Cybersecurity Frameworks and Information Security Standards

Subjects: Computer Science, Cybernetics

Contributor: Hamed Taherdoost

Businesses are reliant on data to survive in the competitive market, and data is constantly in danger of loss or theft. Loss of valuable data leads to negative consequences for both individuals and organizations. Cybersecurity is the process of protecting sensitive data from damage or theft. To successfully achieve the objectives of implementing cybersecurity at different levels, a range of procedures and standards should be followed. Cybersecurity standards determine the requirements that an organization should follow to achieve cybersecurity objectives and facilitate against cybercrimes. Cybersecurity standards demonstrate whether an information system can meet security requirements through a range of best practices and procedures. A range of standards has been established by various organizations to be employed in information systems of different sizes and types.

Keywords: cybersecurity framework ; cybersecurity standard ; information security framework ; information security standard ; cybersecurity requirements ; information security requirements

1. Introduction

A standard is described as an ideal condition with a minimum achievement limit [1]. It also refers to technical specifications that are required to be applied by a service facility to enable service users to acquire the maximum function, purpose, or profit from the services [2]. Many international organizations, associations, and consortia have a vital role in the development of standards [3][4]. According to www.standards.org.au (accessed on 1 February 2022), standards are represented as documents which define specifications, procedures, and guidelines, aiming to ensure safety, consistency, and reliability of products, services, and systems. Moreover, based on the provided definition by ISO/IEC, standards are documents or rules made based on a general agreement and validated by a legal entity, which help to achieve optimal results, as a guideline, model, or sample, in a particular context [5]. A standard practically meets user demands, considers the limitations of technology and resources, and also meets the verification requirements [2].

The most commonly used “standard” term refers to established documents by professional bodies to be used by other organizations (i.e., technical standards, program standards), or standards of technical practice (i.e., practical cybersecurity standards).

The sets of practices or technical methods that help organizations to secure their cyber environment are referred to as cybersecurity standards [6]. Cybersecurity standards include users, network infrastructure, software, hardware, processes, and information in system storage media that can be connected to the Internet network [6]. The scope of cybersecurity standards is broad in that it covers security features in applications and cryptographic algorithms that mainly provide perspective toward security controls, processes, procedures, guidelines, and baselines [7]. Security experts recommend implementing cybersecurity standards as a fundamentally essential element consisting of a collection of best practices to protect organizations from cybersecurity threats and risks [8].

The main aim of cybersecurity standards is to prevent or mitigate cyberattacks and reduce the risk of cyber threats [9]. The implementation of standards will provide benefits in saving time, decreasing costs, increasing profits, improving user awareness, minimizing risks, and offering business continuity [7]. Additionally, using standards facilitates the compliance of an organization to industry best practices and procedures and provides the opportunity to compare a security system on an international level [10]. Hence, applying cyber security standards has been established in different organizations or businesses to protect assets against cyber threats [11][12]. As a result, different cyber security standards have been developed by various organizations to ensure that organizations of different size and nature implement appropriate measures to prevent and mitigate cyber threats [13]. However, since a considerable number of standards have been developed to cover different aspects of cyber security in various organizations, it may be challenging for business owners to choose the appropriate standard that is the best match for their business [14].

2. Cybersecurity Standards and Frameworks

Cybersecurity standards are generally classified into two main categories, including information security standards and information security governance standards [15]. Information security standards and frameworks mainly concentrate on security concerns, such as the ISO 27000 series, ISF SOGP, NIST 800 series, SOX, and Risk IT. Selecting the most appropriate standard or framework is a serious decision that should be made based on the requirements of the organization to examine if it adequately suits the demands of the business. In some cases, employment of a single standard does not suffice to meet expectations of a business. Thus, managers need to examine whether they need to consider more than one standard [2].

Open standards and frameworks are easily available and optional to be employed. Thus, organizations can use some parts or all of the guidelines, as required, or use them in combination, integrated with other standards, to complement and strengthen other requirements [16]. Performance standards can be a policy or law to be complied with by certain countries. They may also be required by the responsible organization, association, or regulatory body to be complied with by the implementing organization [17]. A country or company is authorized to reject rules or standards published by others, or to develop their own proprietary standards or local regulatory standards [18].

