Analysis of Cybersecurity Standard and Framework Components

Melwin Syafrizal[1], Siti Rahayu Selamat[1], Nurul Azma Zakaria[3]

[1]Faculty of Computer Science, Universitas Amikom Yogyakarta, Indonesia
[2,3]Center for Advanced Computing Technology, Universiti Teknikal Malaysia Melaka, Malaysia (UTeM)

***Abstract*:** Satisfactory cybersecurity protection, encompassing all data security solutions, can only be achieved by adopting a cybersecurity framework that provides a structure and methodology for protecting critical digital assets. In addition, security experts recommend using cybersecurity standards which consist of a collection of best practices to protect organizations from cyber threats. However, many organizations, companies and governments lack experienced personnel in the cybersecurity domain, so they have difficulty adopting a standard approach or cybersecurity framework. Protecting organizations from cyber threats while demonstrating compliance with laws and standards is seen as extremely complex due to the difficulty on choosing the appropriate standard to be used. Moreover, lack of knowledge on the elements needed that offered by the standard is lead to the problem on identifying the started point where the protection will be began. Therefore, in this paper, a literature and the analysis is presented in identifying the elements of cybersecurity standard and framework that can be facilitate the organization or government on choosing the appropriate standard and framework to be used and utilized. The literature review was carried out to understand the various types of cybersecurity standards and frameworks and the analysis is conducted to identify the elements in each of them. In this paper, eight steps are presented and include the types of international standards, which are general, local regulation, as well as specific standards used in the industrial sector, to conclude the findings of the analysis. Furthermore, a relation map is presented using Writing a Literature Review release 2.0 approach to show the relationship between the literature review and future research.

***Keywords*:** best practice, cybersecurity, domain, framework, guidelines, standards**.**

1. Introduction

Digital technology and data have become an important part of human life today. Work, personal relationships, decision making, and daily activities rely heavily on devices and data. Unfortunately, there are threats that people overlook such as bad people who intend to steal personal data or business data with different motivations.

A survey agency in 2017 stated that rules or standards related to cybersecurity are almost unknown in the business world. Unless companies are involved in projects or tenders with mandatory requirements to meet cybersecurity security standards, new companies are trying to study security standards more intensively [1]. Research in 2019 stated that one in five companies (18%), and one in seven charities (14%) currently need a supplier that can meet cybersecurity standards, although some companies still do not consider suppliers a potential source of cyber risk [2].

However, the public is starting to be aware of technological developments and the ease of internet access increases active internet users every year. In addition, the condition of the Covid-19 pandemic around the world has triggered an increase in the number of internet users, increased online activity, increased bandwidth [3] that lead to an increased threat to digital data security [4] belonging to individuals, companies to governments.

Moreover, the increasing number of victims of internet fraud and its impact on online privacy issues shows that user privacy protection efforts are still low. It can also be an indicator of weak self-control in internet users [5]. Personal information or sensitive data that is leaked to the public accidentally can go viral in a matter of seconds. Files, images, or videos can become popular topics of conversation worldwide through social networking sites [6].

The public can see the lack of knowledge in society, organizations or businesses regarding the role of cybersecurity standards and frameworks. This may also be related to the lack of public awareness of the application of cybersecurity to secure IT assets, information (digital data) belonging to individuals or organizations.

Further, this paper will discuss: 1. Introduction; 2. Definition and related work, there is an explanation of the differences between standards and frameworks, as well as best practices and guidelines, cybersecurity standards and cybersecurity frameworks; 3. Methodology; 4. Analysis and Discussion, 5. Conclusions and Future work.

2. Definitions and Related Work

Using of information technology and internet connection is a risky investment, like a double-edged knife, one side of the blade is needed to support work, but on the other hand it presents a big threat if you do not master, are unable to manage, and act not according to the rules (standards). Not having a clear framework to protect all its assets, processes, and resources, will prevent the organization or business from focusing on achieving the larger organizational goals.

A cybersecurity strategy cannot be implemented effectively without the right cybersecurity framework [7] and cybersecurity standards as guidelines or techniques for protecting the environment or cyber organizations, including best practices that can be used for business or industry. A cybersecurity framework (CSF) can consists of security standards, implementations and best practices for managing cybersecurity. CSFs are very flexible and can reduce implementation costs, help protect and secure infrastructure, and other sectors (private or government) that are important to the economy and national security [8] [9].

Various types of organizations or businesses, private or public sector, local to multi-national companies, household businesses to critical infrastructure of a country start applying operational standards to safety standards to protect assets against owned business processes.

Some critical public infrastructures, which still use old systems in various countries, may be quite safe from cyberattacks, however, many critical infrastructures that have integrated information technology into their structures, apparently still lack adequate information security practices [166]

The electricity network is one of the critical infrastructures that are managed by the government and connected to the internet infrastructure which has a high threat level. Smart grid operators and stakeholders are well aware of the need for cybersecurity standards. There are quite a number of state regulations and organizational standards that provide standard recommendations to protect the power grid from cyber threats [10].

President Obama, in February 2013, commissioned NIST to establish a "Cybersecurity Framework." The framework is voluntary. Organizations or private sectors can adopt this framework into best practice for securing their own critical organization or [11].

Education, government and industry in several countries operate independently and do not cooperate. The US Department of Commerce, led by NIST, builds partnerships between academia, the private sector, and governments, by promoting secure networks and cybersecurity education ecosystems, in the form of training, and the Cybersecurity Framework - National Initiative for Cybersecurity Education (NICE) [12].

In the health sector, Diabetes Technology Society (DTS) launched the DTS Cybersecurity Standard for Connected Diabetes Devices (DTSec) project, to ensure the security of information sources for patients, doctors, hospitals, to equipment and drug suppliers. These resources are stored on servers and communicated (usually wirelessly) by mobile devices. Threats to cloud-connected diabetes monitoring devices including unauthorized disclosure or modification of therapeutic data, or deletion of device functionality will have a major impact on people with diabetes [13]

Based on the threats to the critical infrastructure and the environment on the usage of information technology with the implementation of the network as the platform in the organizations, businesses and governments, it indicates that cybersecurity standards and frameworks are needed to ensure the data and the infrastructure is protected.

2.1 Standards and Framework

Standard is an ideal condition as a minimum achievement limit [14], sometimes also defined as the highest or perfect achievement. Standards also mean technical specifications that must be met by a service facility so that service users can obtain the maximum function, purpose, or profit from the services provided.

According to www.standards.org.au, standards are voluntary documents that define specifications, procedures and guidelines that aim to ensure products, services and systems are safe, consistent and reliable [15]. While, ISO/IEC defined standards as rules or documents made based on a general agreement and approved by a legal entity, which defines the general use, regulation, regulation, or quality of an activity, which has the objective of achieving optimal results in a particular context as a guideline, model, or sample [16] [17].

A standard can be developed by a company or country, into a proprietary standard or local regulation standard, there are also specific industry standards or standards for service performance or product eligibility. Currently most international standards are voluntary standards, so adherence to standards is optional. A standard may also be required by the responsible organization, association or regulatory body to be complied with by the implementing organization under it in accordance with legal or regulatory provisions. Performance standards can be a policy or law that must be complied with by certain countries or organizations in a country, such as FISMA, HIPAA and GDPR.

Standards in Information Technology (IT) describes about an agreement between vendors who agree to use the same technology, so that between hardware and systems can communicate, and ensure services can be accessed. Open standards can be used by any type of organization by paying the cost of downloading a copy of the document, giving the user the opportunity to use part or all of the guidelines as needed or use it with other standards [18]. Several standards can be used together with other standards to complement and strengthen other requirements, such as those in ISO, BSI, and NIST with their Special Publications 800 series guideline.

Many international organizations, consortia and associations are involved in standard development. Some standards are "open" to all types of businesses and government organizations; others are "closed" specific to certain industries/businesses. Implementation of standards is expected to provide benefits in saving time and finances, so that production and profits increase, minimize risks, increase user awareness, and business continuity. Several standards development organizations such as ITU-T produced standards called "recommendations" for telecommunications networks [19], or IEEE-SA (Standards Association) which contributed by developing many standards for various fields, such as telecommunications, information technology and power plants [20].

A country has the authority to issue their standards, or reject rules or standards published by other countries. Standards can be anything that is determined by a country or organization to regulate, monitor, or assess an activity. The most common use of the term "standard" usually refers to documents that professional bodies establish for use by other organizations (i.e. program standards, technical standards), or standards for technical practice (i.e. practical cybersecurity standards).

A standard specifies what must be done to comply with the standard; by explaining and providing methods one by one in order to complete the process. Whereas a framework is a general guideline that can be adopted by businesses/companies/institutions, covering many components or domains, but does not specify the steps that must be taken [21].

A framework according to the Collins English Dictionary is the use of a complete set of rules, ideas or guidelines to describe a problem or determine what to do [14]. In general, a framework only provides a general description as a basis for building something or achieving a big, useful goal.

Typically, a framework is used to summarize the achievement of objectives, describe the scope, guide implementation and evaluation, and determine the quality standards to be achieved. Several detailed aspects of the analysis sometimes relate to standard aspects. Frameworks are often considered to be similar to "models" or "methods," because many frameworks consist of one or more models. There are frameworks based on modeling techniques (such

as process models, workflow models, life cycle models) and some based on best practices.

The framework gives users more freedom to choose part of the method or the whole use of the framework. Users are given the freedom to choose the methods or models or technical practices that are in the framework and offer general guidelines that can be adopted, as well as suggestions for the organization to be able to apply them in the organization. For example, ISO 31000 offers a framework for managing organizational risk, and there are general methods and guidelines for its application in organizations [22]. Another example, the PMBOK Guide presents processes and knowledge about the project life cycle, stakeholders, project organization, and offers guidance on how to develop a scope. Guide to Project Management Knowledge Bodies and often referred to as a framework for managing a single project [17].

Based on the definition discussed, the differences between standards and framework can be summarized in Table 1.

