Chapter 11
Cybersecurity Standards and Policies for CPS in IoE

Kashif Naseer Qureshi, Garret O'Keeffe, Shane O'Farrell, and Graham Costelloe

11.1 Overview

Cybersecurity standards and policies are significant as a guideline and basic framework to protect the systems, networks, and other data processing components. Internet of Everything (IoE) is one of the new concepts where people, devices and processes, and systems are interconnected for data communication. These networks are further connected with backbone wired and wireless networks to collaborate in real time. The cybersecurity standards and frameworks can help to ensure the security and privacy of users and mitigate the potential risks and systems vulnerabilities. This chapter discusses the existing standards and frameworks to cover all Cyber-Physical Systems (CPS) for IoE networks. The chapter also suggests a standard framework to adopt and ensure confidentiality, integrity, and availability. The technical comparison of existing standards also discusses understanding the overall elements.

K. N. Qureshi (✉) · G. O'Keeffe
Department of Electronic & Computer Engineering, University of Limerick (UL), Limerick, Ireland
e-mail: kashifnaseer.qureshi@ul.ie; garret.okeeffe@mastercard.com

S. O'Farrell · G. Costelloe
Munster Technological University, Cork, Ireland
e-mail: shaneofarerell@mtu.ie; grahamcostelloe@mtu.ie

K. Naseer Qureshi et al. (eds.), *Cybersecurity Vigilance and Security Engineering of Internet of Everything*, Internet of Things,
https://doi.org/10.1007/978-3-031-45162-1_11

11.2 Introduction

A standard is an agreed way to build something, manage a process, or deliver a service for better processes and quality. Standards are represented as documents that define specifications, procedures, and guidelines, aiming to ensure the safety, consistency, and reliability of products, services, and systems. They are aggregated and distilled knowledge of the subject matter experts in the field who know the needs of the stakeholders they represent. Cybersecurity standards are designed to improve the security of IT systems, the networks they run on, and the infrastructure it is stored and processed on. Cybersecurity standards define the functional requirements to implement information security as well as the assurance requirements within the technology [1]. Cybersecurity standards are developed by cybersecurity subject matter experts to help people develop a system or assess an off-the-shelf or bespoke system to design or validate the application's security features [2].

As people, devices, and processes are involved in IoE networks and need proper security standards and frameworks to protect the user's data, standards need to be largely technology agnostic but must provide enough guidance to ensure the IoE system is as secure as possible without impeding the functionality of the system from doing its job. Standards cover a diverse set of areas, especially for IoE networks, and can range from a technical standard defining the cryptographic specifications for a crypto module to defining a process that ensures software is built in the recommended way (reducing the number of potential security flaws in the implementation) [3].

Both standards and guidelines provide guidance aimed at enhancing cybersecurity, but guidelines usually lack the level of consensus and formality associated with standards. Standards are a set of specifications that an organization should implement designed to reduce the risk to its clients. By implementing the standards, the company can categorically state that they have reached the quality as set out in the standard. In the case of a cybersecurity or data protection standard or regulation, this means clients of that organization can then be assured that their data is at least in some part secure against exfiltration, change, or misuse [4].

Standards provide a set of techniques, controls, and processes that they can implement to achieve and maintain a certain level of security. Standards also allow the organization to assess itself against a certain bar. Aligning with standards also helps a company when defining their approach to cybersecurity for themselves as they will have to build processes and mitigating controls specific to their organization to meet the standards they are trying to achieve. Standards tend to be created for organizations in specific industries and are used as a way of a) achieving a certain level of quality and b) assuring other clients or partners that they have met the level of quality needed to be trusted [5]. In the IoE networks, healthcare, education, transportation, and industrial companies are involved and need cybersecurity standards and frameworks to protect and secure systems. For example, the Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) develops standards in many areas, including information technology, telecommunications,

and power generation. An example of IEEE-USA's security work is its 802 Local Area Network (LAN)/Metropolitan Area Network (MAN) Standards Committee [6].