The effective implementation of cybersecurity standards as guidelines or techniques which include best practices to be used in business or industry is not possible without the employment of the relevant cybersecurity framework [19][20]. Cybersecurity standards explain and provide methods one by one, specify what is expected to be done to complete the process, and clarify methods to coincide with the standard, whereas a cybersecurity framework is a general guideline that covers many components or domains that can be adopted by businesses/companies/institutions, which does not specify the steps that are required to be taken [21]. Satisfactory cybersecurity protection can be achieved by adopting a cybersecurity framework that describes the scope, implementation, and evaluation processes, and also provides a general structure and methodology for protecting critical digital assets [22]. In fact, organizations can refer to cybersecurity frameworks to realize guidelines in the successful implementation of cybersecurity standards to be better equipped to identify, detect, and respond to cyberattacks [23].

Cybersecurity frameworks are flexible and can provide users with the freedom to choose some parts or the whole model, methods, or technical practices, offering general and adoptable guidelines, as well as offering suggestions to be applied within the organization [24]. Implementation costs can be reduced as a result of the flexibility of cybersecurity frameworks. This can be effective to protect the infrastructure against cyber threats and secure critical sectors in the nation and economy. Therefore, cybersecurity frameworks (CSFs) have been developed by academic institutions, international organizations, countries, and corporations to ensure cyber resilience [25]. Businesses that seek to successfully implement cyber security standards are dependent on cybersecurity frameworks to harmonize policy, business, and technological approaches that are effective to mitigate cybersecurity issues and address cyber risks [26]. Thus, to ensure the protection of data and the infrastructure in organizations, businesses, and governments, cybersecurity standards and frameworks are required [27]. The difference between a standard and a framework is summarized in **Table 1**.

Table 1. Difference between a standard and a framework.

Standard	Framework
▪ Documents that determine procedures, specifications, and guidelines to ensure the safety, reliability, and consistency of services, products, and systems. ▪ Standards can be developed by a company or country into a proprietary standard or local regulation standard. ▪ Standards are guides to comply with the implementing organization in accordance with legal or regulatory provisions. ▪ Standards can be used together with other standards to complement and strengthen other requirements. ▪ Some standards are “open” to all types of businesses and government organizations; others are “closed,” which means they are specific to certain industries or businesses. ▪ A standard is what must be done to comply with the standard, by explaining and providing methods one by one in order to complete the process.	▪ Frameworks are general guidelines that cover a wide range of domains and components in organizations; however, the steps to follow are not specifically determined. ▪ A framework determines the basics to establish something or accomplish a goal. ▪ A framework is employed for determining the quality standards that should be achieved, describing the scope, defining evaluation and implementation, and summarizing the objectives and outcomes.

3. Cybersecurity Standards—Information Security Standards

Cybersecurity standards, as key parts of IT governance, are consulted to ensure that an organization is following its policies and strategy in cybersecurity [3]. Therefore, by relying on cybersecurity standards, an organization can turn its cybersecurity policies into measurable actions. Cybersecurity standards clarify functional and assurance steps that should be taken to achieve the objectives of the organization in terms of cybersecurity. It may seem costly for a business to invest in the implementation of cybersecurity standards; however, the confidence and trust that it brings are more beneficial for the organization [28].

Written cybersecurity standard documents describe requirements to be respected by the organization and are easy to be controlled by stakeholders or relevant auditors. However, standards do not include how to achieve the standard requirements. The most popular and frequently used cybersecurity standards, are shown in **Figure 1**. In a general classification, the ISO 27000 series, BSI, and SoGP are provided. Additionally, some standards that are common in industry are presented in the Industry Related category.

