electronics

MDPI

Review

Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview

Hamed Taherdoost

Department of Arts, Communications and Social Sciences, University Canada West, Vancouver, BC V6B 1V9, Canada; hamed.taherdoost@gmail.com or hamed@hamta.org; Tel.: +1-236-889-5359

Abstract: 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. However, it is challenging for businesses to adopt the standard that is the most appropriate based on their cybersecurity demands. Reviewing the experiences of other businesses in the industry helps organizations to adopt the most relevant cybersecurity standards and frameworks. This study presents a narrative review of the most frequently used cybersecurity standards and frameworks based on existing papers in the cybersecurity field and applications of these cybersecurity standards and frameworks in various fields to help organizations select the cybersecurity standard or framework that best fits their cybersecurity requirements.

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

Citation: Taherdoost, H. Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *Electronics* **2022**, *11*, 2181. https://doi.org/10.3390/electronics11142181

Academic Editor: Krzysztof Szczypiorski

Received: 8 June 2022
Accepted: 11 July 2022
Published: 12 July 2022

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].

This study aims to provide an overview of the most frequently used cyber security standards based on existing papers in the cyber security field, clarifying their features and applications in different industries. A wide range of cyber security standards and frameworks are available to ensure the protection of data in different industries; however, this review paper aims to provide a comparative concept regarding cyber security standards and frameworks and facilitate the selection of the most appropriate cyber security standards and frameworks. This paper can be also helpful for academic purposes to determine the direction of further studies in this field.

In the first section, an overview of the most common cyber security standards and frameworks is provided. Then, a narrative literature review that is the result of extracting and analyzing 17 papers published about cybersecurity standards between 2000 to 2022, considering the aim of each study, the main findings of the research, as well as relevant industry and employed standards is provided. Finally, a concluding discussion is presented that clarifies the contribution of different standards for specific purposes.

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, referred to in this paper, are shown in Figure 1. It is important to note that cybersecurity frameworks may not be limited to what is presented in the scope of this study, since new frameworks are constantly being published based on demands. 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.

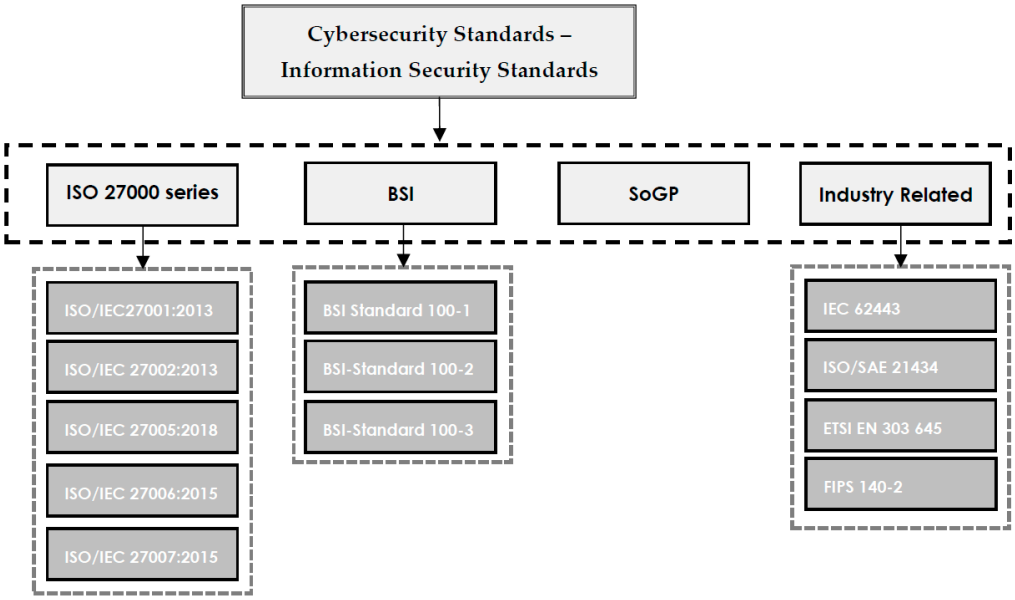

Figure 1. Cybersecurity standards—information security standards.

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

In the following, the most popular cybersecurity standards, including the ISO 27000 series, SoGP, and BSI, are described to provide an overview and facilitate the process of decision making.

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].

In the following, the most popular cybersecurity standards, including the ISO 27000 series, SoGP, and BSI, are described to provide an overview and facilitate the process of decision making.

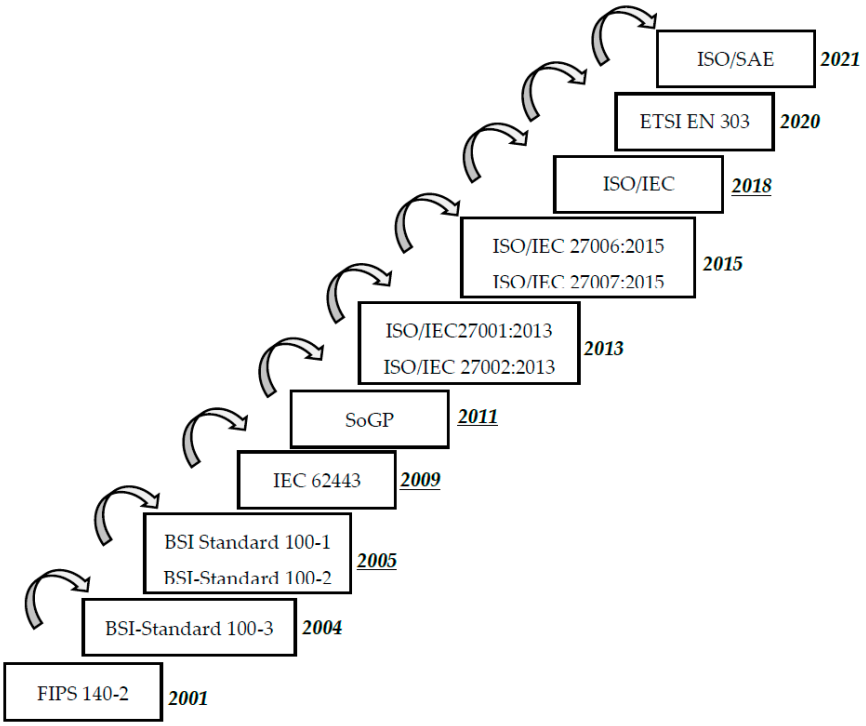

Figure 2. Timeline of cybersecurity standards evolution.