The International Organization for Standardization (ISO) is a nongovernmental organization that comprises standards bodies from more than 160 countries, with 1 standards body representing each member country [7]. For example, the American National Standards Institute represents the United States. ISO members are national standards organizations that collaborate in the development and promotion of international standards for technology, scientific testing processes, working conditions, societal issues, and more. ISO and its members then sell documents detailing these standards [3]. There are many international, regional, national, industry, and government groups involved in the development of cybersecurity standards. Standards Developing Organization (SDO) is an organization whose primary mission is the development of voluntary consensus standards on an international, regional, or national basis. Most SDOs cover a wide variety of technical areas, not just cybersecurity. In many cases, several stakeholders from within an industry will come together to ally with the specific goal of writing a standard. An example of this is PCI-DSS which is a standard focused on improving payment account security by ensuring that all companies that accept, process, store, or transmit payment card data abide by it. This standard was brought about by an alliance of Visa, MasterCard, AmEx, Discover, and JCB [8].

Standards differ in the ways that they are regulated. Depending on which governing body or regulatory organization, compliance with standards may be optional, or compliance may be a requirement. Voluntary standards are generally called voluntary because their use is optional, although a regulating agency could adopt or mandate their use. Mandatory standards are standards whose use is prescribed by a regulatory agency or implementing organization. Mandatory standards typically implement laws and regulations [9]. For example, PCI is a mandatory standard for the payment card industry. Companies rarely only use one set of standards. Business problems are very often solved using a combination of technology, management, and business processes, and because of this, several standards will normally come into play to ensure the successful and safe implementation of the project. An example might be the PCI standards imposed by an IoE company developing a software product for credit card transactions, but the standards used for the network communications are also in play as well as those used for developing an overall information systems management strategy for the wider organization such as ISO27000 series [10].

An Information Security Policy should offer a framework from which an organization can implement all security controls and processes deemed necessary and enforceable. A framework is a bunch of tools, guidance, and resources to help an organization with how it should think about a certain goal and how to achieve it. A standard is much more specific in its criteria for achieving that standard (although often not giving guidance on how to achieve it). The IoE networks need standards and frameworks to ensure data security from external or internal sources. Figure 11.1 shows the IoE standards overview.

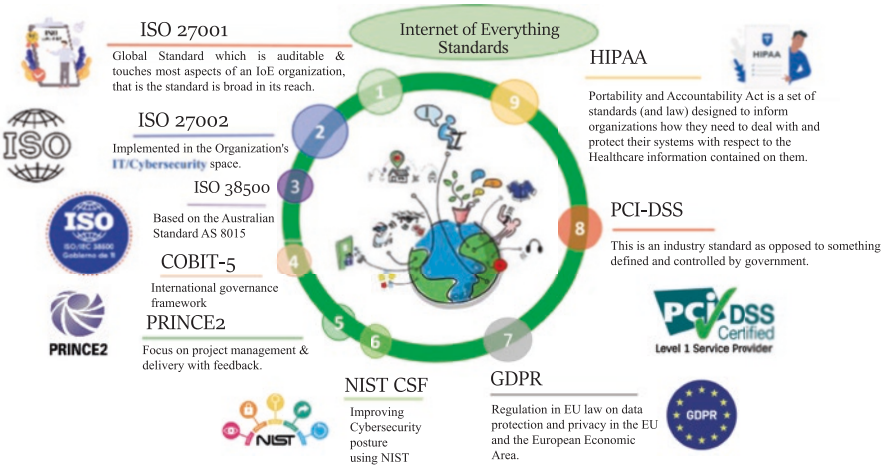

Fig 11.1 IoE standards overview

11.3 Information Security Standards Requirements, Policy, and Elements

Confidentiality, Integrity, and Availability (CIA) is the main principle of information security. Information security requirements for IoE networks should cover the following main area:

