Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P144-cd

How Can ISO/IEC 27001:2013 be Associated with ISO/IEC 27001:2022, ISO/IEC 27002:2022, and 27019:2018 Using the Mapping Table?

Erfan Koza

Clavis Institute for Information Security, University of Applied Sciences, Erfan.Koza@hs-niederrhein.de

Asiye Öztürk

Clavis Institute for Information Security, University of Applied Sciences, Asiye.Oeztuerk@hs-niederrhein.de

After the amendment of ISO/IEC 27001:2022 as a normative standard for the declaration of requirements for an information security management system and ISO/IEC 27002:2022 as an informative reference and implementation guideline for the practical implementation of an ISMS, the challenge for the players in the energy industry is to combine and reference the newly defined and structured requirements and contents of ISO/IEC 27001:2022 and ISO/IEC 27002:2022 with the not yet updated industry-specific requirements of ISO/IEC 27019:2018. This ensures the state of the art in information security with reference to operational technology for power generation and distribution grid operations. The challenge here is to transfer the existing statement of applicability ISO/IEC 27001:2013 into the new ISO/IEC 27001:2022 structure and to subsequently link this with the industry specific requirements of ISO/IEC 27019:2018. In this paper, we show the changes in content and structure that amendment of ISO/IEC 27001 entails. Furthermore, the advantages and disadvantages of the amendment are listed. Subsequently, a mapping tool will be presented.

Keywords: ISO/IEC 27001:2022, Operational Technology, Energy Utility Systems, Information Security, ISMS

1. Introduction

The 27000 series of standards was produced jointly with the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The 27000 series is based on British Standard 7799 from the British Standards Institution. The processes include a framework based on ISO 9000, which is provided in all standards of the ISO standard as an idea for continuous improvement. The aspects relating to information security, implementation in processes, and ongoing operation of the ISMS are described as an incremental process, analogous to digitization. The ISO/IEC 27000 series of standards can be structurally divided into five sections (Figure 1). The first section of the ISO/IEC 27000 series begins with ISO/IEC 27000 (e. g. overview, vocabulary, and main definition), in which the relevant terminologies in context of information security are described in the form of a glossary. ISO/IEC 27000 (2020) This is used as a terminological basis, for example, to enable a uniform language among ISMS Stakeholder in the first and second line of defense. The ISO/IEC 27000 can be also used for a better technical understanding among internal and external users like between a Chief Information Security Officer (CISO) and a system operator or an auditor. ISO/IEC 27000 (2020)

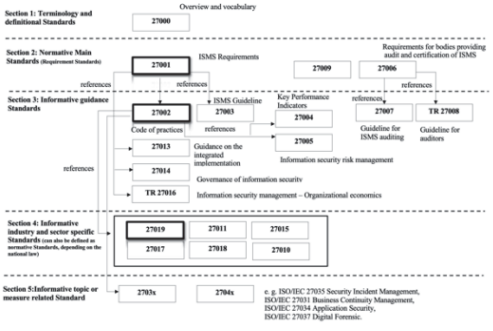

Fig. 1. Structure of ISO/IEC 27000 Standards

The next section (section 2) includes the normative standard ISO/IEC 27001.

The cross-industry or sector-independent standard ISO/IEC 27001 provides the basis and requirements for ISMS. ISO/IEC 27001 (2013) The structural design of ISO/IEC 27001 can be divided into two superordinated areas. The first area (Table 1) is based on the idea of continuous improvement and covers a total of seven topics (clauses 4 to 10) in order to declare the necessary financial, personnel and technical-, organization-processual requirements for the ISMS-implementation, operation, and ongoing optimization and improvement of an ISMS (Table 1). This area is also defined in the standard world as the so-called high-level structure, which is essentially used for the implementation of an Integrated Management System (IMS). The IMS follows the goal of simultaneously operating several management systems in a resource-saving, harmonized manner without redundancy.

Table 1. High-level structure of ISO/IEC 27001:2013

High-level structure of ISO/IEC 27001:2013
Clause 4: Context of the Organization (4.1 / 4.2 / 4.3 / 4.4)
Clause 5: Leadership and Commitment (5.1 / 5.2 / 5.3)
Clause 6: Planning (6.1 / 6.2)
Clause 7: Support (7.1 / 7.2 / 7.3 / 7.4 / 7.5)
Clause 8: Operation (8.1 / 8.2 / 8.3)
Clause 9: Performance Evaluation (9.1 / 9.2 / 9.3)
Clause 10: Improvement (10.1 / 10.2)

The second area called Annex A lists the specific objectives and controls in the context of information security. The requirements are defined in the annex A with a total of 114 controls in 14 individually sections (Table 2).