3.2. 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].

3.2.1. ISO/IEC27001:2013

ISO/IEC 27001 is an internationally recognized standard that determines requirements to implement a certified information security management system (ISMS) for a business through seven key elements [10]. These steps include specifications for installation, performance, operation, controlling and monitoring, review, maintenance, and improvement of the system. General requirements for the treatment and assessment of risks that exist in the information system of the organizations are also included, regardless of the size, type, and nature of the business. ISO/IEC 27001 is commonly used along with ISO/IEC 27002, which clarifies security control objectives and recommendations, since it does not list specific security controls. Employment of ISO/IEC 27001 helps organizations to manage and protect the valuable information of employees and clients, manage information risks, and protect and develop their brands [31].

3.2.2. ISO/IEC 27002:2013

ISO/IEC 27002 is the code of practice for information security controls that lists a structured series of information security controls to comply with ISO/IEC 27001. However, security controls that are not specifically mentioned in this list are not mandatory to be employed by organizations. Best practice recommendations to be used by responsible individuals when they try to implement information security management are provided in ISO/IEC 27002 [32]. This includes managing assets in an organization, securing human resources, managing operations and communications, securing environmental and physical aspects, managing business continuity, and managing compliance and information security incident areas [25].

3.2.3. ISO/IEC 27005:2018

Guidelines for risk-based implementation of cyber security risk management are provided in ISO/IEC 27005. ISO/IEC27005 supports concepts and requirements that are specifically listed in the ISO/IEC 27001. To completely understand ISO/IEC 27005, organizations need to gain knowledge about the processes and concepts of ISO/IEC 27001 and previously, ISO/IEC 27002. ISO/IEC 27005 can be applicable to implement a satisfactory risk-based information system in organizations of different sizes and sectors [33]. An information risk management process that consists of seven main elements, including installation of context, assessing risk, treating risk, accepting risk, communicating risk, consulting risk, as well as monitoring risk and reviewing risk, is employed in ISO/IEC 27005 [25].

3.2.4. ISO/IEC 27006:2015

The main purpose of ISO/IEC 27006 is to determine formal processes and requirements that should be respected by third-party bodies that provide information security auditing and certifying services for other organizations. The employment of ISO/IEC27006 helps bodies to be recognized as trustable and reliable organizations to operate ISMS certification in organizations [10].

Other standards put forth by ISO/IEC JTC 1 are ISO/IEC 27003:2017: information security management systems—guidance, ISO/IEC27000:2018: information security management systems—overview and vocabulary, ISO/IEC 27007:2017: guidance for information security management systems—auditing, ISO/IEC 27004:2016: information security management—monitoring, measurement, analysis, and evaluation, ISO/IEC 27013:2015: guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1, ISO/IEC TS 27008:2019: guidelines for the assessment of information security controls, ISO/IEC 27009:2016: sector specific application of ISO/IEC27001: requirements, ISO/IEC TR 27016:2014: information security management—organizational economics, ISO/IEC 27011:2016: code of practice for information security controls based on ISO/IEC 27002 for telecommuting organizations, ISO/IEC 27018:2019: code of practice for protection of personally identifiable information in public clouds, ISO/IEC 27010:2015: code of practice for information security controls based on ISO/IEC 27002 for cloud services, ISO/IEC 27017:2015: code of practice for information security controls based on ISO/IEC 27002 for cloud services, ISO/IEC 27019:2017: information security controls for the energy utility industry, and ISO/IEC 27014:2013: governance of information security [25].

3.3. 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].

3.4. 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 [34].

3.4.1. BSI Standard 100-1

The first standard in the BSI IT series is BSI Standard 100-1, which describes the main requirements that should be followed to implement ISMS. There is entire conformity between BSI Standard 100-1 and ISO Standard 27001. Moreover, recommendations and solutions of ISO standards are taken into consideration in this standard [10]. This standard mainly concentrates on managing the challenges of planning information technology process in the ISO 27001 standard.

3.4.2. BSI-Standard 100-2

BSI-Standard 100-2 includes the employment of IT security management in a practical step by step manner, covering suggestions for the selection of appropriate measures in information technology security, concepts to implement information technology security, and information technology security concepts. Additionally, general requirements to employ ISO 27001, 27002 and 13335 standards are interpreted using notes and examples that will facilitate establishment of a successful ISM [34].

3.4.3. BSI-Standard 100-3

This series of BSI standards concentrates on risk analysis. Organizations apply this approach to promote their risk analysis while they implement the IT-Grundschutz manual. This risk analysis is conducted based on the principles of the IT-Grundschutz [34].

3.5. 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 in this study.

3.5.1. IEC 62443

IEC 62443 is an international series of standards in cybersecurity that is focused on the employment of cybersecurity requirements for operating technology in systems used for industrial automation and control purposes [35]. This series of standards that was initially established by the ISA99 committee addresses current and future cyber security concerns in industrial automation and control systems (IACSs). The International Electrotechnical Commission (IEC) has adopted this standard and asks security experts in industrial automation and control systems from all over the world to help develop the standard [35]. Since the standard has divided cybersecurity topics into different categories, it is not limited to the technology sector; however, it also considers mitigating cyber threats regarding processes, employees, and countermeasures.