- Ensure user security by applying authorization and authentication to avoid unauthorized access to sensitive data.
- Ensure business continuity in any situation the business should run and normal.
- Timely identify the information security risks and come up with the risk management plan.
- Conduct training programs to make information security awareness to the organization.
- Ensure the data protection in IoE networks.
- Identify the new technology to protect the IoE systems.
- Identify and follow the industry standard to protect the data and organizations.
- It should include end-to-end security processes throughout the organization.
- The policy should be easy to understand and implement in heterogeneous IoE networks.
- Policy should be revised in a regular interval.
- Policy should focus on the organization goals.

11.3.1 Information Security Policy Elements

Purpose It covers overall approach of information security. This policy is for proper controls in IT department of an assurance company to ensure changes to production systems meet security standard and proper controls on production systems. The minimum number of people has access to production systems and data, ensuring data confidential for customers. The policy should set out the clear objectives for the information security. It should be able to set out how it will allow an organization to protect its IT or IoE networks assets, retain data integrity, be able to identify misuse of IT property (networks, assets), and protect it from security threats.

Audience It define the audience to whom the information security policy applies. The audience for this is the IT development team and production support team. This is not for system users. The policy should be able to identify the key stakeholders of the policy and also identify any high priority users whose policies might be more applicable depending on the data/responsibilities they may be working on/with.

Information Security Objectives Offer a secure, safe, data consistent environment and secure IoE systems from data breaches/threats by implementing a policy.

Authority and Access Control It defines hierarchical pattern and network security policy. The development team should only have access to development and test environments. Production support teams have access to production systems. Each user will have their own unique account, making their accounts individually traceable. By identifying the common users and the important users who will be working with more sensitive data and being able to authorize these users based on their relevant permissions or role-based access controls. There will be the physical control policies where certain uses will only be able to access certain physical areas of the organization.

Data Classification It classifies the data into categories "top secret," "secret," "confidential," and "public." Production environment is made up of multiple systems containing their own data. This data is to be reviewed for classifications such as health information only accessible to privileged users.

Data Support and Operations All confidential data must be encrypted at rest/storage and in transit. Backup of data is to be encrypted and stored in a secure location, with access limited to the backup team. All data transfer of confidential information must be encrypted and sent over a TLS connection. All data should be tagged with the relevant labels that will then associate their level of risk and only allow the specific users such as public, restrictive, confidential, and highly confidential data classifications. Numerous tools can be used to provide this element.

Security Awareness and Behavior Training is to be provided to the IT development team that how to develop best practices in the organization. Production support team is to be trained to handle confidential information. Awareness relies upon the sharing of knowledge with all staff not just the IT department or staff. Even having all the next-gen firewalls and security policies in place if a user clicks on a suspicious link and doesn't inform anybody, there is a massive threat of data breaches or an attack unfolding on the IT systems. The use of proxies can also help a business through web filtering and enforcing an acceptable Internet usage policy.

Encryption Policy Hide the data from unauthorized access. All disks containing confidential information must be encrypted.

Data Backup Policy Protect the data by making a copy of sensitive data in a secure environment. A full backup should to be taken every night and incremental every 10 min. Full backup should be stored in secure location limited to backup team and kept for 365 days.

Responsibilities, Rights, and Duties of Personnel It defines the responsibilities clearly. System to provide a report on the information held by us for an individual. System to provide the functionality to delete individuals from production systems. Helps to provide oversight on an organization's standard (ISO27001, ISO27002, COSO, CIS, and GDPR). There will be many different responsibilities which an organization will need to comply with. GDPR is the protection of personal data and the privacy of EU citizens. The security policy is responsible for protecting an organization's IT infrastructure.

11.4 Existing IoE Security Standards

This section discusses the most common existing cybersecurity standards and framework designed for communication systems and networks. These standards are also used for IoE networks because these networks are heterogeneous in nature and connected with backbone, clouds, and edge computing. These all systems are handled by organizations and companies.