Table 2. Overview of Annex A ISO/IEC 27001:2013

Annex A	***Description of Controls***
A.5	Information Security Policies
A.6	Organization of Security
A.7	Human resource security
A.8	Asset management
A.9	Access control
A.10	Cryptography
A.11	Physical and environmental security
A.12	Operation security
A.13	Communication security
A.14	System acquisition, development, and maintenance
A.15	Supplier relationship
A.16	Information security incident management
A.17	Information security aspects of business continuity management
A.18	Compliance

The 114 controls can be operationally embedded and implemented in the organization's own structure with the help of the informative guide ISO/IEC 27002 "Code of practices" in the third section. ISO/IEC 27002 (2022)

ISO/IEC 27002 has a descriptive character in this context and is a corresponding orientation aid that provides information on how these action goals can be achieved and controls implemented. The fourth section contains the informative industry- and sector-specific standards (e. g., IS0/IEC 27010 until ISO/IEC 27019, except for ISO/IEC 27799) which essentially thematize the state of the art depending on the sector. The last section (section 5) includes the series of standards ISO/IEC 27030 until ISO/IEC 27044, which representative standards as informative topic or measure related guidance.

To use this referencing feature, the standards must be created in such a way that they are in time and content compatible with each other, so that a direct and simple reference between the standards is possible. Owing the time delays in the update processes of ISO/IEC 27001:2022, ISO/IEC 27002:2022 and 27019:2018, as well as the defined 36-month transition period in which the old ISO/IEC 27001:2013 can still be used, an industrial issue arises for mapping and referencing the new ISO/IEC 27001:2022 with the old ISO/IEC 27019:2018, as an updated version of ISO/IEC 27019 is not expected until 2025.

2. Research question and research approach

The key question for energy industry stakeholders, who begin with replacement their Statement of Applicability (SoA) based on ISO/IEC 27001:2013 to the new structure of ISO/IEC 27001:2022 and reference it simultaneously with ISO/IEC 27019:2018 to meet legal requirements of the European Union's Network and Information Security (NIS) Directive (NIS 1.0), was:

How can the two standards (ISO/IEC 27001:2022 "cross-sectoral requirement for ISMS" and ISO/IEC 27019:2018 "energy-sector-specific requirement for ISMS") be operated resource-saving, efficient and compatible, despite the different update status.

In this context, the aim is to approximate the content of the standards by means of a semantic analysis and to be able to present them in a more transparent manner for stakeholders in the energy industry. This approximation attempt is of elementary importance, because no uniform and robust mapping methodology exists for the two standards. Therefore, this research process and its result can be considered as a generic solution that can be implemented worldwide and by any organization in the field of power system and distribution system operation. With the mapping and associated transition of SoA 27001:2013 to SoA 27001:2022 and referencing ISO/IEC 27019:2018, as well as the associated artifact (excel-based mapping tool), Critical Infrastructures from the energy industry will enable the efficient and consistent design of their update and transition processes. In addition, the mapping tool can be used to redefine the audit process based on ISO/IEC 27001:2022.

3. Research Results

The individual results of the semantic analysis are as follows. First, the most important changes in the amendment process of ISO/IEC 27001 are listed and commented upon compared to the previous version. In addition, the advantages and disadvantages of the proposed method are discussed. This is followed by a presentation on the mapping tool.

3.1. *Main Changes of ISO/IEC 27001:2022*

There are significant structural changes, which address in detail the syntactic structure and presentation as well as the semantic consolidation of the subject areas. First, the most obvious change concerns the structure of the measure targets or controls. These were organized in new groups, the so-called "clauses", and provided with a simple taxonomy including associated attributes. In addition, the content itself has been greatly modernized. The 114 controls form ISO/IEC 27001:2013 have been compressed from a total of 14 security-related topic areas to four and to just 93 normative controls. These changes are in detail:

- New basic structure - 14 clauses restructured into 4 clauses,
- Chapter 5, Clause "Organizational controls" contains 37 controls (e. g., roles and responsibilities, Identity Access Management, information security incident Management etc.)
- Chapter 6, Clause "People controls" contains 8 controls (e.g., personnel processes – onboarding, offboarding, emergency boarding, information security awareness and training, etc.)
- Chapter 7, Clause "Physical controls" contains 14 controls (e.g., perimeter and object protection, handling of operating resources, clean desk and clear screen etc.)
- Chapter 8, Clause "Technological controls" contains 34 controls (e. g., securing end devices, access control, IT operations, logging and monitoring, Intrusion Detection Systems, network segmentation, und application security etc.)
  and monitoring, network segmentation, etc.).

All controls from the old version except for A. 11.2.5 "Removal of Assets" were adopted and consolidated, and a further 11 new controls were added. This means that a total of 56 controls from ISO/IEC 27001:2013 have been consolidated into 24 controls in ISO/IEC 27001:2022 (e.g., A.13.2.1, A.13.2.2 and A.13.2.3 into 5.14 "Information transfer" or A.8.3.1, A.8.3.2 and A.8.3.3 into 7.10 "Storage media").

The 11 new controls are:

- 5.7 Threat intelligence (identification and handling of threats) embedded in organization controls,
- 5. 23 Information security for use of cloud services embedded in organization controls,
- 5. 30 ICT readiness for business continuity embedded in organization controls,
- 7.4 Physical security monitoring embedded in physical controls (monitoring the security of physical perimeters and infrastructures),
- 8.9 Configuration management,
- 8.10 Information deletion,
- 8.11 Data masking,
- 8.12 Data leakage prevention,
- 8.16 Monitoring activities (monitoring and anomaly detection in networks),
- 8.23 Web filtering and
- 8.24 Secure coding (requirements for secure software development) embedded in technological controls.