3.5.2. ISO/SAE 21434

This standard is focused on cybersecurity risk management requirements in the engineering of electronic systems of road vehicles and includes production, operation, development, maintenance, etc. concepts in engineering [36]. It also includes both components and interfaces of road vehicles. The main aim of this standard is to ensure that cybersecurity concerns are addressed in the engineering of road vehicles and that they are protected against different cyber-attacks [36].

3.5.3. ETSI EN 303 645

Cybersecurity is becoming a growing challenge, as more devices are connected to the Internet and more people are sharing their personal data using the Internet of Things. This standard targets all parties that are involved in manufacturing and developing products and appliances that work based on the Internet of Things technology [37]. The standard has collected a wide range of best practices and requirements in internet-connected products and appliances to ensure the security of consumers' data. The main focus of this standard is on the establishment of organizational policies and technical controls that are applicable to all IoT devices [37].

3.5.4. FIPS 140-2

Federal Information Processing Standards (FIPS) were initially published by the National Institute of Standards and Technology (NIST). This standard includes hardware and software requirements to protect cryptography modules. Cryptography modules include valuable information that should be secured with respect to integrity and confidentiality concerns. Four security levels, from the lowest to the highest, are defined in FIPS 140-2. This standard is established based on the joint collaboration of the Canadian government Communications Security Establishment (CSE) and National Institute of Standards and Technology (NIST) to ensure that cryptographic modules meet requirements of NIST. Therefore, if a product meets FIPS 140-2 requirements, it is accepted by federal agencies of United States and Canada at the same time [38].

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 that are referred to in this paper are shown in Figure 3. It is important to note that cybersecurity frameworks may not be limited to what is presented in the scope of this study, since new frameworks are constantly being published based on demands.

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 con-

trol to protect the assets of their companies through the establishment of an information technology governance model [39].

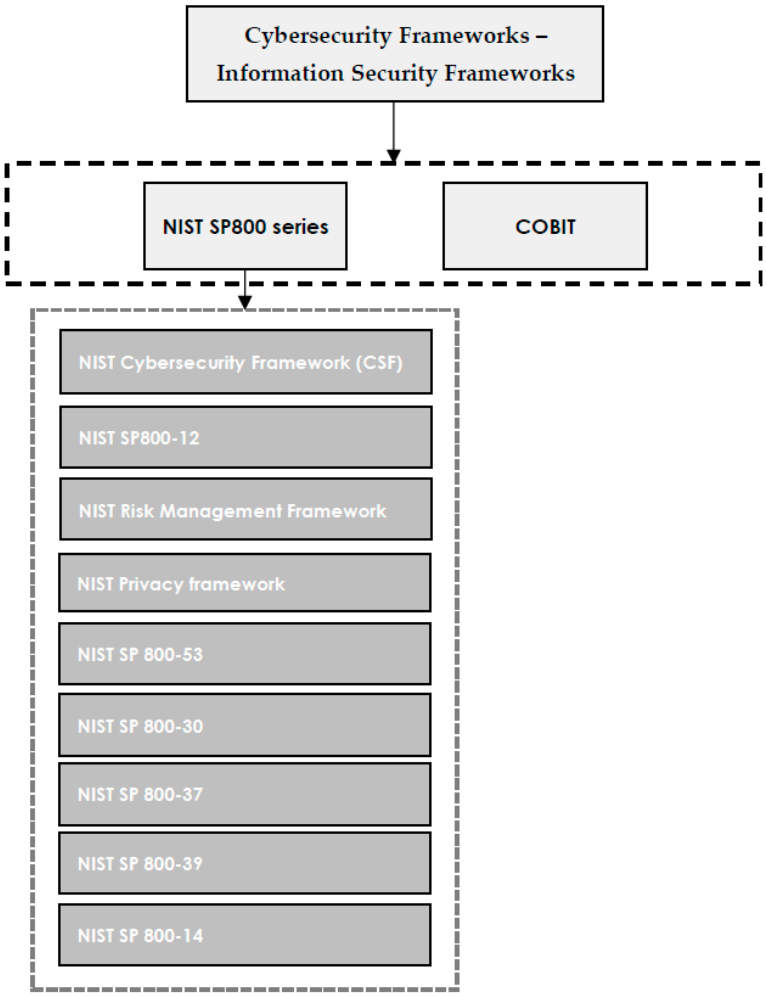

Figure 3. Cybersecurity frameworks—information security frameworks.

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 [40].

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 [41].

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 [42].

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 [43]. 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 [44].

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 [45] 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 [43].

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 [43]. 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 [43]. 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 [43].

5. Research Methodology

In this section, the employed process to conduct a literature review in this study is described in details. The objective of the narrative literature review is to respond to the research questions, including how information security standards are being used in different fields and the current condition of the most frequently used information security standards.

The screening for paper selection was conducted in a process that includes several steps. In the first step, a collection of papers based on the literature relevant to information security standards was extracted from the Science Direct database using the “information

security standards", "cyber security standards", and "cybersecurity standards" as keywords in several steps. Limiting the search to the English language and studies that were published from 2000 to 2022 indicated that 253.187 papers were published on information security standards, 15710 papers were published about cyber security standards, and 5054 were found using the cybersecurity standards keyword.

To analyze the literature review in more depth and limit the number of articles, the query of title, abstract, or author-specified keywords was applied to manually re-screen the search results. The results indicated that there were 1.136 publications on information security standards, 203 publications on cyber security standards, and 99 publications using the cybersecurity standards keyword. In the next step, the search result was limited to considering review articles and research articles. Therefore, book chapters, book reviews, discussions, editorials, mini reviews, news reports, short communications, and others were excluded from the search to narrow the search. As a result, 857 publications were found using the information security standards keyword, 164 results were found using the cyber security standards keyword, and 84 results were found using the cybersecurity standards keyword.