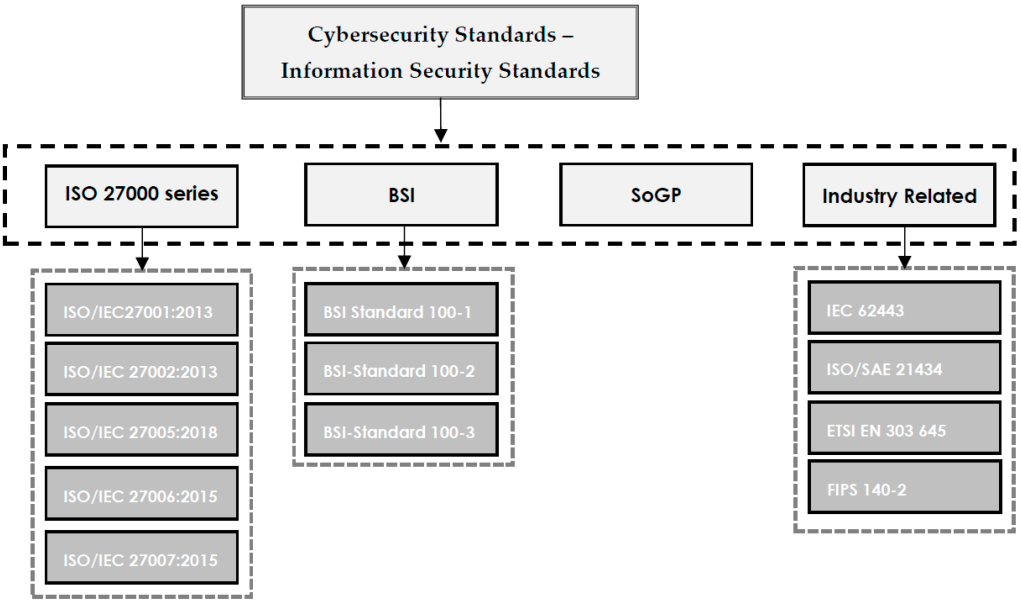

Figure 1. Cybersecurity standards—information security standards.

The evolution of cybersecurity standards over time is also represented in **Figure 2**.

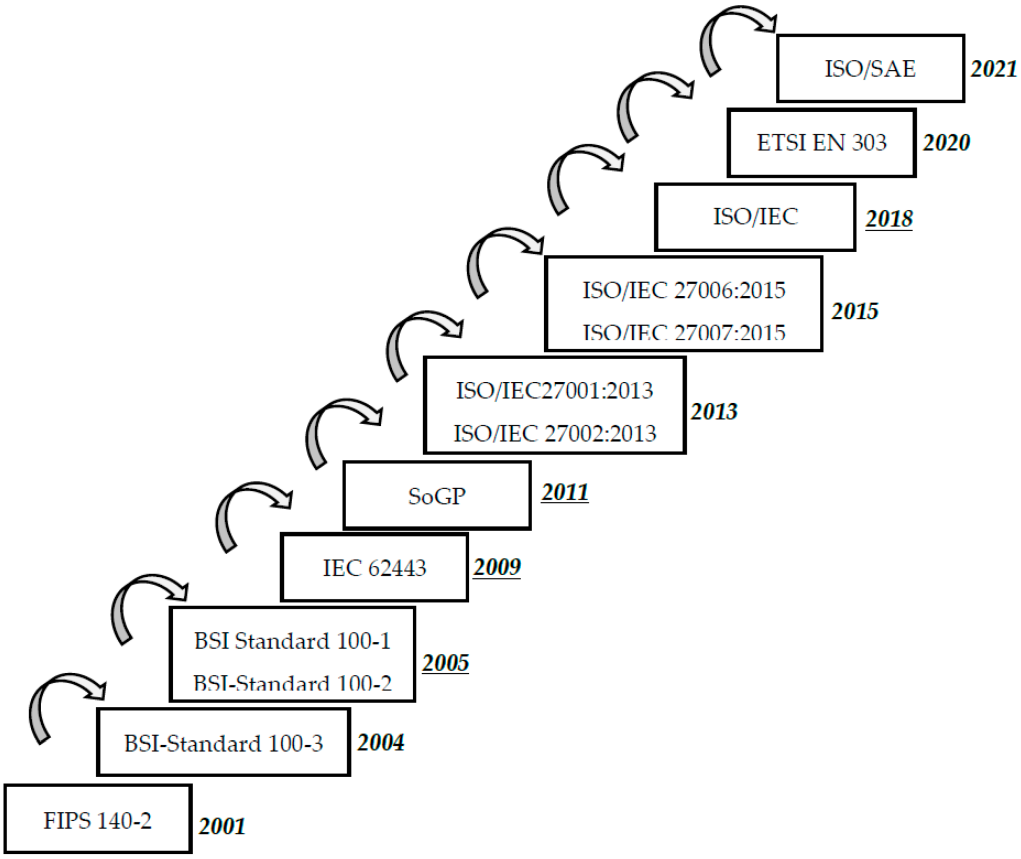

Figure 2. Timeline of cybersecurity standards evolution.