Table 1. Differences between standard and framework

Standards	Framework
• Voluntary documents that define specifications, procedures and guidelines to ensure products, services and systems are safe, consistent and reliable • Rules or documents made based on a general agreement and approved by a legal entity, which defines the general use, regulation, regulation, or quality of an activity • Can be developed by a company or country, into a proprietary standard or local regulation standard • To be complied with by the implementing organization under it in accordance with legal or regulatory provisions • 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" specific to certain industries or businesses • Specifies what must be done to comply with the standard; by explaining and providing methods one by one in order to complete the process	• A general guideline that can be adopted by businesses/companies/institutions, covering many components or domains, but does not specify the steps that must be taken • Only provides a general description as a basis for building something or achieving a big, useful goal • Used to summarize the achievement of objectives, describe the scope, guide implementation and evaluation, and determine the quality standards to be achieved

2.2. Best Practice and Guidelines

Best Practice is an example of how to work best based on existing situations and conditions, and other organizations have successfully implemented it in their organizational environment. Cybersecurity Best Practice, often refers to policies, procedures, strategies, or other activities related to cybersecurity. In general, the public has accepted this rule or activity as the best or more cost-effective solution. Most elements of a cybersecurity framework are best practices, from objectives to specific procedures or requirements.

A guideline is a set of documents or instructions that can assist in making a plan, or directing action or a guide for building an idea. Another guideline definition is suggested practice activities, which enable users to more freely translate, apply, or use them.

Guidelines do not have to relate to a specific methodology or category. In theory, guidelines differ from "standards and best practices," in that there are authorities making recommendations for standards and best practices, whereas guidelines are free to create by anyone. For ISO, directions are the first version of the document before the birth of a standard. Generally, the length of time between changing the status of issuing directions to formal status as standard is 5 years. The differences between best practice and guidelines is summarized in Table 2.

Table 2. Differences between best practice and guidelines

Best Practice	Guidelines
• Refers to policies, procedures, strategies, or other activities • Rule or activity as the best or more cost-effective solution • There are authorities making recommendations for standards and best practices	• A set of documents or instructions that can assist in making a plan, or directing action or a guide for building an idea • Do not have to relate to a specific methodology or category • Free to create by anyone

However, in cybersecurity, standards are often referred to as guidelines, standards and cybersecurity guidelines that provide directions for improving cybersecurity. Guidelines usually have no relation or agreement with existing standards.

2.3 Cybersecurity Standards

Cybersecurity standards are sets of technical rules or practices commonly used to protect the cyber environment or users in organizations with internet connections. The cyber environment includes the users themselves, network infrastructure, hardware, software, processes and services, local, cloud, or transit information, including system storage media that can be connected directly or indirectly to the internet network. The main objective is to reduce risk, including prevention or mitigation of cyberattacks.

Internet infrastructure and applications are increasing. Governments and businesses are increasingly aware of the opportunities and threats that arise from this development. They need standards to ensure the quality of work and service quality, as well as guarantee the security of data transactions and information. Increasing information security, software, network systems, information technology (IT) infrastructure, and other critical infrastructure is the goal of implementing cybersecurity standards. It can also define functional requirements, and guarantees in processes, systems, production environments, assets, and technology.

Cybersecurity standards can have a broad and deep scope, ranging from cryptographic algorithms to completeness of security features in applications, such as web browsers, and independent Information Security Management. A standard must be able to meet user needs, practical, low cost, taking into account the limitations of technology and resources to meet the standard. It must also meet the verification requirements of the standard; users expect to be able to assess security quality themselves, even when testing framework strength with other security testing activities.

In 2012, ISO issued a guideline for cybersecurity [23], a 50-page document that still leaves many unanswered questions about best practices and cybersecurity implementation. In general, the main purpose of this standard, namely: to provide a set of guidelines to stakeholders involved in cybersecurity organizations. With a series of instructions that refer to the domains contained in this standard, stakeholders can apply minimum controls throughout their organization to protect personal and organizational assets from the risk of threats from Cyberspace [24] [25]. Several cybersecurity standards can be classified as standalone standards such as IEC 62351, IEEE 1686, ISO/IEC DIS 15408-1, ISO/IEC 27019, GB/T 22239; others are classified as standard series such as ISO/IEC 27000, and IEC 62443 (ISA 99); or as a regulation such as NERC CIP [26].

2.4 Cybersecurity Framework

Cybersecurity Framework is a set of guidelines for companies or to follow to be better equipped to identify, detect and respond to cyberattacks. It also includes guidance on how to prevent to recover from attacks. The Cybersecurity Framework should include a set of standards, methodologies, procedures and processes that harmonize policy, business and technological approaches to address cyber risks. Cybersecurity Framework should include voluntary consensus standards and industry best practices to the extent possible [27].

The NIST Cyber security Framework (CSF) is a set of best practices, standards, and recommendations that help organizations increase their cybersecurity measure. The CSF was compiled by NIST after former United States President Barack Obama signed an executive order in 2014 [11]. NIST's CSF publishes a cybersecurity category that is more or less detailed than others. Cybersecurity Framework NIST has three main parts: 1) core framework; 2) the level of implementation of the framework; and 3) framework profile. The core framework has several functions: identify, protect, detect, respond, and recover [8] as depicted in Figure 1.

Figure 1. Cybersecurity Framework from NIST

NIST's U.S. eCommerce Department has released Cybersecurity Framework version 1.1 to improve the performance of Critical Infrastructure. Focus on vital sectors and industries of the country, protecting national and economic security, including energy, banking, communications and defense industries. Companies large and small in all industrial sectors can use this framework and recommend it to federal, state and local governments [8]. Many organizations and businesses in the USA as well as other countries have adopted NIST Special Publications as the standard, although the documents were originally published as guidelines for use by American Federal agencies.

A company headquartered in Canada has developed a methodology for implementing a management system for information security based on the ISO 27001 standard guidelines namely "Integrated Implementation for ISMS and Management Standards", based on the PDCA cycle as shown in Figure 2 which is divided into four phases: Plan, Do, Check and Act. Each phase has 2 to 8 steps (21 steps total) as shown in Figure 2. These steps are divided into 101 activities and tasks, which constitute a “Practical Guide” that considers the main stages of implementation from start to finish and suggests appropriate “best practices” for each organization [28].

Figure 2: Integrating the implementation of ISMS with Management Standards [28].

ISO 9001:2013 has actually abolished the PDCA model under the pretext of continuous improvement, and PDCA is just one of several approaches to meeting that requirement. There are other approaches, and organizations are now free to use them or not. The purpose of an information security management system (ISMS) is to maintain the confidentiality, integrity and availability of information by implementing a risk management process and giving confidence to interested parties to manage risk independently and correctly. Figure 3 shows an integrated ISO 27001: 2013 framework that incorporates the PDCA.

The ISMS is an integrated part of the organization's processes or operations and the overall management structure; information security is included in the design process, information systems, and control. The ISMS consists of the components of the Policy, Resources, Management Process, Information Risk Assessment and Treatment Risks, Statement of Conduct, documented information, and ISMS processes relevant to the organization. If previously standards can be used to assess conformity, now to assess organizations to meet the security requirements of the organization itself [29].

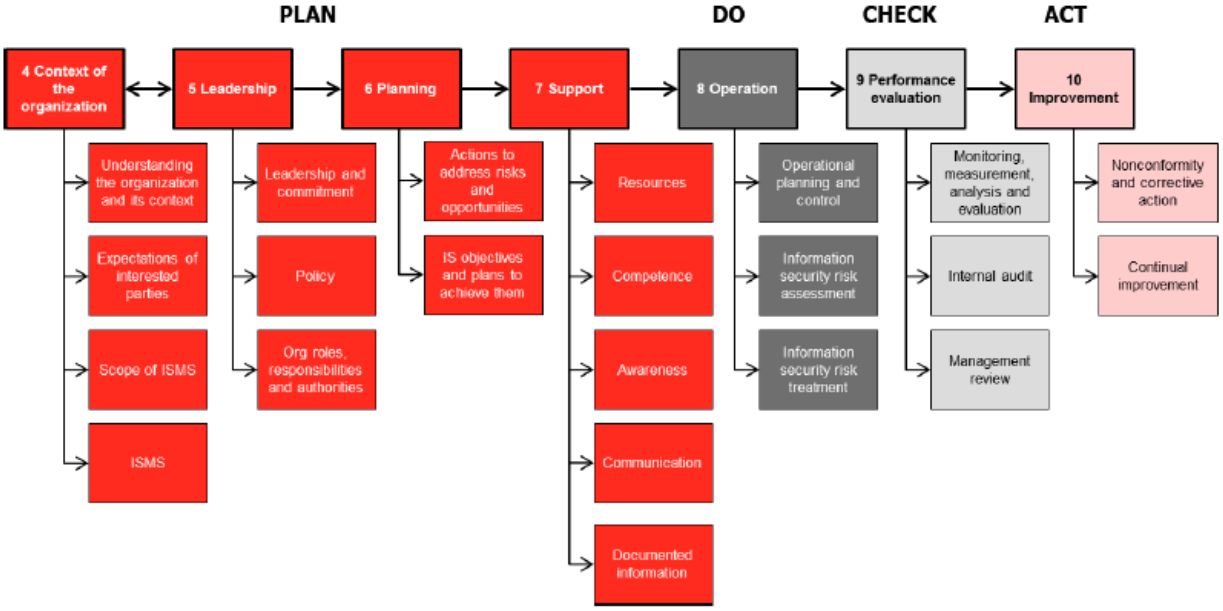

Figure 3: ISO 27001:2013 Framework Structure

3. Research Methodology

The methodology consists of six steps as illustrated in Figure 4. The steps are searching for references, reading and sorting references, understanding definitions and functions, collecting specific data about components, analyzing components and, presenting and discussing the analysis.

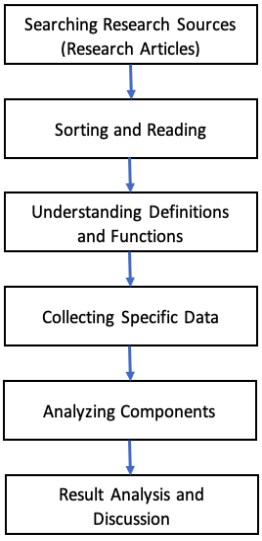

Figure 4. Methodology

These steps are performed in order to identify the differences, the importance and the components of cybersecurity standard and framework to be tailored to the needs of each organization or businesses to the government.