The titles, keywords, and abstracts of all extracted papers were scanned and analyzed in terms of relevance to the topic of the research and response to research questions based on their main focus area. Therefore, studies with no focus on the research topic were excluded from the review. If the title or abstract of a study revealed relevance to the domain of this study, it was included for further examination; otherwise, it was eliminated. Then, extracted papers were narrowed to 43 studies based on the title, abstract, and keywords. In the next step, duplicate papers were found and eliminated from the final list. In cases where the abstract of the study was unclear, the study was carried into the next stage to examine the full content of the study. Through this detailed refining process, 17 studies that met all the criteria were retrieved. Therefore, the papers that met the criteria to be used as the basis of this narrative literature review are presented below. Figure 4 shows the decision process of selecting the final papers for a narrative literature review.

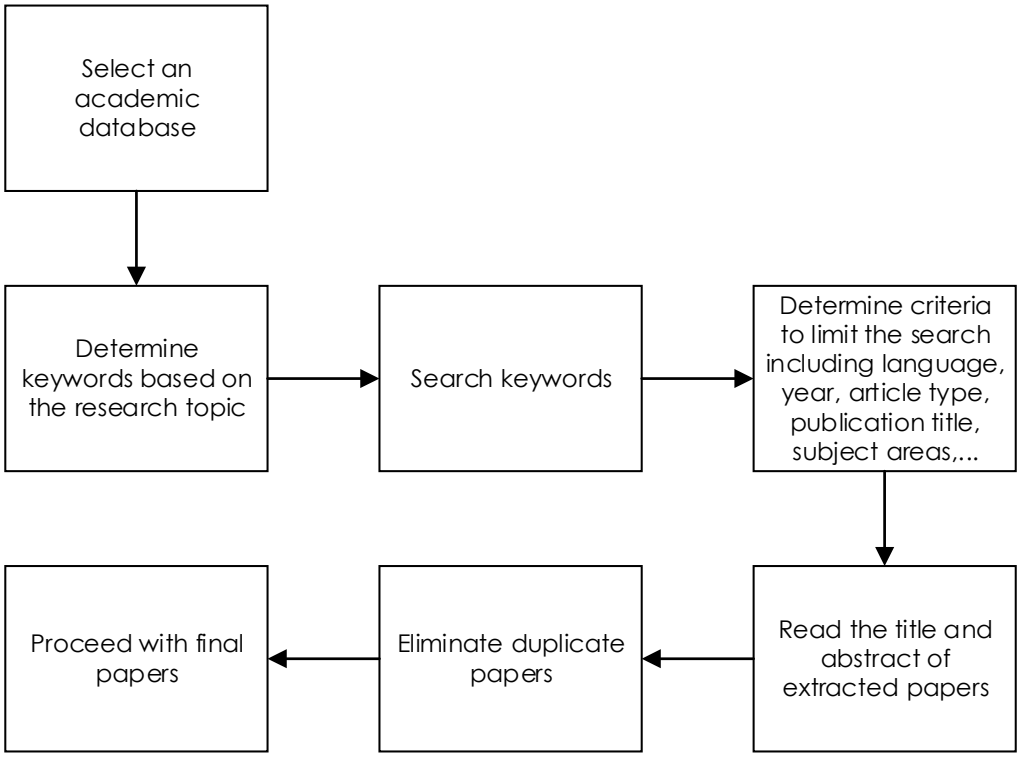

Figure 4. Flowchart of selecting papers in a narrative literature review.

Figure 5 shows the details of the process to select the final papers that were reviewed in this study.