3.1. ISO/IEC 27000 Series

ISO/IEC 27000 concentrates on security in information systems management (ISM) and is published by the International Organization for Standardization (ISO) and the International Electro Technical Commission (IEC) [15]. The family of ISO/IEC 27000 standards was initially recognized as BS7799 and then introduced as ISO standards as soon as the ISO added it to the ISMS standards [29]. Methods and practices to ensure effective implementation of information security in an organization are described in detail in ISO 27001, focusing on providing a secure and trustable exchange of data and communication channels. The main consideration of ISO 27001 in accomplishing managerial and organizational objectives and sub objectives is through stressing risk approaches. However, the ISO 27000 series has not been shown to successfully work as a complete information systems management (ISM) solution to be integrated into larger systems.

ISO 27001, which is the first series of ISO/IEC 27000 standards, dates back to 2005. However, four standards, including 27001, 27002, 27005, and 27006, are currently published and widely used in organizations [30].

3.2. ISF Standard of Good Practice for Information Security

The standard of good practice (SoGP) was initially published in 1996 by the Information Security Forum (ISF), which is an international organization based in London, with staff in New York City. The Information Security Forum (ISF) is a non-profit and independent organization that concentrates on the development of best practices and benchmarking in the information security area [7]. Companies and individuals in manufacturing, financial services, transportation, chemical/pharmaceutical, retail, government, telecommunications, media, transportation, energy, and professional services from all over the world can join the ISF. The standard that includes best practices in cyber security is also revised every two years to cover the most recent best practices in information security. The standard is mainly designed to concentrate on six major aspects, including installing computers, application of critical business processes, managing security and networks, developing systems, and securing the environment for the end user [2].

3.3. BSI IT-Grundschutz

BSI IT is published by a German governmental agency called Bundesamt für Sicherheit in der Informationstechnik, which is abbreviated as BSI. BSI is responsible for managing the security of computers and communication for the German government, focusing on security of computer applications, cryptography, internet security, security products, and security test laboratories [10]. BSI has provided recommendations for approaches, processes, methods, and procedures that are related to cyber security. It also covers key areas in information security that are required to be considered while setting approaches for companies and public authorities [31].

3.4. Industry Related Standrads

Apart from the general classification of cybersecurity standards, a class of cybersecurity standards focusing on their application in business and technology, including IEC 62443, ISO/SAE 21434, and ETSI EN 303 645, is also provided here.

4. Cybersecurity Frameworks—Information Security Frameworks

The cybersecurity framework is the structure that an organization needs with respect to becoming protected against cyber-attacks. Some cybersecurity frameworks are mandatory and others are often strongly encouraged by regulators [25]. Thus, frameworks guide organizations in the implementation process to meet standard requirements. The main goal of a cybersecurity framework is to reduce the risk of cyber threats through learning from the best practices [3]. The most popular and frequently used cybersecurity frameworks are shown in **Figure 3**.