11.4.1 ISO 27KX – ISO

This standard is the most commonly used set of standards in cybersecurity. These standards are generally concerned with the implementation of a certified information security management system within an organization. This means that the organization is doing its best and following best practices to ensure they are protecting user's data.

11.4.2 ISO 27001

This standard has the specifications for creating, operating, and controlling an ISMS. ISO 27002 then lists a structured set of controls to comply with 27001. 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 [11]. The ISO standards also provide standards and guidance. ISO 27001 is an international standard that lays out a specification for an Information Security Management System (ISMS). This standard aims to address data security by focusing on people and processes and also technology same as in IoE networks. The standard has a heavy focus on its risk-assessment approach which stipulates that a risk assessment must be carried out before any controls can be selected and implemented. This standard follows a Plan-Do-Check-Act model and has an independently accredited certification to align the ISMS with information security best practices. ISO 27001 has an international presence that many organizations recognize and trust. The ISO 27001 primary focus is on information security controls, unlike COBIT which is considerably broader in scope, focusing on information technology governance. The primary benefits of implementing ISO 27001 are the following:

1. The identification of critical information through the detailed analysis.
2. The implementation of security controls following the analysis.
3. A completed information security risk assessment of the system under review.
4. These benefits all lead to developing and supporting a more secure culture in the organization.

11.4.3 ISO 27002

ISO 27002 is a supplementary standard that focuses on information security controls and provides best practice guidance on applying the controls listed in Annex A of ISO 27001. The ISO 27002 framework is much more cyber-focused than the ISO 27001 standard. The standard highlights how each control operates, the purpose of the control, and how to oversee the implementation. There is no certification or accreditation for ISO 27002. ISO 27002 framework documents have the following policies and points:

- *Risk Assessment*: Understand assets, their threats, and how likely the threat can successfully be used to exploit an asset
- *Security Policy*: Formal document outlining what is required when implementing the system(s)
- *Organization of Information Security*: Details how authorized staff focus on data security

- *Asset Management*: An inventory and classification of assets details
- *Human Resource Security*: Details of the management around the lifecycle of employees, e.g., the security of personnel joining and leaving an organization
- *Physical security*: Managing and limiting access to physical systems including perimeters and facilities
- *Communication and Operations*: Technical operations-based security, e.g., network systems and firewalls, Internet front doors
- *Access Control*: Management and securing of access to infrastructure
- *Information Systems Acquisition, Development, and Maintenance*: Security from the ground up
- *Incident Management*: Security incidents and related processes and procedures around cybersecurity
- *Business Continuity Management*: Business-critical functions and protecting these
- *Compliance*: Complying with standards, rules, and regulations and applicable laws

11.4.4 ISO 38500

This standard guides advising, informing, or assisting directors where a director may be any of the organization's senior members, external, technical, legal, and professional bodies. The standard also guides those advising, informing, or assisting governing bodies including executive managers, members of groups monitoring the resources within the organization, external business or technical specialists, internal and external service providers, and auditors [12]. A principal advantage of the ISO 38500 IT governance framework is to ensure that accountability is assigned for all IT risks and activities. The objective of this standard is to provide a framework of principles for directors to use when *evaluating*, *directing*, and *monitoring* the information technology in the organization. The standard is applicable for both large and small industries in the ICT space in IoE networks. The standard is applicable across all organizations including public and private companies and government entities which use IT. The standard strives to promote effective and efficient IT services in organizations through the following:

- Building stakeholders' confidence on organizing IT governance
- Guiding governing bodies about use of IT in the organization
- Establishing familiarity with the principles of the governance of IT
- This standard context consists of five elements:
  - Source of authority
  - Regulatory obligations
  - Business pressure
  - Stakeholder expectations
  - Business needs

11.4.5 HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) is a set of standards (and laws) designed to inform organizations how they need to deal with and protect their systems concerning the healthcare information contained in them [13]. It is predominantly focused on the privacy of the data, but compliance with HIPAA is designed to ensure the CIA of PHI is maintained.