In the first step, the literature review survey follows the Writing a Literature Review release 2.0 approach [30]. In this step, a systematic search is carried out that can represent cybersecurity standards and frameworks, from scientific papers and books, as well as technical reports that explain cybersecurity standards and frameworks. The rigorous selection of papers from this process aims is to ensure the relevance of the source and the completeness of the paper content. Literature searches from well-known publisher databases covering cybersecurity topics, namely Elsevier (Science Direct), Association for Computing Machinery (ACM), IEEEXplore, EmeraldinSight, including searches on aggregate databases such as Scopus, WOS and Google (scholar.google.com, google.com, and books.google.com), which keeps records from various publishers.The search for electronic papers was carried out with the keywords "cybersecurity framework", "cyber security framework", "cybersecurity standards" and "cyber security standards", which identified more than 16,417 findings. Then more specifically, choose papers, proceedings, technical reports or parts of 263 titles of books to be downloaded or read by looking at the titles, keywords, and abstracts. List of reference sources as in Table 3.

Table 3. Initial search data for the cybersecurity framework and standard cybersecurity keywords

Science Direct				
Keyword	Results	Open Access	Open Archive	Year
“cybersecurity framework”	126	17	2	2008-2021
“cyber security framework”	68	5	0	2009-2021
“cybersecurity standard”	81	14	1	2003-2020
“cyber security standard”	87	4	0	2003-2020
ACM				
Keyword	Results	Journal/ Magazine	Proceeding/ Book	Year (DL)
“cybersecurity framework”	47	10	26	2008-2020
“cyber security framework”	19	1	18	2014-2020
“cybersecurity standard”	3	3	0	2008 & 2020
“cyber security standard”	3	1	2	2011 & 2020
IEEE Xplore (All Results)				
Keyword	Results	Conferences	Journals	Year (All)
“cybersecurity framework”	664	454	137	2004-2020
“cyber security framework”	2,349	1,767	444	1999-2021
“cybersecurity standard”	547	374	74	2005-2020
“cyber security standard”	1,612	1,244	227	2001-2020
IEEE Xplore (Open Access only)				
Keyword	Results	Early Access Article	Journals	Year (All)
“cybersecurity framework”	68	2	64	2014-2020
“cyber security framework”	169	2	166	2013-2020
“cybersecurity standard”	32	0	30	2016-2020
“cyber security standard”	91	2	88	2016-2020
Emeraldinsight				
Keyword	Results	Only Open Access	Only content I’ve access to	Year
“cybersecurity framework”	638	30	510	2003-2020
“cyber security framework”	Over 2000	78	Over 1000	2003-2020
“cybersecurity standard”	624	25	466	2002-2020
“cyber security standard”	Over 2000	63	Over 1000	2002-2020
Scopus				
Keyword	Results	Open Access	Other	Year
“cybersecurity framework”	107	8	99	2010-2020
“cyber security framework”	62	5	57	2006-2020
“cybersecurity standard”	66	8	58	2003-2020
“cyber security standard”	57	0	57	2003-2020
WoS				
Keyword	Results	Open Access	Proceeding	Year
“cybersecurity framework”	54	8	33	2010-2020
“cyber security framework”	25	2	17	2010-2020
“cybersecurity standard”	3	0	2	2010-2020
“cyber security standard”	3	0	1	2010-2020
Google				
Keyword	scholar	google.com	books	Year
“cybersecurity framework”	3,690	383,000	40	2015-2020
“cyber security framework”	1,510	279,000	15	2015-2020
“cybersecurity standard”	409	23,600	9	2015-2020
“cyber security standard”	183	198,000	6	2015-2020

In the second step, the paper is read to get the overview from the abstract, the first paragraph or theoretical basis, research methods and results. The descriptive data obtained is about 231 notes, and then, the analysis is done manually to obtain 165 publications relevant to the research.

Then, in the third step, in-depth review is conducted in order to understand and to extract the definition and use of standards, frameworks, best practices, guidelines, cybersecurity standards and cybersecurity frameworks.

Then, more specific data about the standard components and cybersecurity framework is collected in the fourth step. Based on the search on the websites, it shows that 184,000,000 articles are about "top cyber security standards" and 105,000,000 articles are about "top cybersecurity framework".

In general, the findings show about 250 types of cybersecurity frameworks and standards in use globally throughout the world. However, information about cybersecurity frameworks and well-known standards is difficult to obtain from journals, with few private sites/blogs or companies discussing them. Big industry/business, or governments, in general, develop their cybersecurity frameworks and standards to suit their needs. Today, many companies use more than one framework and standard in their business operations. Some cybersecurity standards and frameworks can be found on internet sites, with the google.com search engine as summarized in Table 4.

Table 4. Cybersecurity standards and frameworks popular on the internet

Name	Stands for	Type	Scope
International Standard and Framework (General)			
NIST CSF [31] [32] [33] [34] [35] [36] [9]	the National Institute of Standards and Technology-Cybersecurity Frameworks	Framework	Cybersecurity Critical Infrastructures Improves
Name	**Stands for**	**Type**	**Scope**
ISO/IEC 27001:2013 [37] [38] [39] [32] [40] [41] [42]	the International Organization for Standardization & the International Electrotechnical Commissions	Framework	Information Security Managements Systems
COBIT 5 [43] [44] [44] [21]	Control Objectives for Information and Related Technologies from ISACA	Framework	IT practices and governance
COSO [45] [46] [47] [48] [49] [50] [51] [52] [53]	Committee of Sponsoring Organizations – the Treadways Commissions	Framework	An Implementation Guide for the Healthcare Provider Industry & Financial reporting
NICE Framework [54] [55] [56] [12] [57] [58] [59] [60]	the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework	Framework	create sustainable education, training and workforce development programs to raise cybersecurity awareness
ETSI TC CYBER [61] [62] [63] [32] [64]	European Telecommunications Standards Institute Technical Committee on Cybersecurity	Framework	Cybersecurity Framework
CIS CSC [65] [66] [67] [7]	The Center for Internet Security - Critical Security Controls from SANS Institute	Framework	Effective Cyber Defense (SysAdmin, Audit, Network and Security
NIST SP 800 (series) [68] [69] [70][71] [33] [72] [73] [74]	NIST Special Publication	Standard	guidelines, recommendations, technical specifications, & annual cybersecurity reports
ISO/IEC 27032:2012 [75] [76] [77] [23]	ISO/IEC	Standard	Guidelines for Cybersecurity
CSA CCM [78] [79] [80] [81] [82]	Cloud Security Alliance's Cloud Controls Matrix)	Standard	Cloud Security
PAS 555 2013 [83] [84]	Publicly Available Specification from British Standard Institution	Standard	Cyber security risk-governance & management-specification
BS 7799-3:2017 [85] [86]	British Standard from British Standard Institution	Standard	Guidelines for Information security risk management
ISF SoGP [87] [32] [88]	Standard of Good Practices from Information Security Forum	Standard	Information Security
IASME [89] [7] [32]	Information Assurance for Small, and Medium, Enterprise	Standard	Information assurance standard based on ISO 27000 for small businesses
Local regulations related to cybersecurity			
NZISM [90]	New Zealand Information Security Manual (NZ)	Framework	Protective Security Requirements
NY DFS [91]	New York Department of Financial Services(US)	Framework	cybersecurity framework including licenses
HISO 10029:2015 [90]	Health Information Standards Organisation (NZ)	Framework	Health Information Security Framework
SNI ISO/IEC 27001:2013 [92] [93] [94] [95]	Standard Nasional Indonesia	Framework	Information Security Managements Systems
European GDPR [96] [56] [97] [98] [99] [4] [100] [101]	General Data Protection Regulation (EU)	Regulation	Regulation to Data Protection
FISMA [102] [103][104] [105] [81] [106]	Federal Information System Management Act (U.S. Federal Law)	Regulation	regulations for federal data security standards and guidelines
GB/T 22239-2019 [69] [10] [64]	National Standard of the People's Republic of China	Standard	Information security technology - Baseline for classified protection of cybersecurity
ASD Essential 8 [107] [108]	Australian Signals Directorate - Essential 8 (Australia)	Standard	Strategies to Mitigate Cyber Security Incidents
FedRAMP [104] [109] [79] [110] [88] [111] [112]	Federal Risk and Authorization Management Program (U.S. General Service Administration)	Standard	security assess, authorization, & continuous monitoring for cloud products/services
Cybersecurity for Industry-Specific Standards			
HITRUST CSF [113] [114] [35] [115]	Health Information Trust Alliance - Common Security Framework	Framework	certified framework for health care organizations to protect electronic health information
HIPAA [116] [117] [118] [119] [120] [121] [122] [123] [124]	The Health Insurance Portability and Accountability Act of 1996	Regulation	Protected Health Information
SOX [125] [126] [127] [128] [129] [130] [131] [132] [133] [134]	The Sarbanes–Oxley Act	Regulation	Financial Security
SOC 2 – AICPA [79] [96] [81] [135]	System and Organizational Controls 2 Report	Regulation	Report based on AICPA for managing customer data based on five “trust service principles”
PCI DSS [136] [137] [138] [65] [139] [81] [140] [141] [142] [143]	Payment Card Industry Data Security Standard	Standard	Security requirements to the cardholder data environment (CDE)
ISA/IEC 62443 [69] [144] [145] [146] [147] [148] [149]	International Society for Automation/ International Electrotechnical Commission	Standard	Security for Industrials Automations and Control System
ETSI TS 103 645 [101] [150]	European Telecommunications Standards Institute Technical Specification	Standard	Cyber Security for Consumer Internet of Things
NERC CSS-CIP [151] [152] [153] [154] [155] [156] [25]	Norths Americans Electrics Reliability Corporations-Cyber Security Standards	Standard	Critical Infrastructures Protections

SCAP [157] [102] [158] [159]	Security Content Automation Protocol	Standard	automated configuration, vulnerability, patch checking, technical control compliance activities, & security measurement
FINRA [160] [161] [162] [163] [164] [165]	Financial Industry Regulatory Authority	Standard	protect investors from potential abuses and ensure ethical conduct within the financial industry

The cybersecurity standards and frameworks are then searched again on the scholar.google.com search site and the publisher database with the keyword standard name which is given two quotes [" "] to find out how many other researchers have discussed and published in various international papers, and the results as listed in Table 5. As listed in Table 5, Intitle: column is indicates the standard name listed on the paper title found at scholar.google.com, and Total column is indicates the summation of papers found at scholar.google.com + Science Direct + ACM + IEEE Xplore + EmeraldinSight + Scopus + WoS.