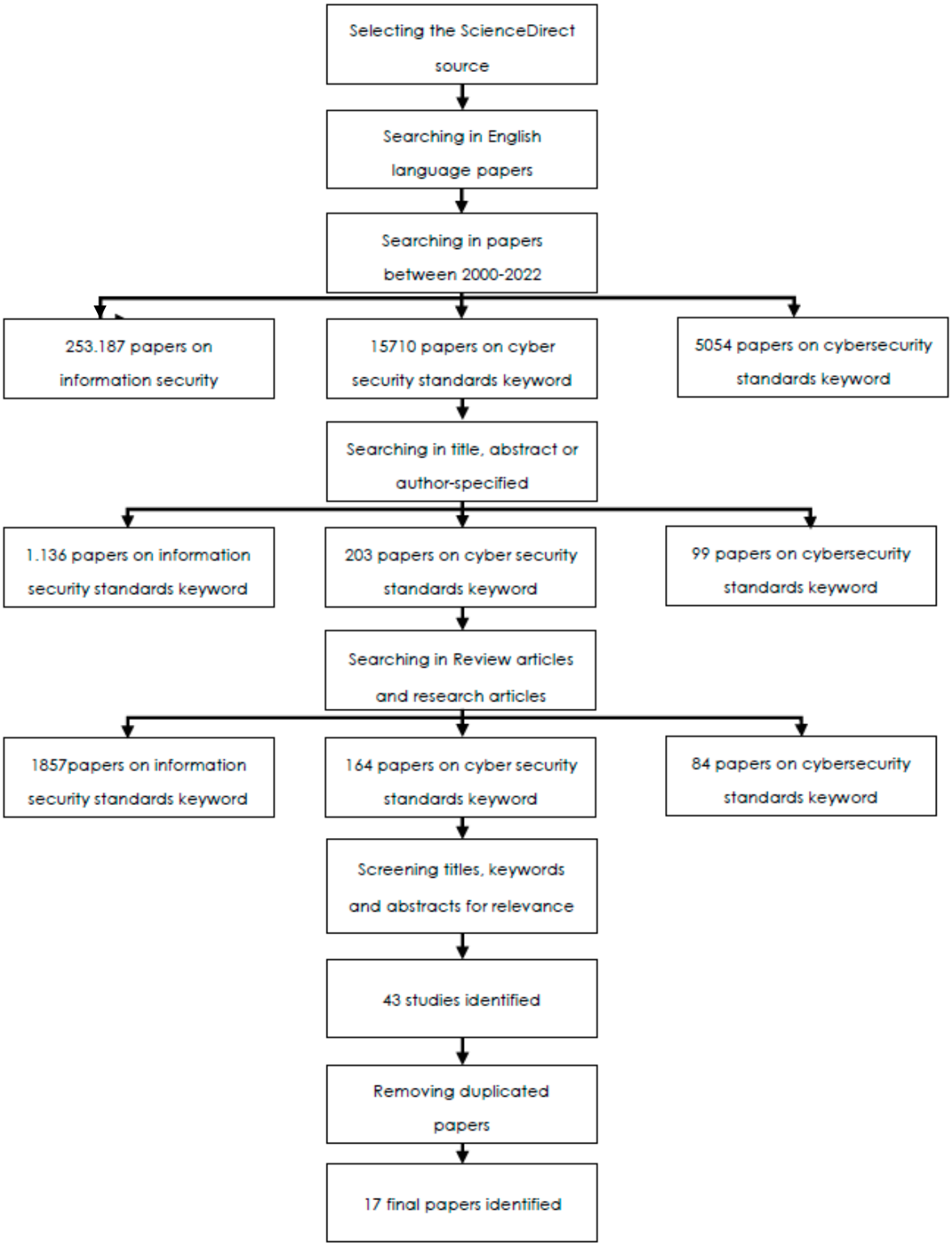

Figure 5. Flowchart of selecting papers for this narrative literature review.

6. Review of Information Security Standards

Table 2 summarizes the data of 17 extracted articles. For each paper, the title of the paper, author, and publication year are inserted in separate columns. Moreover, the aim

of the research, main findings of the research, relevant industry or field of usage, and employed standards were listed to provide an overview of the existing literature. The number of Science Direct citations as of 29 July 2022 are also inserted in a separate column to clarify how each paper is referenced.

Table 2. Review of information security standards/cybersecurity standards [27,28,46–60].

Source	Year *	Citation **	Aim of the Research	Main Findings	Field ***	Employed Standards
Piasecki, Urquhart, and McAuley	2021	1	To provide a clarification on the significance of employing edge computing models to better manage cyber threats to smart homes and realize inadequacies in existing standards.	In designing products, data protection should be regarded by reliance on organizational and technical safeguards to make sure that security of personal data is provided.	Smart homes	ENISA, DCMS
Breda and Kiss	2020	3	To describe how organizations that define information security standards are founded and the description of standards.	Employment of solutions for physical protection and application of the protected relevant areas lead to addressing the risk of nonconformity with information security standards.	Electromagnetic shielding emission security	ISO/IEC 27001, MSZ 15601-1:2007, ISO/IEC 27000, MSZ 15601-2:2007, ISO/IEC 27002, ISO 140-4:1998, IEEE-299-2006, MIL STD 285
Priyadharshini, Gomathy, and Sabarimuthu	2020	0	To provide an overview of the necessities for micro grids that determine cybersecurity challenges.	Presenting a guideline for professionals to select the guidelines and architecture for specific fields.	Micro grids	IEC 62,541, IEEE 1686, IEEE 1402, IEC 62443 (ISA 99), G3-PLC, ISO/IEC 27019, DHS Cyber Security, NIST SP 800-82, Security Profile for AMI, DHS Catalog, Privacy and Security—AMI, ISO/IEC 14543, ISO/IEC 27001 and 27002, AMI System Security, IEC62351Parts 1-8 IEC 62056-5-3, NIST SP 800-53, ISO/IEC 15408/Common Criteria, GB/T 22239, ISO/IEC 18045/CEM, NIST SP 800-124, NERC CIP, NISTIR 7628, IEEE C37.240
Srinivas et al.	2019	60	To review cyber threats, challenges, cybersecurity standards, and architecture in different governments, discussing challenges and strategies in the implementation of cybersecurity standards.	Providing recommendations for effective cyber defense and cyber security.	Government	CIMF

Table 2. *Cont.*

Source	Year *	Citation **	Aim of the Research	Main Findings	Field ***	Employed Standards
Leszczyna	2018	48	To provice an overview on smart grid standards that illustrate challenges in cybersecurity.		Smart grids	IEC 62,541, IEEE 1686, IEEE 1402, IEC 62443 (ISA 99), NIST SP 800-82, DHS Cyber Security, Security Profile for AMI, Privacy and Security—AMI, DHS Catalog, G3-PLC, AMI System Security, IEC 62056-5-3, ISO/IEC 27019, ISO/IEC 14543, NIST SP 800-53, GB/T 22239, ISO/IEC 18045/CEM, NIST SP 800-124, ISO/IEC 27001 and 27002, IEC62351Parts 1-8, NERC CIP, ISO/IEC 15408/Common Criteria, NISTIR 7628, IEEE C37.240
Leszczyna	2018	41	To provide an overview to identify the appropriate cybersecurity standard based on the requirements of smart grids.	An overview of cybersecurity standards for the smart grid area is provided for selection, based on the case.	Smart grids	NERC CIP, IEC 62443, NISTIR 7268, IEEE C37.240, ISO 15118, Privacy and Security of AMI, DHS Catalog, ISO/IEC 27019, IEC 62351, Cyber Security Procurement Language for CS, AMI System Security Requirements, IEEE 1686, VGB S-175
Hemphill and Longstreet	2016	16	To compare and evaluate existing standards for the U.S. retail economy data.	Proposing self-regulation standards for the industry	U.S. retail economy	Payment Card Industry Data Security Standard (PCI DSS)
Everett	2011	9	To focus on the importance of increasing awareness regarding risk management in information security.	Being pushed to implement a standard regardless of increasing personnel awareness is waste of time and money.		ISO 27005, ISO 31000
Papapanagiotou, Marias, and Georgiadis	2010	10	To review specifications of standards to promote the level of security and trust in mobile and wireless communication.	ADOPT (Ad hoc Distributed OCSP for Trust) performs better in comparison to other standards in terms of overhead and security.	Mobile and wireless networks	CSI, ADOPT, CPC-OCSP, CRLs, SCVP
Siponen and Willison	2009	200	To analyze and provide a comparison regarding BS ISO/IEC17799: 2000, BS7799, SSE-CMM standards, and GASPP/GAISP, aiming to realize their validation and application.	BS7799 and its derivatives, GASPP/GAISP, and SSE-CMM, are universal or generic standards in scope that do not consider the special requirements of different industries.		BS ISO/IEC17799: 2000, BS7799, SSE-CMM, and GASPP/GAISP,