11.4.6 GDPR

GDPR is intended to cover the data privacy both in Europe and outside the EU through ensuring that any company who collects the data anywhere in the world must agree to comply with GDPR before being allowed get the data.

11.4.7 PCI-DSS

This is an industry standard as opposed to something defined and controlled by the government. Payment Card Industry Data Security Standard (PCI-DSS) is the result of an alliance of several credit card companies to ensure the safe, standardized handling of credit card data. It is not a law or regulation; it is self-imposed by the industry. Most small stakeholders get around their PCI requirements by using a PCI-compliant third-party provider. The PCI DSS is a collection of security standards governed by the Payment Card Industry Security Standards Council (PCI-SSC) [14]. This framework has been designed to secure credit and debit card transactions against data theft. PCI-DSS is a requirement for any organization that processes credit or debit card transactions. PCI certification is also considered the best way to safeguard sensitive data and information for card processing organizations.

PCI requires that all level 1 businesses (those organizations processing more than six million credit card transactions per year) undergo a yearly PCI audit conducted by a qualified auditor. PCI issued version 4.0 on March 31, 2022. The PCI DSS is a global standard that establishes a baseline of technical and operational standards for protecting financial account data. PCI-DSS v4.0 replaces the current PCI-DSS version 3.2 standard. Failure to comply with PCI-DSS means organizations will face huge financial penalties, damage to the company's reputation, and a loss of customer trust. Complying with PCI-DSS is a must for card processing organizations.

11.4.8 NIST-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.

11.4.9 COBIT

The Control Objectives for Information and Related Technologies (COBIT) framework was developed in 1993 by ISACA and has been revised several times with COBIT-5 (2012) now the current standard. COBIT is an international governance framework and is extensive. COBIT-5 certification is available [15]. COBIT-5 is globally accepted through its use of a common language with a focus on communication among all stakeholders. The COBIT framework aims to help organizations to create a governance system that is flexible and tailorable. COBIT describes how IT tasks can be positioned into generic processes and control objectives. Cybersecurity is only one of the many parts of this IT governance.

Although COBIT is large and complex, it does provide a common language for IT professionals, stakeholders, and management. COBIT 5 does an emphasis on information security. This aids organizations meet their business challenges, especially in areas of regulatory compliance, risk management, and lining up IT strategy with organizational goals. COBIT-5 is based on five principles that are essential for the effective management and governance of enterprise IT as follows:

- *Meeting stakeholder needs* – All operations and processes should be directed toward achieving business objectives and more.
- *Covering the enterprise end-to-end* – Creating value through governance and assigning roles and responsibilities …
- Applying a single integrated framework throughout
- *Enabling a holistic approach* – Allowing for greater organizational collaboration and achievement of common goals
- *Separating governance from management* – COBIT-5 firmly believes that activities and responsibilities must be differentiated, because each serves a different purpose.

These five COBIT principles sit on a foundation of seven COBIT enablers. These are to enable the organization to build a holistic framework for the governance and management of IT. In addition, COBIT also defines 37 processes which are further grouped into 5 domains:

- *APO* – Align, Plan, and Organize
- *EDM* – Evaluate, Direct, and Monitor

- *BAI* – Build, Acquire, and implement
- *DSS* – Deliver, Service, and Support
- *MEA* – Monitor, Evaluate, and Access

11.4.10 PRINCE2

The Projects In Controlled Environment (PRINCE2) standard is a *generic project management standard* widely used for managing software projects. PRINCE2 is widely understood and recognized, and there is PRINCE2 accreditation. PRINCE2 specifies what needs to be done rather than how to do it. It claims to be the recipe for the perfect project and also that it can be tailored for any project which can result in it having a very broad scope, defining all and nothing. PRINCE2 has a strong focus on feedback and attempts to be very flexible providing a common vocabulary. PRINCE2 also claims to promote consistency of project work and the ability to reuse project assets. PRINCE2 does not provide any specialist aspect although it's broad; it's not focused on any specific industry and does not provide any leadership capability, nor does it provide specific cybersecurity guidance. PRINCE2 defines a structure of principles, themes, processes, and environment.