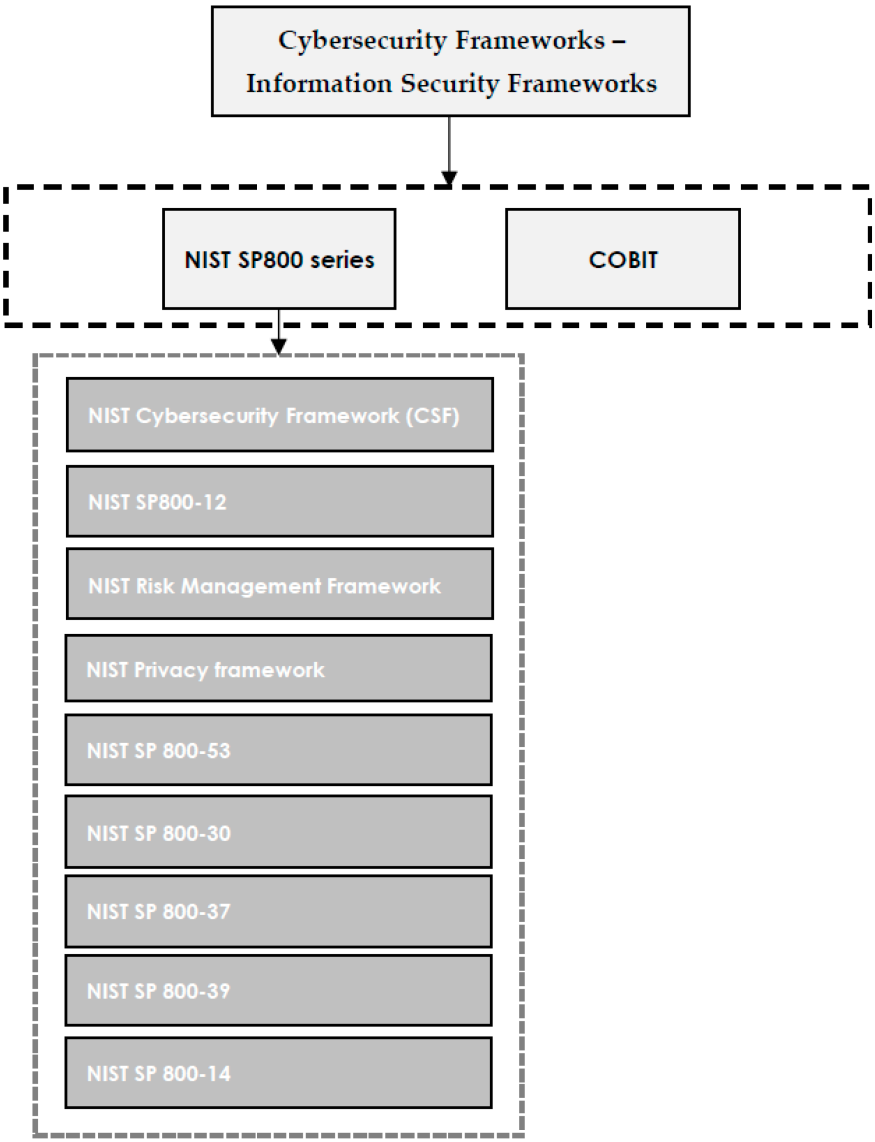

Figure 3. Cybersecurity frameworks—information security frameworks.

4.1. COBIT

As organizations have become more reliant on technology and communication, the likelihood of being threatened by cyber concerns from internal and external sources has been increased dramatically [7]. Hence, organizations need to follow a consistent approach to ensure that they appropriately identify risks and accurately assess and manage cybersecurity risks. This approach is essential for all organizations, regardless of their size, nature, and sophistication in cybersecurity. With this intent, COBIT was developed by the ISACA, Information Systems Audit and Control Association, which is an organization founded in 1967 in the USA in response to the growing concerns of computer systems. COBIT was initially released in 1996 to help users and decision makers in IT systems by developing and improving an authoritative series of information technology control objectives that are generally accepted. Therefore, they can realize the level of required security and control to protect the assets of their companies through the establishment of an information technology governance model [32].

In a general classification, COBIT is a high-level information technology standard in a governance and management framework that concentrates on broad concepts of decision-making processes in IT management, instead of focusing on details [15]. COBIT, which includes 34 main IT processes, encompasses the best practices and approaches regarding process, infrastructure, resource, responsibility, and control management. Each IT process in COBIT includes a series of high-level detailed control objectives recognized as DCOs, totally 318 DCOs, and a range of control objectives recognized as COs. control objectives, are classified into four main categories including planning, implementing, supporting, and monitoring and evaluating [33].

COBIT is the best choice to be implemented as an integrated solution because of its broadness. However, COBIT is not the best solution in cases where the appropriate implementation of security controls is the first priority, since it does not provide guidelines to achieve predefined control objectives [34].

4.2. The SP800 Standard Series

The SP800 standard series was developed by NIST, a non-regulatory federal agency established within the U.S. Department of Commerce. NIST was founded in 1901, and its mission is to improve life and economic security through the development of technology, science, and standards [10]. Industries that are supported by NIST standards and measurements include building and fire research, chemical science and technology, information technology, electronics and electrical engineering, materials science and engineering, technology services, manufacturing engineering, physics, neutron research, and nanoscale science and technology [35].