Table 2. *Cont.*

Source	Year *	Citation **	Aim of the Research	Main Findings	Field ***	Employed Standards
Lai and Dai	2009	6	To describe approaches to implement physical isolation, network isolation, and logical isolation.	Presenting a new revision of implementation guidance for network isolation based on the ISO-17799 standard.	Government departments	ISO-17799
Humphreys	2008	77	To investigate the impact of information security standards on compliance and solving insider threat challenges.	ISO/IEC 27001 can be employed in organizations of different size and nature to address the risks of insider threats.		ISO/IEC 27001
Rowlingson and Winsborrow	2006	9	To compare the Payment Card Industry (PCI) Data Security Standard (DSS) with ISO17799.	The employment of PCI regarding the maturity level of an organization can lead to significantly decreased risk. However, ISO is almost mandatory and its loss will lead to penalty for the business.	Retail industry	Payment Card Industry Data Security Standard (PCI DSS), ISO17799
Broderick	2006	40	To provide a description on the evolution and application of ISMS and how it helps to fit into information protection regulations.			ISO/IEC-17799:2005, BS-7799-2:2002, ISO-27001:2005, ISO/IEC-17799:2000,
Theoharidou, Kokolakis, Karyda, and Kiountouzis	2005	166	To investigate the impact of ISO17799 to address insider threat.	To address the insider threat, we need to employ different IS approaches.		ISO17799
Fumy	2004	4	To review fundamental security mechanisms, including hash functions, encryption algorithms, digital signature schemes, and authentication techniques.	The main security challenge in organizations is its application by people, which should be addressed by training.		ISO/IEC TR 15947, ISO/IEC 24743, ISO/IEC TR 13335-5, ISO/IEC 17799, ISO/IEC 18028,
Gil-García	2004	14	To provide a comparison of the availability of IT standards and policies in the states.	The most significant, frequently reviewed and main concerns states to implement relevant standards among the are security, e-mail usage, internal networks, privacy, and software standards.	U.S. states	Subjects for information policies

* Year of Publication; ** Science Direct Citation (29 June 2022); *** Relevant Industry/Field.

7. Analysis and Discussion

Cybersecurity standards are significant for consideration in different organizations since they help businesses to identify best practices and methods for use to be equipped against cyber threats and the loss of valuable data [61,62]. These standards provide businesses with consistent metrics-based measures to ensure the effectiveness of methods and procedures that are employed to prevent and mitigate cyber threats [63].

As noted in this study, there are plenty of cyber security standards to be employed that are different in scope and features. In this study, an overview of the most frequently used cyber security standards based on existing papers in the cyber security field, their features and application areas, has been developed and a narrative literature review was conducted

by extracting 17 relevant papers that were published from 2000 to 2022 regarding cyber security standards considering the aim of each research, its main findings, relevant industry, and employed standards. Based on the review of these 17 papers in this study, several key contributions in information security standards have been investigated.

Breda and Kiss [46] introduced MIL STD 285 and IEEE-299-2006 as two appropriate standards to implement in electromagnetic shielding emission security in manufacturing based on the design of protected areas by investigating the appropriate standard to provide protective measures. However, among 17 reviewed papers, these two standards were the main focus of just on one article.

Referring to the findings of Siponen and Willison [47] in comparing validation and application of cyber security standards, BS ISO/IEC17799: 2000, BS7799, SSE-CMM, and GASPP/GAISP are standards that are universal and general to be employed in organizations of different sizes and natures.

According to Humphreys [48], who analyzed ISO/IEC 27001 in terms of following the management PDCA cycle and controls in response to insider threats in organizations of different sizes and natures, training personnel regarding security, handling critical information, access controls, the separation of duties, regular back-ups, social engineering, and mobile devices are recognized as major controls in ISO/IEC 27001 to deal with insider threats. Additionally, another study [58] has demonstrated the effectiveness of ISO17799 in addressing insider threats.

Moreover, Hemphill and Longstreet [49] have focused on data breaches in the U.S. retail economy, considering PCI DSS that is the Payment Card Industry Data Security Standard. PCI DSS is a standard in cyber security that is employed in the finance and banking industry for credit cards, debit cards, and pre-paid cards that are issued by Discover, American Express, MasterCard and Visa, and JCB International, among others. This standard is not compulsory to be implemented in the U.S.; however, the combination of self-regulation and market forces in industries that use cards significantly motivates the response to cyber threats.

Security management guidelines and network security guidelines including ISO/IEC 17799, ISO/IEC 24743, ISO/IEC TR 13335-5, ISO/IEC 18028, and ISO/IEC TR 15947 are reviewed by Fumy [28], who concluded that the role of human awareness to combat cyber threats is the most significant issue to be considered.

Moreover, Srinivas [27] analyzes cyber-attacks, along with security requirements and measures, and discusses CIMF, which is the architecture of the cybersecurity incident management framework. Then, introduces the main purpose of CIMF that is to develop an integrated management mechanism to respond cyber threats and incidents.

To compare PCI DSS and ISO17799 [50], both standards were reviewed by Rowlingson and Winsborrow, who finally concluded that although both standards have a lot in common in terms of aim and objectives, they differ significantly in terms of scope. ISO17799 is a general standard that can be employed in a wide range of organizations; however, PCI is applicable for a limited range of information systems, and its implication costs depend on the maturity of the systems and the security processes and controls within a system.