11.4.11 NIST CSF

The Cyber Security Framework (CSF) framework was developed in 2013 and 2014 by NIST. It is the US-based National Institute of Standards and Technology, a non-regulatory section of the US Government. The aim was to help businesses to manage and mitigate cybersecurity risks. NIST has many similarities to ISO 270001 but there are no audits. NIST's CSF is a developing document. NIST frameworks are designed to be flexible and voluntary with a strong industry focus. The focus is intended to help the industry mitigate cybersecurity risks for critical infrastructure. NIST is primarily aimed at IT in the USA and aims to have a low adoption cost, but the CSF is used by organizations and governments around the world. NIST has five core components with further subdivisions into sub-categories. These components are identifying, protecting, detecting, responding, and recovering.

NIST CSF is based on some beliefs that workers outside the security team do not understand cyber-risk and therefore fail to "own" critical mitigation tasks and also how to address risk items and (lack of) knowledge of current tools and what's available in the marketplace. NIST offers the CSF as a set of optional standards, best practices, and recommendations for improving cybersecurity and risk management in the organization.

11.5 Technical Comparison of the Standards

Table 11.1 shows a comparison of cybersecurity standards with consideration of the concepts/attributes which are auditable, cost/effort to implement, targets in terms of cybersecurity, and broadness across the organization. These are the standard affecting the whole organization or quite specifically. The main focus of these standards is covering IoE organizations like industry and whether broad or narrow, IT or CSF, and global or local level networks and organizations. Table 11.1 shows the technical comparison of discussed standards.

11.6 A Security Framework for IoE Networks

As with standards, no one framework covers all aspects of an IoE network and risk requirements. However, to choose a framework, we must first understand what one is and why we might choose it. A cybersecurity framework is a set of best practices, standards, and recommendations that help an organization protect itself from cybersecurity risks. These frameworks guide organizations to implement and meet standard requirements, and by meeting those requirements and implementing the standards, they protect their data. The NIST cybersecurity framework was designed to fill a gap in standards when it comes to cybersecurity. Differing sets of standards, policies, and guidelines in the area have meant that cyber-criminals have been successful in exploiting the many vulnerabilities the gaps the policies and standards have left. NIST aims to collectively tackle the problem with a set of well-defined uniform standards and guidelines aimed to close the gaps and standardize the controls to mitigate the risk. NIST-CSF gives a comprehensive set of guidelines and tools to help you implement a cybersecurity program for the IoE network. The framework is organized into an easily understood set of five key functions.

1. *Identify*: Develop an organizational understanding to manage cybersecurity risk for systems, assets, data, and capabilities.
2. *Protect*: Develop and implement the appropriate safeguards to ensure delivery of services.
3. *Detect*: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
4. *Respond*: Develop and implement the appropriate activities to action regarding a detected cybersecurity event.
5. *Recover*: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber-attack.

As well as giving the guidelines, the framework provides tools to help the organization do the following:

Table 11.1 Technical comparison of standards

–	Primary objective	Type of policy	Standard used/ implemented
ISO 27001	Designed to build the foundations of information security Goal: To plan, implement, operate, monitor, and improve the ISMS There are 114 Annex A controls, divided into 14 categories A significant difference between ISO 27001 and COBIT is ISO 27001 is aimed specifically for information security, whereas COBIT is aimed for management and governance of information technology related business processes	ISMS scope document Information security policy Risk assessment process definition Statement of applicability (whether a control from Annex is applicable) Risk treatment process Information security policy Mobile device policy Remote access/teleworking policy Access control policy Cryptography policy Cryptography key management policy Clear desk and screen policy Acceptable use of information Assets policy Communications (information transfer) policy Secure development policy or plan Supplier management security policy	Global standard Framework which is auditable and touches most aspects of an organization, that is, the standard is broad in its reach ISO certification is valid for 3 years after which a recertification audit needs to be carried out Companies are required to perform surveillance audits for 2 years, and in year 3, a recertification audit is required
ISO 27002	Designed to implement controls and security management Much more cyber focused than ISO 27001 The ISO 27002 framework provides best-practice guidance on applying the controls listed in Annex A of ISO 27001	Cybersecurity Security policy – formal document outlining what is expected when implementing systems The policy offers guidance on the selection, implementation, and management of security controls based on the organization's information security risk environment	Global standard Implemented in the organization's IT/ cybersecurity space The standard is not auditable Process: Identify risks to an organization's information Implement controls appropriate to risks Monitor the organization's performance

(continued)

Table 11.1 (continued)

–	Primary objective	Type of policy	Standard used/ implemented
ISO 38500	A standard which indicates how an organization should evaluate, direct, and monitor their information technology Not as comprehensive as COBIT but aimed at senior management and also auditors	To promote effective and efficient IT services in organizations through: Building stakeholders confidence on organizing IT governance Guiding governing bodies about use of IT in the organization Establishing familiarity with the principles of the governance of IT	Global standard, based on the Australian Standard AS 8015 Many similarities to ISO 27002, implemented in the organization's IT/ cybersecurity space
COBIT-5	COBIT is an international governance framework and structures IT tasks into generic process and control objectives Focuses on management of information technology and governance Cybersecurity is only one part of the IT governance	COBIT 5 key principles: Applying a single integrated framework Meeting the stakeholder needs Covering the enterprise from end-to-end Enabling a holistic approach Separating governance from management 7 COBIT enablers: People, policies, and frameworks People, skills, and competencies Culture, ethics, and behavior Processes Organizational structures Services, infrastructure, and applications Information COBIT 5 defines 37 processes which are grouped in 5 domains: APO – Align, Plan, and Organize BAI – Build, Acquire, and Implement DSS – Deliver, Service, and Support EDM – Evaluate, Direct, and Monitor MEA – Monitor, Evaluate, and Assess	Global Standard. COBIT is an international governance framework and is very well known. COBIT-5 is very broad and touches all areas of the organization

(continued)

Table 11.1 (continued)

–	Primary objective	Type of policy	Standard used/ implemented
PRINCE2	Focus on project management and delivery with feedback Aimed at stakeholders who would likely be senior level managers. There is little focus on cybersecurity – primary focus is on project management	Structured project management with 7 principles but broad and can be used in many areas of the industry. 7 PRINCE2 principles: Continued business justification Learn from experience Defined roles and responsibilities Manage by stages Manage by exception Focus on products Tailor to suit the project environment	Developed originally in the UK as a government standard but now in wider use Used in the UK, Western European countries, and Australia As this is a project management framework, it can be used across the organization where desired There is a PRINCE2 practitioner certification programmer

- Create a risk profile to determine the organization's current level of cybersecurity risk.
- Identify the relevant standards to improve the controls and measures the organization puts in place.
- Help the organization develop new cybersecurity initiatives and requirements.
- Communicate the initiatives throughout the organization.

11.7 Conclusion

IoE networks paradigm emerged with new businesses, industries, and people's everyday routine processes. These networks are heterogeneous in nature and connected with backbone, cloud, and edge computing infrastructure. Due to these networks' complex nature, security threats and attacks are more serious concerns for these networks. The existing cybersecurity frameworks and standards are used in these networks to protect the user data and network. However, the existing cybersecurity standards still need improvements in many aspects. This chapter discussed the existing standard such as ISO 27002, ISO 38500, COBIT/COBIT 5, PRINCE2, and NIST CSF. Although these standards are adopted for backbone networks and by organizations and industries to fulfill security requirements, still there is need to develop more specific standards or frameworks to deal with these networks. This chapter also discusses these standards and compares all technically to examine their features and weaknesses. In last, the chapter also suggested the standard framework and main points to design a more feasible standard for IoE networks.