NIST published its group of 800 documents in 1990, which is considered the oldest publication in its information security standards, covering a wide range of documents that support different aspects of information security [7]. This series of standards includes recommendations, guidelines, technical features, and reports that NIST publishes annually about its cybersecurity activities. The SP 800 standard series was initially developed to address privacy and security requirements in federal information systems; however, it was later used by non-federal organizations as well. To employ the publication for national security systems, it is mandatory to get approval from the relevant federal authority [36]. The SP 800 standard series includes a range of different publications, such as the NIST risk management framework (RMF), NIST cybersecurity framework, the NIST SP 800-39, NIST SP 800-53, NIST privacy framework, and NIST SP 800-37, SP800-12, NIST SP 800-53R1, NIST SP 800-14, and NIST SP 800-30; however, SP800-12 is the most popular document in this series of standards, since it offers a good perspective of the NIST approach [10].

4.2.1. NIST Cybersecurity Framework (CSF)

The “cybersecurity framework” was established by NIST after the executive order was signed by President Obama in 2014. Furthermore, the role of the NIST was updated by the Cybersecurity Enhancement Act of 2014 (CEA) aiming to cover the identification and development of cybersecurity risk frameworks for critical infrastructure operators and owners. Existing business operations and cybersecurity concerns are covered in this framework. Thus, it can be referred to as a foundation for a new a mechanism or cybersecurity program to improve an existing program, which can be adopted as the best practices by organizations or private sectors to secure their own critical organization [37].

The NIST cyber security framework (CSF) helps organizations to increase their cybersecurity measures and provides an integrated organizing structure for different approaches in cybersecurity through collecting best practices, standards, and recommendations. In other words, a framework providing a means of expressing cybersecurity requirements can be effective to point out gaps in the cybersecurity practices of an organization.

4.2.2. NIST Risk Management Framework (RMF)

Every organization is required to follow a process with seven steps, including preparing, categorizing, selecting, implementing, assessing, authorizing, and monitoring in order to manage its privacy and information security risks [7]. This process is designed to be a comprehensive and measurable process that is repeatable at different times. This framework can be also employed in IoT-based environments to address growing privacy and security challenges.

4.2.3. NIST Privacy Framework

The NIST privacy framework [38] concentrates on addressing the concerns of organizations to detect and respond to concerns related to privacy and establish innovative services and products while considering individual privacy [7]. This framework is based on five major functions including identifying, governing, controlling, communicating, and protecting. This framework can also help managers to address privacy concerns in IoT-based environments.

4.2.4. NIST SP800-12

The core principles of cyber security are covered in detail in SP800-12 [10]. It was initially developed to be used in governmental and federal agencies; however, it can also be employed in other organizations focusing on computer security and controls [7]. The approach of the NIST is summarized in the SP800-12 series of standards clarifying the main elements, including the role of computer security in supporting the mission of the business, emphasizing the role of computer security in sound management, the importance of performing cost effective computer security, the importance of clearly defining accountability and responsibilities in computer security, emphasizing the role of system owners outside of the organization, emphasizing the employment of an integrated and comprehensive approach, the importance of assessing computer security on a regular basis, as well as the relationship between computer security and societal factors [7]. Thus, the handbook covers cost considerations, significant concepts, and the correlation between different security controls, eventually offering solutions to ensure that resources are secure [36].

4.2.5. NIST SP 800-53

This standard mainly concentrates on privacy and controls in information systems and organizations aiming to secure assets, individuals, and operations in organizations from different cyber threats, including human error, hostile attacks, failures in structure, natural disasters, privacy risks, and threats from foreign intelligence entities [7].

4.2.6. NIST SP 800-30

This standard mainly concentrates on providing guidance for the development of information systems risk assessment. Risk assessment plans are conducted using NIST SP 800-30 based on the recommendations and principles of the NIST standard. This standard facilitates the understanding of cyber risks for decision makers in the organization [36]. When decision makers realize the risks and issues mentioned by a technician, they can make smart decisions based on the available resources and budget [7].