In studies that have been developed regarding security in the micro grid industry [51], an overview of cyber security standards that may be found useful in this regard has been developed. However, in all these studies, it was concluded that there is no significant standard to guarantee the security of a smart grid, and a combination of standards [53], or the one that is the best match based on the case, should be employed [59].

Broderick [52] analyzed security standards and security regulations, and BS-7799, ISO-17799, ISO-27001, and COBIT were recognized as the most popular information security frameworks and standards that are oriented toward each other. Moreover, the ISO-17799:2005 standard does not include any guide to implement network isolation except for auditing network physical isolation. Additionally, Lai and Dai [56] suggested the provision of a technique viewpoint and a management viewpoint for network isolation purposes.

From the review, it was also concluded that despite the fact that ISO 27500 and ISO 31000 complete each other [54], they do not make explicit reference to each other. Thus, ISO 27500 is just a framework that does not specify any certain method or control.

To evaluate the performance of standards in mobile and wireless communication [55], a prototype implementation has been designed to compare CSI, ADOPT, CPC-OCSP, CRLs, and SCVP standards and relevant resulting parameters, concluding that OCSP-based schemes perform better in comparison to other standards in the ICT industry. Considering security breaches as the result of employing the Internet of Things in smart homes, one study on cybersecurity standards [60] has concentrated on ENISA and DCMS standards as applicable standards for smart homes.

8. Limitations

The scope of the study is limited, since it only refers to the Science Direct database for the extraction of papers. Searching other databases may lead to a broader range of articles and expand the discussion, providing additional literature. Moreover, the search is limited to papers that were published between 2000 and 2022. Thus, articles that are published before 2000 are out of the scope of the study.

9. Conclusions

The paper presented the various types of information security standards and their applications in different fields to ensure the security of data against cyber threats. Based on their nature, some standards are considered mandatory for organizations to follow in order to become certified; however, some standards, such as ISO17799, are applicable to all types of organizations, regardless of their size and type. Moreover, in some cases, the application of one standard may not fulfill all the demands of an organization, and it may be necessary to employ a combination of standards in order to ensure security against cyber threats and data loss.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The author declares no conflict of interest.

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. Commun. Netw. Inf. Secur.* **2020**, *12*, 417–432.
3. Baron, J.; Contreras, J.; Husovec, M.; Thumm, N. *Making the Rules. The Governance of Standard Development Organizations and their Policies on Intellectual Property Rights*; Publications Office of the European Union: Luxembourg, 2019.
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. [CrossRef]
7. Karie, N.M.; Sahri, N.M.; Yang, W.; Valli, C.; Kebande, V.R. A Review of Security Standards and Frameworks for IoT-Based Smart Environments. *IEEE Access* **2021**, *9*, 121975–121995. [CrossRef]
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 Response*; 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 Frameworks*; 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. Comput. Secur.* **2017**, *25*, 535–559. [CrossRef]
13. Kaur, J.; Ramkumar, K. The recent trends in cyber security: A review. *J. King Saud Univ. Comput. Inf. Sci.* 2021, *in press*. [CrossRef]
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: Doha, 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*, 778–811. [CrossRef]
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. [CrossRef]
19. Dedeke, A.; Masterson, K. Contrasting cybersecurity implementation frameworks (CIF) from three countries. *Inf. Comput. Secur.* **2019**, *27*, 373–392. [CrossRef]
20. Taherdoost, H.; Masrom, M. An Examination of Smart Card Technology Acceptance Using Adoption Model. In Proceedings of the 31st International Conference Information Technology Interfaces, Cavtat, Croatia, 22–25 June 2009; IEEE: Cavtat/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. [CrossRef]
23. Ozkan, B.Y.; van Lingen, S.; Spruit, M. The Cybersecurity Focus Area Maturity (CYSFAM) Model. *J. Cybersecur. Priv.* **2021**, *1*, 119–139. [CrossRef]
24. Donaldson, S.; Siegel, S.; Williams, C.; Aslam, A. *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program 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. [CrossRef]
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 recommendations. *Future Gener. Comput. Syst.* **2019**, *92*, 178–188. [CrossRef]
28. Fumy, W. IT security standardisation. *Netw. Secur.* **2004**, *2004*, 6–11. [CrossRef]
29. Koza, E. Semantic Analysis of ISO/IEC 27000 Standard Series and NIST Cybersecurity Framework to Outline Differences 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 Protecció de Dades. *IDP Rev. Internet Derecho Y Política Rev. D'internet Dret I Política* **2021**, *33*, 7.
31. Fonseca-Herrera, O.A.; Rojas, A.E.; Florez, H. A model of an information security management system based on NTC-ISO/IEC 27001 standard. *IAENG Int. J. Comput. Sci.* **2021**, *48*, 213–222.
32. Rumiche Huamani, R.E. *Implementación de un Plan de Seguridad Informática Basado en la Norma ISO IEC/27002, Para Optimizar la Gestión en la Corte Superior de Justicia de Lima*; Universidad Privada del Norte: Trujillo, Peru, 2022.
33. Putri, M.K.; Hakim, A.R. Perancangan Manajemen Risiko Keamanan Informasi Layanan Jaringan MKP Berdasarkan Kerangka Kerja ISO/IEC 27005: 2018 dan NIST SP 800-30 Revisi 1. *Info Kripto* **2021**, *15*, 134–141.
34. Schmitz, C.; Schmid, M.; Harborth, D.; Pape, S. Maturity level assessments of information security controls: An empirical analysis of practitioners assessment capabilities. *Comput. Secur.* **2021**, *108*, 102306. [CrossRef]
35. Leander, B.; Čaušević, A.; Hansson, H. Applicability of the IEC 62443 standard in Industry 4.0/IIoT. In *ARES '19, Proceedings of the 14th International Conference on Availability, Reliability and Security, Canterbury, UK, 26 August 2019*; Association for Computing Machinery: New York, NY, USA; Canterbury, UK, 2019; pp. 1–8.
36. Macher, G.; Schmittner, C.; Veledar, O.; Brenner, E. ISO/SAE DIS 21434 Automotive Cybersecurity Standard—In a Nutshell. In *Computer Safety, Reliability, and Security*; Springer: Cham, Switzerland, 2020; pp. 123–135.
37. Choo, K.-K.R.; Gai, K.; Chiaraviglio, L.; Yang, Q. A multidisciplinary approach to Internet of Things (IoT) cybersecurity and risk management. *Comput. Secur.* **2021**, *102*, 102136. [CrossRef]
38. Boboň, S. *Analysis of NIST FIPS 140-2 Security Certificates*; Masaryk University: Brno, Czech Republic, 2021.
39. Institute, I.G. Aligning COBIT, ITIL and ISO for Business Benefit: Management Summary. A Management Briefing from ITGI and OGC. *IT Gov. Inst.* **2005**, *1*, 5–62.
40. Amorim, A.C.; da Silva, M.M.; Pereira, R.; Gonçalves, M. Using agile methodologies for adopting COBIT. *Inf. Syst.* **2021**, *101*, 101496. [CrossRef]
41. Kozina, M. IT Risk Management in the enterprise using CobiT 5. In Proceedings of the Central European Conference on Information and Intelligent Systems, Varazdin, Croatia, 13–15 October 2021; Faculty of Organization and Informatics Varazdin: Varaždin, Croatia, 2021; pp. 249–256.
42. Saarinen, M.-J.O. NIST SP 800-22 and GM/T 0005-2012 Tests: Clearly Obsolete, Possibly Harmful. *Cryptol. Eprint Arch.* **2022**, *169*, 1–8.