Table 5. Search results on scholar.google.com and publisher databases

No	Standard Name	intitle:	Scholar. google	Science Direct	ACM	IEEE Xplore	Emerald insight	Scopus	WoS	Total
1	**ISO/IEC 27001 (series)**	569	16,300	312	72	57	78	975	117	17,911
2	**NIST SP-800 (series)**	90	11,300	356	94	100	27	187	128	12,192
3	**IASME**	5	8,630	83	0	1	15	13	1	8,743
4	**COBIT 5**	937	7,020	90	29	82	34	205	118	7,578
5	**COSO Framework**	106	3,970	116	1	2	94	48	36	4,267
6	**NICE Framework**	15	2,650	206	84	16	5	0	34	2,995
7	**NIST Cybersecurity Framework**	65	1,800	44	18	17	12	29	17	1,937
8	**NERC CIP**	29	1,510	84	19	37	1	77	31	1,759
9	**Standard of Good Practices**	0	67	583	0	1	186	262	1	1,100
10	**Cloud Controls Matrix**	12	970	51	13	10	2	14	11	1,071
11	**BS 7799-3**	0	341	250	0	0	1	0	1	593
12	**ISO/IEC 27032:2012**	4	443	8	3	1	4	3	2	464
13	**CIS Critical Security Controls**	3	244	7	3	1	2	3	2	262
14	**SOC 2 AICPA**	3	188	10	0	20	22	1	0	241
15	**PAS 555**	0	65	4	1	0	1	0	0	71
16	**ETSI TC CYBER**	0	36	2	0	0	0	0	0	38
17	**GDPR**	2,140	74,200	1,766	920	322	198	1,701	949	80,056
18	**FISMA**	36	7,520	502	70	25	12	70	27	8,226
19	**FedRAMP**	14	1,170	91	15	11	1	14	4	1,306
20	**NZISM**	0	50	261	0	0	0	0	0	311
21	**NY DFS**	1	92	0	0	0	0	1	0	93
22	**SNI ISO/IEC 27001:2013**	9	38	0	0	1	0	0	1	40
23	**GB/T 22239-2019**	1	28	0	0	0	0	0	0	28
24	**ASD Essential 8**	0	5	0	0	0	0	0	0	5
25	**HISO 10029:2015**	0	3	0	0	0	0	0	0	3
26	**HIPAA**	1,610	105,000	10,129	855	201	144	4,754	2,995	124,078
27	**The Sarbanes–Oxley Act**	787	46,700	2,868	125	21	1,200	1,078	589	52,581
28	**FINRA**	138	12,600	316	10	0	230	34	18	13,208
29	**PCI DSS**	160	7,330	621	107	32	33	113	43	8,279
30	**ISA/IEC 62443**	8	1,451	38	9	5	3	24	4	1,534
31	**Security Content Automation Protocol (SCAP)**	23	922	74	22	10	3	19	10	1,060
32	**HITRUST CSF**	0	82	3	2	0	0	0	0	87
33	**ETSI TS 103 645**	0	30	1	1	0	1	0	0	33

There are 19 of the 33 standards listed in Table 5 which in total have more than 1000 articles on scholar.google.com and six quite popular publisher databases. Therefore, it can be conclude that the 17 standards are quite popular among researchers, because they are used as titles so that they are included in the researcher's paper discussion. The search for 'Cloud Control Matrix' and 'Cloud Controls Matrix' found differences in the data on scholar.google.com, IEEE Xplore, and WoS databases so that the authors added up the values of the two databases. Also the standard 'ISA/IEC 62443' with 'ISA 62443' meaning the same is found in different texts, so the authors add the two together.

In the fifth step, the components of cybersecurity standards and frameworks is identify and analysed. During the identification, there are variety of terms and definitions are found that represent the components of the cybersecurity standards and frameworks. In this step, it was found that, from the article collected, the components are existed in 19 popular standards and frameworks related to cybersecurity. Unfortunately, it is very difficult to find the discussion in the latest journal papers but the results are quite a lot and varied found on official websites, blogs, to whitepapers issued by institutions that issue standards and frameworks or developer partners.

Finally, in the sixth step, the findings are discussed and elaborated as shown in Section 4. In this step, the components of cybersecurity standard and framework are presented and the similar components are highlighted.

4. Analysis and Discussion

Based on the data in Table 5, further analysis on over 1000 articles are performed to identify the components in each cybersecurity standard or framework and the findings is shown in Table 6.

Table 6. Components of Cybersecurity Standards and frameworks

ISO/IEC 27001:2013 Control	NIST Cybersecurity Framework Categories	NIST SP 800-53 rev.4 for FISMA & FedRAMP
• Information security policies • Organisation of information security • Human resource security • Asset management • Access control • Cryptography • Physical and environmental security • Operations security • Communications security • System acquisition, development and maintenance • Supplier relationships • Information security incident management • Information security aspects of business continuity management • Compliance	• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy • Access Control • Awareness and Training • Data Security • Information Protection Processes and Procedures • Protective Technology • Anomalies and Events • Security Continuous Monitoring • Detection Processes • Response Planning • Communications (2) • Analysis • Mitigation • Improvements (2) • Recovery Planning	•Access Control (AC) •Awareness and Training (AT) •Audit and Accountability (AU) •Security Assessment & Authorization (CA) •Configuration Management (CM) •Contingency Planning (CP) •Identification & Authentication (IA) •Incident Response (IR) •Maintenance (MA) •Media Protection (MP) •Physical & Environmental Protection (PE) •Planning (PL) •Personnel Security (PS) •Risk Assessment (RA) •Systems & Services Acquisition (SA) •Systems & Communications Protection (SC) •Systems & Information Integrity (SI)
COBIT 5 Domains and Processes	**ISF Standard of Good Practices**	**NICE Framework**
Governance of Enterprise IT • Evaluate, Direct and Monitor (EDM) **Management of Enterprise IT** • Align, Plan and Organise (APO) • Build, Acquire and Implement (BAI) • Deliver, Service and Support (DSS) • Monitor, Evaluate and Assess (MEA)	• Resilience • Risk Assessment • Supply Chain Management • Information Security Assessment • Security Arrangements • Policies, Standards And Procedures • Awareness • Compliance	• Securely Provision • Operate and Maintain • Oversee and Govern • Protect and Defend • Analyze • Collect and Operate • Investigate
IASME Standard Categories	**NERC CIP Standards**	**Components of COSO Framework**
• Organisation • Assessing the Risk • Policy and Compliance • Assets • Personnel • Physical and Environmental Protection • Operations and Management • Access Control • Malware and Technical Intrusion • Monitoring • Backup and Restore • Incident Management • Disaster Recovery & Business Continuity	• Sabotage Reporting • Critical Cyber-Asset Identification • Security Management Controls • Personnel & Training • Electronic Security Perimeter • Physical Security of BES Cyber Systems • System Security Management • Incident Reporting and Response Planning • Recovery Plans for BES Cyber Systems • Configuration Change Management and Vulnerability Assessments • Information Protection	• Control Environment • Risk Assessment • Information and Communication • Monitoring • Control Activities **COSO's ERM-Integrated Framework** • Internal Environment • Objective Setting • Event Identification • Risk Assessment • Risk Response • Control Activities • Information and Communication • Monitoring
CSA Cloud Controls Matrix Domains	**HIPAA Security Rule (Requirement)**	**HIPAA Security Zone**
• Application & Interface Security • Audit Assurance & Compliance • Business Continuity Management and Operational Resilience • Change Control & Configuration Management • Data Security & Information Lifecycle Management • Datacenter Security • Encryption & Key Management • Governance and Risk Management • Human Resources • Identity & Access Management • Infrastructure & Virtualization Security • Interoperability & Portability • Mobile Security • Security Incident Management, E-Discovery & Cloud Forensics • Supply Chain Management, Transparency and Accountability • Threat and Vulnerability Management	• Security Management Process • Assigned Security Responsibility • Workforce Security • Information Access Management • Security Awareness and Training • Security Incident Procedures • Contingency Plan • Evaluation • Business Associate Contracts and other Arrangements • Facility Access Controls • Workstation Use • Workstation Security • Device and Media Controls • Access Control • Audit Controls • Integrity • Person or Entity Authentication • Transmission Security	• Administrative safeguards • Physical safeguards • Technical safeguards **SOX Audit Controls** • Access • Security • Change management • Backup procedures **SOX Security Implementation** • Planning and scoping • Performing a risk assessment • Identifying significant accounts & controls • Formalizing and documenting control design • Evaluating the control design • Testing the control design for effectiveness • Identifying and remediating control deficiencies • Documenting process and results • Building sustainability although

Main elements of GDPR	PCI DSS Security Control & Processes	Eight areas of FINRA
• Breach Response, • Data Governance, • Risk Assessment, • Compliance Management	• Build and maintain a secure network, • Protect cardholder data, • Maintain a vulnerability management program, • Implement strong access control measures, • Regularly monitor and test networks, • Maintain an information security policy	• Governance and Risk Management for Cybersecurity; • Cybersecurity Risk Assessment; • Technical Controls; • Incident Response Planning • Vendor Management • Staff Training • Cyber Intelligence & Information Sharing • Cyber Insurance
ISA/IEC 62443 series of standards	**Security Content Automation Protocol (SCAP) Components**	**FISMA Compliance Requirements**
• System security conformance metrics, • Industrial automation and control system (IACS) - security lifecycle and use-cases • Security program requirements for IACS asset owners • IACS protection levels • Patch Management in the IACS environment • Requirements for IACS service providers • Implementation Guidance for IACS assets owners • Security technologies for IACS • Security Risk Assessment, System Partitioning and Security Levels • System security requirements and security levels • Product Security Development Life-Cycle Requirements • Security for Industrial Automation and Control Systems: Technical Security Requirements for IACS Components	• DataStream • Asset Identification (AID) • Asset Reporting Format (ARF) • Common Platform Enumeration (CPE) • Common Weakness Enumeration (CWE) • Common Configuration Enumeration (CCE) • Common Configuration Scoring System (CCSS) • Open Checklist Interactive Language (OCIL • Open Vulnerability and Assessment Language (OVAL) • Trust Model for Security Automation Data (TMSAD) • Extensible Configuration Checklist Description Format (XCCDF) • Software Identification (SWID) Tagging	• Categorize information systems • Select security controls • Implement security controls • Assess security controls • Authorize information system • Monitor security controls

Then, based on Table 6, an analysis is performed to determine the similar components existed from all standards and frameworks. As described in Table 4, there are 33 standards that were used as initial research sources used in this paper. Some of the general standards, local regulations, and industry-specific standards more specifically as frameworks, standards, or regulations are grouped because they are in the form of laws or regulations. In this analysis, the term domains, elements or categories is defined as components. The findings are summarized in Table 7.