4.2.7. NIST SP 800-37

This standard mainly concentrates on providing guidelines to apply a risk management framework in information systems and organizations. This standard presents guidelines for organizations to implement and manage privacy and security risks regarding the best practices in information systems. The responsibility to manage privacy and security based on this standard belongs to the top management team [7].

4.2.8. NIST SP 800-39

This standard mainly concentrates on guiding organizations to develop a program that is integrated with the aim of managing information security risks regarding the organizational mission, operations, reputation, functions, individuals, image, and organizational assets [36]. This structured and flexible approach specifically concentrates on assessing and monitor risks and responding accordingly. Moreover, this guide towards risk is not intended to take the place of other risk-related measures in organizations [7].

4.2.9. NIST SP 800-14

Commonly used security principles are described in NIST SP 800-14 to help users realize policies in cybersecurity. This standard equips organizations with requirements that they should follow to secure resources of information technology. Employment of NIST SP 800-14 ensures organizations of the readiness of their information technology security solutions in case of cyber threats [36].

References

1. Vaidya, R. Cyber Security Breaches Survey 2019-GOV. UK; Department for Digital, Culture, Media and Sport: London, UK, 2019.
2. Syafrizal, M.; Selamat, S.R.; Zakaria, N.A. Analysis of cybersecurity standard and framework components. Int. J. Com mun. Netw. Inf. Secur. 2020, 12, 417–432.
3. Baron, J.; Contreras, J.; Husovec, M.; Thumm, N. Making the Rules. The Governance of Standard Development Organ izations and their Policies on Intellectual Property Rights; Publications Office of the European Union: Luxembourg, 201 9.
4. Taherdoost, H.; Sahibuddin, S.; Jalaliyoon, N. Smart Card Security; Technology and Adoption. Int. J. Secur. 2011, 5, 74 –84.
5. ISO. ISO/IEC Directives; ISO/IEC: Washington, DC, USA, 2009.
6. Collier, Z.; DiMase, D.; Walters, S.; Tehranipoor, M.; Lambert, J. Cybersecurity Standards: Managing Risk and Creating Resilience. Computer 2014, 47, 70–76.
7. Karie, N.M.; Sahri, N.M.; Yang, W.; Valli, C.; Kebande, V.R. A Review of Security Standards and Frameworks for IoT-Ba sed Smart Environments. IEEE Access 2021, 9, 121975–121995.
8. Knapp, K.J.; Maurer, C.; Plachkinova, M. Maintaining a cybersecurity curriculum: Professional certifications as valuable guidance. J. Inf. Syst. Educ. 2017, 28, 101–114.
9. Purser, S. Standards for Cyber Security. In Best Practices in Computer Network Defense: Incident Detection and Resp onse; Hathaway, M.E., Ed.; IOS Press: Washington, DC, USA, 2014; pp. 97–106.
10. Tofan, D. Information Security Standards. J. Mob. Embed. Distrib. Syst. 2011, 3, 128–135.

