents (risk assessment and treatment, access control policies etc.) and non-mandatory documents (change management policy, password policy and BYOD policies etc.), whereas NISTCSF is suitable and more adopted by technology-based organizations because of wide range of technical controls availability. The core of NIST CSF has five functionalities i.e., identify, Protect, Detect, Respond and Recover., NIST CSF consists of 22 categories i.e., Assets management, Data Security, Detection Process, Mitigation and Recovery Planning, which are similar to the controls given in ISO/IEC27001 Annex A. Further, NIST CSF has 98 subcategories, which were mapped to ISO/IEC27001 and COBIT frameworks.

Table 1. ISO27001 and NISTCSF comparison

	ISO 27001	NIST CSF
Number of Clauses	10	4
Number of Annex (Appendixes)	1	3
Number of Control Domains	14	23
Number of Controls	114	108

4. DIFFERENCE BETWEEN ISO 27001 AND NIST CSF

ISO/IEC27001 is a well-known and widely adopted framework around the world. If accurately implemented, organizations can become ISO27001 certified, which will convince their clients and partners that the organization can provide a risk-free transaction and all their security controls are properly implemented. While comparing ISO 27001

to NIST CSF, it was noticed that there are controls available in ISO27001 which do not match with controls in NIST CSF. Table 2 and Table 3, shows the ISO27001 clauses and controls are not covered in NIST CSF.

Table 2. ISO271001 Clauses

ISO 27001 Clause No	Clause
06.2	Information security objectives and planning to achieve them
07.1	Resources
07.2	Competence
07.5.1	General
07.5.2	Creating and updating
08.1	Operational planning and control
09.2	Internal audit
09.3	Management review
10.2	Continual improvement

Table 3. ISO271001 Controls

ISO 27001 Annex	Control
A.05.1.2	Review of the policies for information security
A.06.2.1	Mobile device policy
A.07.2.3	Disciplinary process
A.08.1.3	Acceptable use of assets
A.09.2.5	Review of user access rights
A.09.2.6	Removal or adjustment of access rights
A.10.1.1	Policy on the use of cryptographic controls
A.10.1.2	Key management
A.11.1.3	Securing offices, rooms and facilities
A.11.1.5	Working in secure areas
A.11.2.8	Unattended user equipment
A.12.1.1	Documented operating procedures
A.13.1.2	Security of network services
A.13.2.2	Agreements on information transfer
A.14.2.6	Secure development environment
A.14.2.9	System acceptance testing
A.14.3.1	Protection of test data
A.15.1.2	Addressing security within supplier agreements
A.16.1.3	Reporting information security weaknesses
A.18.2.1	Independent review of information security

NIST CSF is a structured and planned framework, which can it convenient for organizations to implement it at an enterprise level. Even senior management of an organization found it user friendly and easy to understand. The informative reference of NIST CSF makes it more understandable because a comprehensive mapping with other well-knows frameworks like COBIT, CIS etc. is given in NIST CSF document. A careful comparison of NIST CSF with ISO27001 shows that some of its controls are not covered in SIO27001. Table 4 shows NIST CSF controls are missing in ISO 27001.

Table 4. NIST CFS Controls

NIST CSF Controls ID	Control
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed.
DE.AE-3	Event data are aggregated and correlated from multiple sources and sensors.
DE.AE-5	Incident alert thresholds are established.
DE.CM-1	The network is monitored to detect potential cybersecurity events.
DE.CM-2	The physical environment is monitored to detect potential cybersecurity events.
DE.CM-7	Monitoring unauthorized personnel, connections, devices, and software is performed.
DE. DP-2	Detection activities comply with all applicable requirements.
ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated.
RC.CO-1	Public relations are managed.
RC.CO-2	Reputation after an event is repaired.
RC.CO-3	Recovery activities are communicated to internal stakeholders and executive and management teams.
RS.CO-5	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.

5. CONCLUSION

Both the NIST CSF and the ISO 27001 frameworks for cybersecurity risk management are highly effective. The NIST CSF framework and ISO 27001 standards are both simple to apply for any organization. With the help of these frameworks, organizations may more easily share information regarding cybersecurity concerns across departments and with external parties. It is also possible to merge the best practices of NIST CSF and ISO 27001, instead of using one framework.

6. REFERENCES

[1]. Chithaluru, P., R. Tanwar, and S. Kumar, Cyber-attacks and their impact on real life: what are real-life cyber-attacks, how do they affect real life and what should we do about them?, in Information security and optimization. 2020, Chapman and Hall/CRC. p. 61-77.
[2]. Khan, A., J. Bryans, and G. Sabaliauskaite. Framework for Calculating Residual Cybersecurity Risk of Threats to Road Vehicles in Alignment with ISO/SAE 21434. in Applied Cryptography and Network Security Workshops: ACNS 2022 Satellite Workshops, AIBlock, AIHWS, AIoTS, CIMSS, Cloud S&P, SCI, SecMT, SiMLA, Rome, Italy, June 20–23, 2022, Proceedings. 2022. Springer.
[3]. Taherdoost, H., Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. Electronics, 2022. 11(14): p. 2181.
[4]. Hijji, M. and G. Alam, Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. Sensors, 2022. 22(22): p. 8663.
[5]. 5. Kitsios, F., E. Chatzidimitriou, and M. Kamariotou, Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry. Sustainability, 2022. 14(3): p. 1269.
[6]. Ganji, D., et al., Approaches to develop and implement iso/iec 27001 standard-information security management systems: A systematic literature review. International Journal on Advances in Software, 2019. 12(3).
[7]. Fathurohman, A. and R.W. Witjaksono, Analysis and Design of Information Security Management System Based on ISO 27001: 2013 Using ANNEX Control (Case Study: District of Government of Bandung City). Bulletin of Computer Science and Electrical Engineering, 2020. 1(1): p. 1-11.
[8]. Singgrit, P. and G.C. Pamuji, The Use of ISO 27001 Framework for Government's Online E-Monitoring System Implementation. International Journal of Education, Information Technology, and Others, 2020. 3(3): p. 556-563.
[9]. Goodwin, S. The need for a financial sector legal standard to support the NIST Cybersecurity Framework. in SoutheastCon 2022. 2022. IEEE.
[10]. Alshar'e, M., CYBER SECURITY FRAMEWORK SELECTION: COMPARISION OF NIST AND ISO27001. Applied computing Journal, 2023: p. 245-255.

DOI: https://doi.org/10.15379/ijmst.v10i4.2258