References

1. Qureshi KN, Jeon G, Piccialli F (2020) Anomaly detection and trust authority in artificial intelligence and cloud computing. Computer Networks:107647
2. Jagatheesaperumal SK, Rahouti M (2022) Building Digital Twins of Cyber Physical Systems With Metaverse for Industry 5.0 and Beyond. IT Professional 24 (6):34–40. doi:https://doi.org/10.1109/MITP.2022.3225064
3. Radanliev P, De Roure D, Nurse JR, Nicolescu R, Huth M, Cannady S, Montalvo RM (2019) New developments in Cyber Physical Systems, the Internet of Things and the Digital Economy–discussion on future developments in the Industrial Internet of Things and Industry 4.0. doi:https://doi.org/10.1007/s00146-020-01049-0
4. Zhan J, Dong S, Hu W (2022) IoE-supported smart logistics network communication with optimization and security. Sustainable Energy Technologies and Assessments 52:102052. doi:https://doi.org/10.1016/j.seta.2022.102052
5. Rehman M, Javed IT, Qureshi KN, Margaria T, Jeon G (2022) A Cyber Secure Medical Management System by Using Blockchain. IEEE Transactions on Computational Social Systems:1-14. doi:https://doi.org/10.1109/TCSS.2022.3215455
6. Williams BR, Adamson J (2022) PCI Compliance: Understand and implement effective PCI data security standard compliance. CRC Press,
7. Nah E-H, Cho S, Kim S, Cho H-I, Stingu C-S, Eschrich K, Thiel J, Borgmann T, Schaumann R, Rodloff AC (2017) International Organization for Standardization (ISO) 15189. Annals of laboratory medicine 37 (5):365–370. doi:https://doi.org/10.1128/9781555817282.ch22
8. Mahmud SY, Acharya A, Andow B, Enck W, Reaves B Cardpliance: PCI DSS compliance of android applications. In: Proceedings of the 29th USENIX Conference on Security Symposium, 2020. pp 1517–1533
9. Abdalla RS, Mahbub SA, Mokhtar RA, Ali ES, Saeed RA (2021) 6 IoE Design Principles and. Internet of Energy for Smart Cities: Machine Learning Models and Techniques:145
10. Leite JRE, Ursini EL, Chmielewski AMM, da Silva AJD New Technological Waves Emerging in Digital Transformation: Internet of Things IoT/IoE, 5G/6G Mobile Networks and Industries 4.0/5.0. In: Proceedings of the 8th Brazilian Technology Symposium (BTSym'22) Emerging Trends and Challenges in Technology, 2023. Springer, pp 329–339
11. Alshar'e M (2023) CYBER SECURITY FRAMEWORK SELECTION: COMPARISION OF NIST AND ISO27001. Applied computing Journal:245–255. doi:https://doi.org/10.52098/acj.202364
12. Rama AK, Gunawan E Evaluation of IT Governance Implementation Using COBIT 5 Framework and ISO 38500 at Telecommunication Industries. In: 2020 International Conference on Information Management and Technology (ICIMTech), 2020. IEEE, pp 453–457. doi:https://doi.org/10.1109/ICIMTech50083.2020.9211275
13. Shachar C (2022) HIPAA, privacy, and reproductive rights in a post-Roe era. JAMA 328 (5):417–418. doi:https://doi.org/10.1001/jama.2022.12510
14. Seaman J (2020) PCI DSS: An integrated data security standard guide. Apress,
15. Fernandes AJ, Hartono H, Aziza C (2020) Assessment IT governance of human resources information system using COBIT 5. International Journal of Open Information Technologies 8 (4):59–63