11. Maleh, Y.; Sahid, A.; Alazab, M.; Belaissaoui, M. IT Governance and Information Security: Guides, Standards, and Fra meworks; CRC Press: Boca Raton, FL, USA, 2021.
12. Taherdoost, H. Understanding of E-service Security Dimensions and its effect on Quality and Intention to Use. Inf. Com put. Secur. 2017, 25, 535–559.
13. Kaur, J.; Ramkumar, K. The recent trends in cyber security: A review. J. King Saud Univ. Comput. Inf. Sci. 2021; in pres s.
14. Dong, S.; Cao, J.; Fan, Z. A Review on Cybersecurity in Smart Local Energy Systems: Requirements, Challenges, and Standards. arXiv preprint 2021, arXiv:2108.08089.
15. Arora, V. Comparing Different Information Security Standards: COBIT vs. ISO 27001; Carnegie Mellon University: Doh a, Qatar, 2010.
16. Krechmer, K. The Meaning of Open Standards. In Proceedings of the 38th Annual Hawaii International Conference on System Sciences, Big Island, HI, USA, 3–6 January 2005.
17. Heckman, J.J.; Heinrich, C.; Smith, J. The Performance of Performance Standards. J. Hum. Resour. 2002, 37, 778–81 1.
18. Bloor, M.; Sampson, H. Regulatory Enforcement of Labour Standards in An Outsourcing Globalized Industry: The Case of the Shipping Industry. Work Employ. Soc. 2009, 23, 711–726.
19. Dedeke, A.; Masterson, K. Contrasting cybersecurity implementation frameworks (CIF) from three countries. Inf. Comp ut. Secur. 2019, 27, 373–392.
20. Taherdoost, H.; Masrom, M. An Examination of Smart Card Technology Acceptance Using Adoption Model. In Proceedi ngs of the 31st International Conference Information Technology Interfaces, Cavtat, Croatia, 22–25 June 2009; IEEE: C avtat/Dubrovnik, Croatia, 2009; pp. 329–334.
21. Seeburn, K. Basic Foundational Concepts Student Book: Using COBIT® 5; ISACA: Schaumburg, IL, USA, 2014.
22. Antunes, M.; Maximiano, M.; Gomes, R.; Pinto, D. Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. J. Cybersecur. Priv. 2021, 1, 219–238.
23. Ozkan, B.Y.; van Lingen, S.; Spruit, M. The Cybersecurity Focus Area Maturity (CYSFAM) Model. J. Cybersecur. Priv. 2 021, 1, 119–139.
24. Donaldson, S.; Siegel, S.; Williams, C.; Aslam, A. Enterprise Cybersecurity: How to Build a Successful Cyberdefense P rogram against Advanced Threats; Apress: Berkeley, CA, USA, 2015.
25. Azmi, R.; Tibben, W.; Win, K. Review of cybersecurity frameworks: Context and shared concepts. J. Cyber Policy 2018, 3, 258–283.
26. Shackelford, S.; Russell, S.; Haut, J. Bottoms up: A comparison of voluntary cybersecurity frameworks. UC Davis Bus. Law J. 2015, 16, 217.
27. Srinivas, J.; Das, A.K.; Kumar, N. Government regulations in cyber security: Framework, standards and recommendatio ns. Future Gener. Comput. Syst. 2019, 92, 178–188.
28. Fumy, W. IT security standardisation. Netw. Secur. 2004, 2004, 6–11.
29. Koza, E. Semantic Analysis of ISO/IEC 27000 Standard Series and NIST Cybersecurity Framework to Outline Differenc es and Consistencies in the Context of Operational and Strategic Information Security. Med. Eng. Themes 2022, 2, 26–39.
30. Cordero, J.A.V. Les normes ISO/IEC com a mecanismes de responsabilitat proactiva en el Reglament General de Prot ecció de Dades. IDP Rev. Internet Derecho Y Política Rev. D'internet Dret I Política 2021, 33, 7.
31. Schmitz, C.; Schmid, M.; Harborth, D.; Pape, S. Maturity level assessments of information security controls: An empiric al analysis of practitioners assessment capabilities. Comput. Secur. 2021, 108, 102306.
32. Institute, I.G. Aligning COBIT, ITIL and ISO for Business Benefit: Management Summary. A Management Briefing from I TGI and OGC. IT Gov. Inst. 2005, 1, 5–62.
33. Amorim, A.C.; da Silva, M.M.; Pereira, R.; Gonçalves, M. Using agile methodologies for adopting COBIT. Inf. Syst. 202 1, 101, 101496.
34. Kozina, M. IT Risk Management in the enterprise using CobiT 5. In Proceedings of the Central European Conference o n Information and Intelligent Systems, Varazdin, Croatia, 13–15 October 2021; Faculty of Organization and Informatics Varazdin: Varaždin, Croatia, 2021; pp. 249–256.
35. Saarinen, M.-J.O. NIST SP 800-22 and GM/T 0005-2012 Tests: Clearly Obsolete, Possibly Harmful. Cryptol. Eprint Arc h. 2022, 169, 1–8.

36. Almuhammadi, S.; Alsaleh, M. Information security maturity model for NIST cyber security framework. Comput. Sci. Inf. Technol. 2017, 7, 51–62.
37. NIST. Framework for Improving Critical Infrastructure Cybersecurity. In Cybersecurity Framework; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2014; p. 41.
38. NIST. NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management; U.S. Departement of Commere National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020; p. 43.