Table 7. Analysis of cybersecurity standards and frameworks components
(⊗ = components existed)

No	Name of Standards	Information Security Policies	Asset Management	Access Control	Incident Management (Incident Response Planning)	Risk Management	Risk Assessment	Security Assessment	Governance	Resilience	Awareness and Training (Personal)	Information Protection (Data Security)	Monitoring	Communication	Analysis	Recovery Planning	Monitoring Activity	Business Continuity Plan	Compliance
1	**ISO/IEC 27001:2013**	⊗	⊗	⊗														⊗	⊗
2	**NIST SP 800-53**			⊗	⊗		⊗	⊗			⊗								
3	**IASME**			⊗	⊗		⊗				⊗						⊗	⊗	⊗
4	**COBIT 5**		⊗			⊗	⊗		⊗					⊗			⊗		
5	**COSO Framework**					⊗								⊗			⊗		
6	**NICE Framework**														⊗				
7	**NIST Cybersecurity Framework**	⊗	⊗	⊗		⊗	⊗		⊗		⊗	⊗		⊗	⊗	⊗			
8	**NERC CIP**				⊗						⊗	⊗				⊗			
9	**Standard of Good Practice**				⊗			⊗	⊗							⊗			⊗
10	**Cloud Control Matrix**				⊗	⊗			⊗	⊗		⊗						⊗	⊗
11	**GDPR**						⊗		⊗										⊗
12	**FISMA**			⊗	⊗		⊗	⊗			⊗						⊗		
13	**FedRAMP**			⊗	⊗		⊗				⊗								
14	**HIPAA**	⊗		⊗	⊗						⊗								
15	**The Sarbanes–Oxley Act**						⊗												
16	**FINRA**				⊗	⊗	⊗		⊗		⊗								
17	**PCI DSS**	⊗		⊗													⊗		
18	**ISA/IEC 62443**		⊗					⊗											
19	**Security Content Auto-mation Protocol (SCAP)**		⊗					⊗				⊗							

Table 7 shown the components existed in cybersecurity standards and frameworks that have similarities with other cybersecurity standards. From several components that are owned by each standard and framework, it is found that 2 to 11 similar components owned by 19 other standards and frameworks. In total there are 18 components that have in common between components of the cybersecurity standards and frameworks. Except for the components in FISMA and FedRAMP which have been equivalent to NIST SP 800-53, which have 17 components that have been equalized.

In general, there are many cybersecurity standards or frameworks that have components that are associated (mapping) with other standards, such as: categories contained in the NIST cybersecurity framework that have been associated or mapped to CCS CSC 1, ISA 62443, ISO/IEC 27001: 2013, NIST SP 800-53, Cobit 5, etc. Likewise, the CCM has been mapped to Cobit 5, ENISA IAF, FedRAMP, NIST SP 800-53, GAPP, HIPAA, ISO/IEC 27001: 2013, NERC CIP, PCI DSS, etc. These category standard mapping documents are usually in the form of .xls files which can be downloaded from the standard official website.

The data in Table 6 and Table 7 are needed to learn more about cybersecurity standards and frameworks. These standards and frameworks can generally be adopted without the need to conduct compliance audits if they are not required. If it is needed for the purpose of solving special problems or auditing for compliance with laws or regulations in force in a particular industry or country, the standards and frameworks can be used as references, developed, adjusted or combined with other standards.

Fulfillment of standards for a need in the business or organization world, does not have to meet all the criteria or components contained in one standard (can be selected according to need), and does not have to be implemented in all parts or departments in a company or institution, but can selected in what part or department is ready to be audited according to the desired target achievement.

Compliance with industry standards is more stringent and more complex, because there are more elements that must be met before compliance with regulations. Industry standards such as HIPAA, PCI-DSS and ISA/IEC 62443 are very specific, with many standard elements that are not similar to standard elements in general

5. Conclusions and Future Work

In this paper, many references from various publications in journals, conferences, ebooks, to white papers and various sites on the internet related to the topic of cybersecurity standards and frameworks are used to prove that this topic is still relevant enough to be raised. Topics with a wide variety of research development are found in many literatures and publications on the internet.

Based on searches in several publisher databases, researchers found 33 standards, frameworks and regulations related to cybersecurity which are quite widely discussed in journal papers, conferences to ebooks. Next, choose 19 standards, frameworks and regulations that have the most discussion (a total of more than 1000 titles of journal papers, conferences, and ebooks) which include the names of the standards in the paper titles, theoretical foundations to discussion.

In general, each of the standards, frameworks, and regulations related to cybersecurity has a different components from the others; although there are several components that have similarities or can be associated with components in other standards, as shown in Table 6. Some standards are general in nature so they can be used for various types of businesses, organizations, companies, and governments. Other standards are specific to local regulation, or specific to certain industrial fields. So it can be concluded that each of these standards, frameworks and regulations is very general or very specific according to its purpose. This is why there are many standard elements or requirements needed related to the implementation of cybersecurity or compliance with varying (different) rules.

Furthermore, using the Writing a Literature Review release 2.0 approach [30], it can show the relationship between current research and the future research as shown in Figure 5 that indicates that the analysis of the cybersecurity standards and frameworks are very importance and relevance for future cybersecurity concerns.

Figure 5. Mapping of current research and future research on cybersecurity standards and frameworks

Therefore, there are still many series of further research based on cybersecurity standards, cybersecurity frameworks, or cybersecurity guidelines and best practices that can be applied to current trending issues, such as IoT security, blockchain based cybersecurity frameworks, identity-based encryption, quantum-safe cryptography, hardware - software security module, hardware - software protection (guidelines or best practice), crypto agility, intelligence monitoring, reconciling cybersecurity risk, security encryption and certificate, artificial intelligence for cybersecurity resilience,

virtualization and cloud security, privacy protection and regulation, public safety protection, biometrics security, identity and security management.

References

[1] R. Klahr *et al.*, "Cyber Security Breaches Survey 2017: Main Report," 2017.

[2] R. Vaidya, "Cyber Security Breaches Survey 2019 - GOV.UK," 2019.

[3] S. Kemp, "Digital 2020-July Global Statshot Report," 2020.

[4] H. S. Lallie *et al.*, "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic," *Cryptogr. Secur.*, no. 21 june, pp. 1–20, 2020.

[5] H. Chen, C. E. Beaudoin, and T. Hong, "Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors," *Comput. Human Behav.*, vol. 70, pp. 291–302, 2017.

[6] A. Hamid, M. Alam, H. Sheherin, and A. S. K. Pathan, "Cyber security concerns in social networking service," *Int. J. Commun. Networks Inf. Secur.*, vol. 12, no. 2, pp. 198–212, 2020.

[7] A. Dedeke and K. Masterson, "Contrasting cybersecurity implementation frameworks (CIF) from three countries," *Inf. Comput. Secur.*, vol. 27, no. 3, pp. 373–392, 2019.

[8] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," 2018.

[9] NIST, "NIST Releases Version 1.1 of its Popular Cybersecurity Framework," *NIST*, 2018. [Online]. Available: https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework. [Accessed: 21-Apr-2019].

[10] R. Leszczyna, "A review of standards with cybersecurity requirements for smart grid," *Comput. Secur.*, vol. 77, pp. 262–276, 2018.

[11] S. Shackleford, A. Proia, B. Martell, and A. Craig, "Toward a Global Cybersecurity Standard of Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices," *Leg. Stud. Res. Pap. Ser.*, no. 291, pp. 1–58, 2015.

[12] W. Newhouse, S. Keith, B. Scribner, and G. Witte, "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework," 2017.

[13] D. C. Klonoff, F. Edin, F. Aimbe, and D. N. Kleidermacher, "Now Is the Time for a Cybersecurity Standard for Connected Diabetes Devices," 2016.

[14] C. E. Dictionary, "Collins Dictionary online," *Collins*. 2020.

[15] S. Australia, "What is a Standard?," 2018. [Online]. Available: https://www.standards.org.au/standards-development/what-is-standard. [Accessed: 15-Sep-2020].

[16] ISO/EIC, "ISO / IEC Directives Part 2 Principles and rules for the structure and drafting of ISO and IEC documents," Geneva, 2016.

[17] PMI, *A Guide to the Project MAnagement Body of Knowledge (PMBOK Guide)*, Sixth Edit. Pennsylvania: Project Management Institute, Inc., 2017.

[18] K. Krechmer, "The Meaning of Open Standards," *Proc. 38th Hawaii Int. Conf. Syst. Sci.*, vol. 50, no. 6, pp. 1–9, 2005.

[19] ITU-T, "SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Telecommunication Security : Overview of cybersecurity," 2008.

[20] K. Scarfone, D. Benigni, and T. Grance, "Cyber Security Standards," *Wiley Handb. Sci. Technol. Homel. Secur.*, p. 21, 2009.

[21] K. Seeburn, *Basic Foundational Concepts Student Book: Using COBIT® 5*. ISACA, 2014.