43. Almuhammadi, S.; Alsaleh, M. Information security maturity model for NIST cyber security framework. *Comput. Sci. Inf. Technol.* **2017**, *7*, 51–62.
44. NIST. Framework for Improving Critical Infrastructure Cybersecurity. In *Cybersecurity Framework*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2014; p. 41.
45. 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.
46. Breda, G.; Kiss, M. Overview of Information Security Standards in the Field of Special Protected Industry 4.0 Areas & Industrial Security. *Procedia Manuf.* **2020**, *46*, 580–590.
47. Siponen, M.; Willison, R. Information security management standards: Problems and solutions. *Inf. Manag.* **2009**, *46*, 267–270. [CrossRef]
48. Humphreys, E. Information security management standards: Compliance, governance and risk management. *Inf. Secur. Tech. Rep.* **2008**, *13*, 247–255. [CrossRef]
49. Hemphill, T.A.; Longstreet, P. Financial data breaches in the U.S. retail economy: Restoring confidence in information technology security standards. *Technol. Soc.* **2016**, *44*, 30–38. [CrossRef]
50. Rowlingson, R.; Winsborrow, R. A comparison of the Payment Card Industry data security standard with ISO17799. *Comput. Fraud Secur.* **2006**, *2006*, 16–19. [CrossRef]
51. Priyadharshini, N.; Gomathy, S.; Sabarimuthu, M. A review on microgrid architecture, cyber security threats and standards. *Mater. Today Proc.* **2020**. [CrossRef]
52. Broderick, J.S. ISMS, security standards and security regulations. *Inf. Secur. Tech. Rep.* **2006**, *11*, 26–31. [CrossRef]
53. Leszczyna, R. Cybersecurity and privacy in standards for smart grids—A comprehensive survey. *Comput. Stand. Interfaces* **2018**, *56*, 62–73. [CrossRef]
54. Everett, C. A risky business: ISO 31000 and 27005 unwrapped. *Comput. Fraud Secur.* **2011**, *2011*, 5–7. [CrossRef]
55. Papapanagiotou, K.; Marias, G.F.; Georgiadis, P. Revising centralized certificate validation standards for mobile and wireless communications. *Comput. Stand. Interfaces* **2010**, *32*, 281–287. [CrossRef]
56. Lai, Y.-P.; Dai, R.-H. The implementation guidance for practicing network isolation by referring to ISO-17799 standard. *Comput. Stand. Interfaces* **2009**, *31*, 748–756. [CrossRef]
57. Gil-García, J.R. Information technology policies and standards: A comparative review of the states. *J. Gov. Inf.* **2004**, *30*, 548–560. [CrossRef]
58. Theoharidou, M.; Kokolakis, S.; Karyda, M.; Kiountouzis, E. The insider threat to information systems and the effectiveness of ISO17799. *Comput. Secur.* **2005**, *24*, 472–484. [CrossRef]
59. Leszczyna, R. Standards on cyber security assessment of smart grid. *Int. J. Crit. Infrastruct. Prot.* **2018**, *22*, 70–89. [CrossRef]
60. Piasecki, S.; Urquhart, L.; McAuley, P.D. Defence against the dark artefacts: Smart home cybercrimes and cybersecurity standards. *Comput. Law Secur. Rev.* **2021**, *42*, 105542. [CrossRef]
61. Taherdoost, H.; Sahibuddin, S.; Jalaliyoon, N. A review paper on e-service; technology concepts. *Procedia Technol.* **2015**, *19*, 1067–1074. [CrossRef]
62. Taherdoost, H.; Hassan, A. Development of An E-Service Quality Model (eSQM) to Assess the Quality of E-Service. In *Strategies and Tools for Managing Connected Customers*; Ho, R.C., Ed.; IGI Global: Hershey, PA, USA, 2020; pp. 177–207.
63. Mishra, S.; Alowaidi, M.A.; Sharma, S.K. Impact of security standards and policies on the credibility of e-government. *J. Ambient Intell. Humaniz. Comput.* **2021**, *12*, 1–12. [CrossRef]