[22] ISO31000, "ISO 31000:2018(en) Risk management — Guidelines," *ISO Online Browsing Platform (OBP)*, 2018. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en. [Accessed: 12-Sep-2019].

[23] ISO/IEC27032, "ISO/IEC 27032:2012(en) Information technology — Security techniques — Guidelines for cybersecurity," *ISO*, 2012. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en.

[24] Deloitte, "A Deloitte Practical Guide For ISO27032 – Guidelines for Cybersecurity," 2012.

[25] M. Syafrizal, S. R. Selamat, and N. A. Zakaria, "Cybersecurity domains classification using mindmapping technique forpublic knowledge," *Test Eng. Manag.*, vol. 83, no. 10900, pp. 10900–10916, 2020.

[26] R. Leszczyna, "Standards on cyber security assessment of smart grid," *Int. J. Crit. Infrastruct. Prot.*, vol. 22, pp. 70–89, 2018.

[27] B. Obama, "Executive Order-Improving Critical Infrastructure Cybersecurity," 2013.

[28] P. Eric Lachapelle and P. Mustafe Bislimi, "ISO 27001 Information Technology – Security Techniques Information Security – Management Systems - Requirements," 2015.

[29] P. Biswas and A. Consultant, "ISO 27001:2013 Information Security Management System," *APB Consultant*, 2015. [Online]. Available: http://isoconsultantpune.com/iso-270012013-information-security-management-system/. [Accessed: 22-Apr-2019].

[30] R. T. Watson and J. Webster, "Analysing the past to prepare for the future: Writing a literature review a roadmap for release 2.0," *J. Decis. Syst.*, vol. 00, no. 00, pp. 1–19, 2020.

[31] Amazon Web Services, "NIST Cybersecurity Framework - Aligning to the NIST CSF in the AWS Cloud," 2017.

[32] A. Ibrahim, C. Valli, I. McAteer, and J. Chaudhry, "A security review of local government using NIST CSF: a case study," *J. Supercomput.*, vol. 74, no. 10, pp. 5171–5186, 2018.

[33] P. P. Roy, "A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard," *2020 Natl. Conf. Emerg. Trends Sustain. Technol. Eng. Appl. NCETSTEA 2020*, vol. 53, pp. 27001–27003, 2020.

[34] M. Benz and D. Chatterjee, "Calculated risk? A cybersecurity evaluation tool for SMEs," *Bus. Horiz.*, vol. 63, no. 4, pp. 531–540, 2020.

[35] A. Kohnke, K. Sigler, and D. Shoemaker, *Implementing Cybersecurity: A Guide to the National Institute of Standards and Technology Risk Management Framework*. CRC Press, 2017.

[36] L. Johnson, "Cybersecurity framework," *Secur. Control. Eval. Testing, Assess. Handb.*, no. February 2014, pp. 537–548, 2020.

[37] C. Carvalho and E. Marques, "Adapting ISO 27001 to a Public Institution," *Iber. Conf. Inf. Syst. Technol. Cist.*, vol. 2019-June, no. June, pp. 19–22, 2019.

[38] A. Phirke and J. Ghorpade-Aher, "Best practices of auditing in an organization using ISO 27001 standard," *Int. J. Recent Technol. Eng.*, vol. 8, no. 2 Special Issue 3, pp. 691–695, 2019.

[39] V. Diamantopoulou, A. Tsohou, and M. Karyda, "From ISO/IEC27001:2013 and ISO/IEC27002:2013 to GDPR compliance controls," *Inf. Comput. Secur.*, 2020.

[40] G. Disterer, "ISO/IEC 27000, 27001 and 27002 for Information Security Management," *J. Inf. Secur.*, vol. 04, no. 02, pp. 92–100, 2013.

[41] W. Knowles, J. M. Such, A. Gouglidis, G. Misra, and A.

Rashid, "Assurance techniques for industrial control systems (ICS)," *CPS-SPC 2015 - Proc. 1st ACM Work. Cyber-Physical Syst. and/or Privacy, co-located with CCS 2015*, pp. 101–112, 2015.

[42] ISO/IEC27001, "ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements," *ISO/IEC 27001:2013(en) Information technology — Security techniques — Information security management systems — Requirements*, 2013. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en. [Accessed: 21-Apr-2019].

[43] W. H. Tsai, C. L. Hsieh, C. W. Wang, C. T. Chen, and W. H. Li, "The impact of IT management process of COBIT 5 on internal control, information quality, and business value," *IEEE Int. Conf. Ind. Eng. Eng. Manag.*, vol. 2016-Janua, pp. 631–634, 2016.

[44] S. De Haes, W. Van Grembergen, and R. S. Debreceny, "COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities," *J. Inf. Syst.*, vol. 27, no. 1, pp. 307–324, 2013.

[45] J. Ma and C. Ma, "Factor analysis based on the COSO framework and the goverment audit performance of control theory," *Procedia Eng.*, vol. 15, pp. 5584–5589, 2011.

[46] R. F. Premuroso and R. Houmes, "Financial statement risk assessment following the COSO framework: An instructional case study," *Int. J. Account. Inf. Manag.*, vol. 20, no. 1, pp. 26–48, 2012.

[47] B. P. Lawson, L. Muriel, and P. R. Sanders, "A survey on firms' implementation of COSO's 2013 Internal Control–Integrated Framework," *Res. Account. Regul.*, vol. 29, no. 1, pp. 30–43, 2017.

[48] E. Karanja, "Does the hiring of chief risk officers align with the COSO/ISO enterprise risk management frameworks?," *Int. J. Account. Inf. Manag.*, vol. 25, no. 3, pp. 274–295, 2017.

[49] R. Von Solms and M. Willett, "Cloud computing assurance - A review of literature guidance," *Inf. Comput. Secur.*, vol. 25, no. 1, pp. 26–46, 2017.

[50] R. Kral, "Integrating a Compliance and Ethics Program With a Control Framework Leveraging Coso'S Internal Control–Integrated Framework," *Edpacs*, vol. 57, no. 6, pp. 11–17, 2018.

[51] A. Schandl and P. L. Foster, "COSO Internal Control - Integrated Framework: An Implementation Guide for the Healthcare Industry," *COSO - Committee of Sponsoring Organizations of the Treadway Commission*, no. January, p. 5, 2019.

[52] I. Udeh, "Observed effectiveness of the COSO 2013 framework," *J. Account. Organ. Chang.*, vol. 16, no. 1, pp. 31–45, 2019.

[53] M. R. M. Dangi, A. Nawawi, and A. S. A. P. Salin, "Application of COSO framework in whistle-blowing activities of public higher-learning institutions," *Int. J. Law Manag.*, vol. 62, no. 2, pp. 193–211, 2020.

[54] C. Paulsen, E. McDuffie, W. Newhouse, and P. Toth, "NICE: Creating a cybersecurity workforce and aware public," *IEEE Secur. Priv.*, vol. 10, no. 3, pp. 76–79, 2012.

[55] K. S. Jones, A. S. Namin, and M. E. Armstrong, "The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: Results from interviews with cybersecurity professionals," *ACM Trans. Comput. Educ.*, vol. 18, no. 3, 2018.

[56] CSEC2017 Joint Task Force, ACM, IEEE-CS, A. SIGSEC, and I. WG, "Cybersecurity Curricula 2017," 2017.

[57] K. Kim, T. A. Yang, J. Smith, and D. J. Kim, "An exploratory analysis on cybersecurity ecosystem utilizing the NICE framework," *Proc. - 2018 Natl. Cyber Summit Res. Track, NCS 2018*, pp. 1–7, 2018.

[58] J. Jacob, W. Wei, K. Sha, S. Davari, and A. Yang, "Is the NICE Cybersecurity Framework (NCWF) Effective for a Workforce Comprised of Interdisciplinary Majors?," *Int. Conf. Sci. Comput.*, pp. 124–130, 2018.

[59] I. Alsmadi and M. Zarour, "Cybersecurity Programs in Saudi Arabia: Issues and Recommendations," *1st Int. Conf. Comput. Appl. Inf. Secur. ICCAIS 2018*, pp. 6–10, 2018.

[60] R. Hodhod, S. Khan, and S. Wang, "CyberMaster: An expert system to guide the development of cybersecurity curricula," *Int. J. online Biomed. Eng.*, vol. 15, no. 3, pp. 70–81, 2019.

[61] ENISA, "Definition of Cybersecurity-Gaps and overlaps in standardisation," 2015.

[62] ETSI, "draft ETSI TR 103 456," 2017.

[63] R. Koch, "On the future of Cybersecurity," *Proc. 12th Int. Conf. Cyber Warf. Secur. ICCWS 2017*, pp. 202–209, 2017.

[64] R. Leszczyna, "Cybersecurity and privacy in standards for smart grids – A comprehensive survey," *Comput. Stand. Interfaces*, vol. 56, no. July 2017, pp. 62–73, 2018.

[65] S. Ghaisas, M. Motwani, B. Balasubramaniam, A. Gajendragadkar, R. Kelkar, and H. Vin, "Towards automating the security compliance value chain," *2015 10th Jt. Meet. Eur. Softw. Eng. Conf. ACM SIGSOFT Symp. Found. Softw. Eng. ESEC/FSE 2015 - Proc.*, pp. 1014–1017, 2015.

[66] U.S. FCC, "Cyber Security Planning Guide," 2016.

[67] A. Dutta and E. Al-Shaer, "'What', 'Where', and 'Why' Cybersecurity Controls to Enforce for Optimal Risk Mitigation," *2019 IEEE Conf. Commun. Netw. Secur. CNS 2019*, pp. 160–168, 2019.

[68] S.-53Ar4 NIST, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations Assessing Security and Privacy Controls in Federal Information Systems and Organizations," Gaithersburg, MD, 2014.

[69] X. Hao, F. Zhou, and X. Chen, "Analysis on security standards for industrial control system and enlightenment on relevant Chinese standards," *Proc. 2016 IEEE 11th Conf. Ind. Electron. Appl. ICIEA 2016*, pp. 1967–1971, 2016.

[70] S. Khou, L. O. Mailloux, J. M. Pecarina, and M. McEvilley, "A Customizable Framework for Prioritizing Systems Security Engineering Processes, Activities, and Tasks," *IEEE Access*, vol. 5, pp. 12878–12894, 2017.

[71] Y. Supriyadi and C. W. Hardani, "Information system risk scenario using COBIT 5 for risk and NIST SP 800-30 Rev. 1 a case study," *Proc. - 2018 3rd Int. Conf. Inf. Technol. Inf. Syst. Electr. Eng. ICITISEE 2018*, pp. 287–291, 2018.

[72] M. Al Fikri, F. A. Putra, Y. Suryanto, and K. Ramli, "Risk assessment using NIST SP 800-30 revision 1 and ISO 27005 combination technique in profit-based organization: Case study of ZZZ information system application in ABC agency," *Procedia Comput. Sci.*, vol. 161, pp. 1206–1215, 2019.

[73] J. I. NIST, "Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy," *NIST Spec. Publ. 800-37r2*, p. 164, 2018.

[74] NIST_CSRC, "Computer Security Resource Center," *CSRC*, 2018. [Online]. Available: https://csrc.nist.gov/publications/sp. [Accessed: 21-Apr-2019].

[75] S. Hurttila, "FROM INFORMATION SECURITY TO CYBER SECURITY MANAGEMENT – ISO 27001 & 27032 APPROACH," TALLINN UNIVERSITY OF TECHNOLOGY, 2018.

[76] R. De Bruin and S. H. Von Solms, "Cybersecurity Governance: How can we measure it?," *2016 IST-Africa Conf. IST-Africa 2016*, pp. 1–9, 2016.

[77] A. S. Markov and V. L. Tsirlov, "GUIDELINES FOR

CYBERSECURITY IN THE CONTEXT OF ISO 27032," *Cyber Secur. Issues*, vol. 1, no. 2, pp. 28–35, 2014.

[78] N. Pumvarapruek and T. Senivongse, "Classifying cloud provider security conformance to cloud controls matrix," *2014 11th Int. Jt. Conf. Comput. Sci. Softw. Eng. "Human Factors Comput. Sci. Softw. Eng. - e-Science High Perform. Comput. eHPC, JCSSE 2014*, vol. 66, pp. 268–273, 2014.

[79] B. Honan, V. Jirasek, T. Editor, and D. M. Rogers, *CSA Guide to Cloud Computing*. 2015.

[80] J. Kanpariyasoontorn and T. Senivongse, "Cloud service trustworthiness assessment based on cloud controls matrix," *Int. Conf. Adv. Commun. Technol. ICACT*, pp. 291–297, 2017.

[81] C. Di Giulio, R. Sprabery, C. Kamhoua, K. Kwiat, R. Campbell, and M. N. Bashir, "IT Security and Privacy Standards in Comparison: Improving FedRAMP Authorization for Cloud Service Providers," *Proc. - 2017 17th IEEE/ACM Int. Symp. Clust. Cloud Grid Comput. CCGRID 2017*, pp. 1090–1099, 2017.

[82] C. S. Alliance *et al.*, "Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) 3.0.1," 2018.

[83] BSI_ZZ/1, "PAS 555:2013-Cyber security risk. Governance and management. Specification," *BSI*, 2013. [Online]. Available: https://shop.bsigroup.com/ProductDetail?pid=000000000030261972. [Accessed: 21-Apr-2019].

[84] R. S. H. Piggin, "Governance, risk and compliance: impediments and opportunities for managing operational technology risk in industrial cyber security and safety," *9th IET Int. Conf. Syst. Saf. Cyber Secur.*, pp. 4.2.2-4.2.2, 2014.

[85] BSI_IST/33, "BS 7799-3:2017 Information security management systems. Guidelines for information security risk management," *BSI*, 2017. [Online]. Available: https://shop.bsigroup.com/ProductDetail?pid=000000000030354572. [Accessed: 20-Apr-2019].

[86] F. Siavashi, D. Truscan, and J. Vain, "Vulnerability Assessment of Web Services with Model-Based Mutation Testing," *2018 IEEE Int. Conf. Softw. Qual. Reliab. Secur.*, pp. 301–312, 2018.

[87] M. Chaplin and J. Creasey, "The 2011 Standard of Good Practice Principal," *Inf. Secur. Forum*, no. June, 2011.

[88] V. J. R. Winkler, *Securing the Cloud - Cloud Computer Security Techniques and Tactics*, vol. 95, no. 2. 2017.

[89] M. Bada and J. R. C. Nurse, "Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs)," *Inf. Comput. Secur.*, vol. 27, no. 3, pp. 393–410, 2019.

[90] Health Information Standards Organisation (N.Z.) and New Zealand. Ministry of Health, *HISO 10029:2015 Health information security framework*. 2015.

[91] S. Galli, "NYDFS cybersecurity regulations: A blueprint for uniform state statute," *North Carolina Bank. Inst.*, vol. 22, no. 1, 2018.

[92] Y. Nugraha, T. Roberts, I. Brown, and A. S. Sastrosubroto, "The Future of Cybersecurity Capacity in Indonesia Research Report 2016," 2016.

[93] M. J. Islami, "Challenges in The Implementation of National Cybersecurity Strategy of Indonesia from The Global Cybersecurity Index Point of View," *J. Masy. Telemat. dan Inf.*, vol. 8, no. 2, pp. 137–144, 2017.

[94] M. Nancylia, E. K. Mudjtabar, S. Sutikno, and Y. Rosmansyah, "The measurement design of information security management system," *Proc. 2014 8th Int. Conf. Telecommun. Syst. Serv. Appl. TSSA 2014*, 2015.

[95] A. B. Setiawan and A. S. Sastrosubroto, "Strengthening the security of critical data in cyberspace, a policy review," *Proceeding - 2016 Int. Conf. Comput. Control. Informatics its Appl. Recent Prog. Comput. Control. Informatics Data Sci. IC3INA 2016*, pp. 185–190, 2017.

[96] J. R. Vacca, *Computer and Information Security Handbook - Third Edition*, vol. 3. Morgan Kaufmann - Elsevier, 2017.

[97] NCSC & NCA, "The cyber threat to UK business," 2017.

[98] ENISA, "ENISA Threat Landscape Report 2017," ENISA, 2018.

[99] K. Watson and D. M. Payne, "Ethical practice in sharing and mining medical data," *J. Information, Commun. Ethics Soc.*, 2020.

[100] Center for Long-Term Cybersecurity, "Cybersecurity futures 2025: Insights and findings," no. February, p. 128, 2016.

[101] ETSI, "ETSI, Cyber Security for Consumer Internet of Things," vol. 1, pp. 1–16, 2019.

[102] CNSS, "National Information Assurance (IA) Glossary," 2010.

[103] L. G. D. Toomer, "FISMA compliance and cloud computing," *Proc. 2011 Inf. Secur. Curric. Dev. Conf. InfoSecCD'11*, pp. 99–103, 2011.

[104] L. P. Taylor, *FISMA Compliance Handbook - Second Edition*. 2013.

[105] J. Andress, S. Winterfeld, and L. Ablon, *CYBER WARFARE Techniques, Tactics and Tools for Security Practitioners*, 2nd ed. Syngress is an imprint of Elsevier, 2014.

[106] E. G. Amoroso, "Cyber Security Handbook and Reference Guide," 2019.

[107] I. A. Gheyas and A. E. Abdallah, "Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis," *Big Data Anal. Access*, vol. 1, no. 1, p. 6, 2016.

[108] Australian Government ASBFEO, "Cyber Security: The Small Business Best Practice Guide," 2017.

[109] S. Winterfeld and J. Andress, *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. 2013.

[110] M. Greer, "Cloud and the Government FITARA and FedRAMP : Accelerating Federal Cloud Adoptioning," *IEEE Cloud Comput.*, vol. 2, no. November 18, 2015.

[111] C. Di Giulio, R. Sprabery, C. Kamhoua, K. Kwiat, R. H. Campbell, and M. N. Bashir, "Cloud Standards in Comparison: Are New Security Frameworks Improving Cloud Security?," *IEEE Int. Conf. Cloud Comput. CLOUD*, vol. 2017-June, pp. 50–57, 2017.

[112] C. Di Giulio, R. Sprabery, C. Kamhoua, K. Kwiat, R. H. Campbell, and M. N. Bashir, "Cloud security certifications: A comparison to improve cloud service provider security," *ACM Int. Conf. Proceeding Ser.*, 2017.

[113] R. Sabillon, V. Cavaller, and J. Cano, "National Cyber Security Strategies: Global Trends in Cyberspace," *Int. J. Comput. Sci. Softw. Eng.*, vol. 5, no. 5, pp. 2409–4285, 2016.

[114] LLC HITRUST Alliance, "Introduction to the HITRUST CSF," no. September, pp. 1–18, 2017.

[115] J. Lamp, C. E. Rubio-Medrano, Z. Zhao, and G. J. Ahn, "The danger of missing instructions: A systematic analysis of security requirements for MCPS," *Proc. - 2018 IEEE/ACM Int. Conf. Connect. Heal. Appl. Syst. Eng. Technol. CHASE 2018*, pp. 94–99, 2019.

[116] K. J. Nahra, "HIPAA security enforcement is here," *IEEE Secur. Priv.*, vol. 6, no. 6, pp. 70–72, 2008.

[117] R. Wu, G. J. Ahn, and H. Hu, "Towards HIPAA-compliant healthcare systems," *IHI'12 - Proc. 2nd ACM SIGHIT Int. Heal. Informatics Symp.*, pp. 593–601, 2012.

[118] T. Alshugran, J. Dichter, and M. Faezipour, "Formally expressing HIPAA privacy policies for web services," *IEEE Int. Conf. Electro Inf. Technol.*, vol. 2015-June, pp. 295–299, 2015.

[119] Y. Jung and M. Kim, "HIPAA-Compliant Privacy Policy Language for e-Health Applications," *Procedia Comput. Sci.*, vol. 58, pp. 283–289, 2016.

[120] B. C. Drolet, J. S. Marwaha, B. Hyatt, P. E. Blazar, and S.

D. Lifchez, "Electronic Communication of Protected Health Information: Privacy, Security, and HIPAA Compliance," *J. Hand Surg. Am.*, vol. 42, no. 6, pp. 411–416, 2017.

[121] O. Kafali, J. Jones, M. Petruso, L. Williams, and M. P. Singh, "How Good Is a Security Policy against Real Breaches? A HIPAA Case Study," *Proc. - 2017 IEEE/ACM 39th Int. Conf. Softw. Eng. ICSE 2017*, pp. 530–540, 2017.

[122] B. J. Evans, "HIPAA's Individual Right of Access to Genomic Data: Reconciling Safety and Civil Rights," *Am. J. Hum. Genet.*, vol. 102, no. 1, pp. 5–10, 2018.

[123] P. R. Anish, V. Joshi, A. Sainani, and S. Ghaisas, "Towards enhanced accountability in complying with healthcare regulations," *Proc. - 2019 IEEE/ACM 1st Int. Work. Softw. Eng. Heal. SEH 2019*, pp. 25–28, 2019.

[124] A. Jayanthilladevi, S. K, and B. E, "Healthcare Biometrics Security and Regulations: Biometrics Data Security and Regulations Governing PHI and HIPAA Act for Patient Privacy," pp. 244–247, 2020.

[125] H. Chang and H. H. Choy, "The effect of the Sarbanes–Oxley Act on firm productivity," *J. Cent. Cathedra*, vol. 9, no. 2, pp. 120–142, 2016.

[126] M. Hoag, M. Myring, and J. Schroeder, "Has Sarbanes-Oxley standardized audit quality?," *Am. J. Bus.*, vol. 32, no. 1, pp. 2–23, 2017.

[127] H. S. Bhabra and A. T. Hossain, "The Sarbanes-Oxley Act and corporate acquisitions," *Manag. Financ.*, vol. 43, no. 4, pp. 452–470, 2017.

[128] I. M. Gordon and J. A. Nazari, "Review of SOX in the business ethics literature," *Manag. Audit. J.*, vol. 33, no. 5, pp. 470–502, 2018.

[129] B. Chu and Y. Hsu, "Non-audit services and audit quality — the effect of Sarbanes-Oxley Act," *Asia Pacific Manag. Rev.*, vol. 23, no. 3, pp. 201–208, 2018.

[130] M. S. Kim, J. Dandu, and P. Iren, "The effect of SOX on audit quality," *J. Financ. Crime*, vol. 26, no. 3, pp. 897–909, 2019.

[131] F. Xiao *et al.*, "Design and Analysis of a Strengthen Internal Control Scheme for Smart Trust Financial Service," *IEEE Access*, vol. 7, pp. 163202–163218, 2019.

[132] B. Fischer, B. Gral, and O. Lehner, "SOX section 404 twenty years after: Reviewing costs and benefits," *ACRN J. Financ. Risk Perspect.*, vol. 9, no. 1, pp. 103–112, 2020.

[133] J. Krishnan, J. Krishnan, and S. Liang, "Internal control and financial reporting quality of small firms: A comparative analysis of regulatory regimes," *Rev. Account. Financ.*, vol. 19, no. 2, pp. 221–246, 2020.

[134] A. Rupp, "Securitization and earnings management: evidence from the Sarbanes–Oxley act," *J. Financ. Regul. Compliance*, 2020.

[135] S. Bozkus Kahyaoglu and K. Caliyurt, "Cyber security assurance process from the internal audit perspective," *Manag. Audit. J.*, vol. 33, no. 4, pp. 360–376, 2018.

[136] G. Ataya, "PCI DSS Audit and Compliance," *Inf. Secur. Tech. Rep.*, vol. 15, no. 4, pp. 138–144, 2011.

[137] B. R. Williams and A. A. Chuvakin, *PCI compliance: Understand and implement effective PCI data security standard compliance, fourth edition*, Fourth. Syngress is an imprint of Elsevier, 2014.

[138] PCI SSC and S. A. P. S. I. Group, "Best Practices for Implementing a Security Awareness Program - Information Supplement," 2014.

[139] S. Yulianto, C. Lim, and B. Soewito, "Information security maturity model: A best practice driven approach to PCI DSS compliance," *Proc. - 2016 IEEE Reg. 10 Symp. TENSYMP 2016*, pp. 65–70, 2016.

[140] PCI Security Standards Council, "Information Supplement : Guidance for PCI DSS Scoping and Network Segmentation," no. December, p. 26, 2017.

[141] L. Elluri, A. Nagar, and K. P. Joshi, "An Integrated Knowledge Graph to Automate GDPR and PCI DSS Compliance," *Proc. - 2018 IEEE Int. Conf. Big Data, Big Data 2018*, pp. 1266–1271, 2019.

[142] S. Rahaman, G. Wang, and D. Yao, "Security certification in payment card industry: Testbeds, measurements, and recommendations," *Proc. ACM Conf. Comput. Commun. Secur.*, pp. 481–498, 2019.

[143] B. A. Sassani Sarrafpour, R. Del Pilar Soria Choque, B. Mitchell Paul, and F. Mehdipour, "Commercial security scanning: Point-on-Sale (POS) vulnerability and mitigation techniques," *Proc. - IEEE 17th Int. Conf. Dependable, Auton. Secur. Comput. IEEE 17th Int. Conf. Pervasive Intell. Comput. IEEE 5th Int. Conf. Cloud Big Data Comput. 4th Cyber Sci.*, pp. 493–498, 2019.

[144] S. R. Chhetri, N. Rashid, S. Faezi, and M. A. Al Faruque, "Security trends and advances in manufacturing systems in the era of industry 4.0," *IEEE/ACM Int. Conf. Comput. Des. Dig. Tech. Pap. ICCAD*, vol. 2017-Novem, pp. 1039–1046, 2017.

[145] M. Rekik, C. Gransart, and M. Berbineau, "Cyber-physical security risk assessment for train control and monitoring systems," *2018 IEEE Conf. Commun. Netw. Secur. CNS 2018*, 2018.

[146] N. Tuptuk and S. Hailes, "Security of smart manufacturing systems," *J. Manuf. Syst.*, vol. 47, no. May, pp. 93–106, 2018.

[147] B. Leander, A. Čaušević, and H. Hansson, "Applicability of the IEC 62443 standard in Industry 4.0 / IIoT," *ACM Int. Conf. Proceeding Ser.*, 2019.

[148] C. Jansen, "Stabilizing the Industrial System: Managed Security Services' Contribution to Cyber-Peace," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 5155–5160, 2017.

[149] A. Corallo, M. Lazoi, and M. Lezzi, "Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts," *Comput. Ind.*, vol. 114, p. 103165, 2020.

[150] G. Bendiab, K. P. Grammatikakis, I. Koufos, N. Kolokotronis, and S. Shiaeles, "Advanced metering infrastructures: Security risks and mitigation," *ACM Int. Conf. Proceeding Ser.*, 2020.

[151] C. NERC, "NERC Cyber Security Standards , CIP-002-1 through," 2006.

[152] Symantec Inc., "Solution Overview: Symantec Managed Services North American Electric Reliability Corporation (NERC) Cyber Security Standard," 2006.

[153] G. A. Weaver, C. Cheh, E. J. Rogers, W. H. Sanders, and D. Gammel, "Toward a cyber-physical topology language: Applications to NERC CIP audit," *Proc. ACM Conf. Comput. Commun. Secur.*, pp. 93–104, 2013.

[154] NERC, "CIP-011-2 -Cyber Security - Information Protection Standard Development Timeline," no. August, pp. 1–19, 2014.

[155] J. M. Cole, "Challenges of implementing substation hardware upgrades for NERC CIP version 5 compliance to enhance cybersecurity," *Proc. IEEE Power Eng. Soc. Transm. Distrib. Conf.*, vol. 2016-July, 2016.

[156] D. Christensen, M. Martin, E. Gantumur, and B. Mendrick, "Risk Assessment at the Edge: Applying NERC CIP to Aggregated Grid-Edge Resources," *Electr. J.*, vol. 32, no. 2, pp. 50–57, 2019.

[157] NIST 800-115, "Technical Guide to Information Security Testing and Assessment Recommendations of the National Institute of Standards and Technology," *Nist Spec. Publ.*, vol. 800, pp. 1–80, 2008.

[158] W. M. Fitzgerald and S. N. Foley, "Avoiding inconsistencies in the security content automation protocol," *2013 IEEE Conf. Commun. Netw. Secur. CNS 2013*, pp. 454–461, 2013.

[159] A. O. Adetunji, S. Butakov, and P. Zavarsky, "Automated Security Configuration Checklist for Apple iOS Devices Using SCAP v1.2," *2018 Int. Conf. Platf. Technol. Serv.*

PlatCon 2018, pp. 2–6, 2018.

[160] R. Kuhlman and J. Kempf, "FINRA publishes its 2015 'Report on Cybersecurity Practices,'" *J. Invest. Compliance*, vol. 16, no. 2, pp. 47–51, 2015.

[161] R. Kuhlman and J. Kempf, "Report on Cybersecurity Practices," 2015.

[162] B. Rubin and A. Pollet, "2016 FINRA analysis: a record-breaking year for fines," *J. Invest. Compliance*, vol. 18, no. 2, pp. 1–8, 2017.

[163] D. Nathan and B. Popken, "More of an SRO – FINRA unveils its priorities for 2018," *J. Invest. Compliance*, vol. 19, no. 1, pp. 39–41, 2018.

[164] S. Light, J. Normile, and L. Licht, "FINRA 529 Plan Share Class Initiative encourages firms to self-report violations," *J. Invest. Compliance*, vol. 20, no. 3, pp. 20–22, 2019.

[165] B. Rubin and A. Pollet, "FINRA's disciplinary actions in 2018:Increased fines ordered with significant drop in number of cases," *J. Invest. Compliance*, vol. 20, no. 3, pp. 1–5, 2019.

[166] J. Srinivas, A. Kumar, and N. Kumar, "Government regulations in cyber security : Framework , standards and recommendations," *Futur. Gener. Comput. Syst.*, vol. 92, pp. 178–188, 2019.