The illustration below visualizes the modifications listed above.

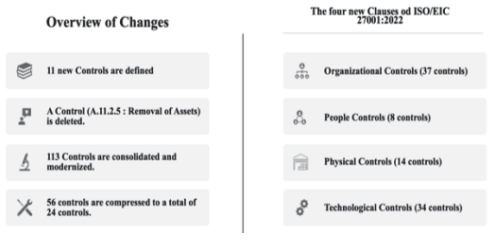

Fig. 2. Overview of Changes in context of ISO/IEC 27001:2022

3.2. *New Taxonomy and Attributes*

Further changes concern the syntactic representation of the individual controls, which are represented in particular by the newly defined taxonomy and attributes for each control. ISO/IEC 27001:2022 uses the attribute "Information Security Properties" to help assign controls to the basic values of information security or to the protection goals of information security (confidentiality, integrity, availability) and uses the attribute "Control Type" to classify these controls in terms of their effectiveness. The Control Type or the methodical assignment of the individual controls to the defence phases prevention, reaction, correction and detection helps to better understand the controls.

In addition, the controls were assigned to the phases of the NIST Cybersecurity Framework (NIST CSF) "Identify, Protect, Detect, Respond, and Recover" via another attribute, "Cybersecurity Concepts," which in turn makes it much easier to merge ISO/IEC 27001:2022 and NIST CSF. NIST (2018)

Figure 3 illustrates the new attributes and taxonomy of ISO/IEC 27001:2022.

Control Type	Information Security Properties	Cybersecurity Concepts	Operational Capabilities	Security Domains
#Preventive	#Confidentiality	#Identify	#Governance	#Governance_and_Ecosystem
#Detective	#Integrity	#Protect	#Asset_management	#Protection
#Corrective	#Availability	#Detect	#Information_protection	#Defence
		#Responde	#Human_resource_Security	#Resilience
		#Recover		

Fig. 3. New taxonomy and attributes of ISO/IEC 27001:2022

3.3. *Advantages and disadvantages*

The purpose of updating or amending the ISO/IEC 27001 and 27002 standards is to keep the standard up to date and to simplify it, thus responding to the dynamic changes in information security requirements and hybrid threat vectors. The update has integrated topics and areas that were previously not or insufficiently considered (e. g., Threat Intelligence or web filtering or secure coding) and brought them into line with the current state of the art.

These include technical requirements such as safeguarding when dealing with cloud systems and cloud service providers or monitoring system and user activities within the IT infrastructure. This is also required by the Network and Information Security (NIS) Directive 2.0, so attack detection systems such as network-based and cost-based instruction detection systems (IDS) should be embedded and operated in combination to monitor possible anomalies and exploitation of vulnerabilities in real time and to be able to isolate and thus respond to them immediately in the event of suspicion or misuse.

Regarding simplification of the standard, the total number of controls has been reduced by combining them, and the complexity of the structure has been reduced by adapting 14 subject areas to four clauses. Another advantage includes the declaration and embedding of attributes.

These now prevent misinterpretation and can avoid errors in implementation or errors in understanding. The advantage of the new structure is a clear separation into organizational, physical, personnel and technical measures, so that it is made clearer to organizations that information security must be implemented at several levels and is not just the responsibility of the IT department. This differentiation also addresses the holistic approach to information security, which can be represented by the triangulation of information security (e.g., technical security, organizational security, and individual human security). However, the changes from ISO/IEC 27001:2022 have an impact on existing embedded ISMS. ISO/IEC 27001 (2022)

It is therefore necessary to review the already implemented procedures and processes and to customize or modify them if necessary. This can be seen as disadvantageous by the respective organizations. It takes time and requires additional effort at the beginning. Furthermore, it will take time for mandatory works (especially ISO/IEC 27019, but also various industry-specific standards) that refer to the ISO/IEC 27001:2022 and ISO/IEC 27002:2022 standard to take the new structure into account. In the meantime, mapping tables must be used.

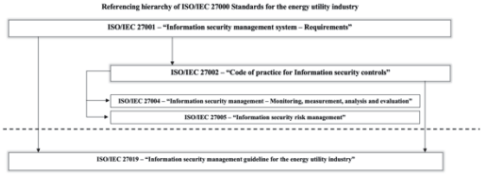

Fig. 4. Hierarchy of ISO 27000 series for energy utility industry

3.4. *SoA 27001:2022*

Organizations that have established an ISMS based on ISO/IEC 27001:2013, but especially those organizations that are certified in accordance with this standard, must consider the changes made to ISO/IEC 27001 and 27002 and implement the new or changed requirements. As part of the defined risk handling methodology according to ISO/IEC 27001 Chapter 6.1.3 c, it must be verified whether the organization's existing measures also meet the requirements from the updated and new controls.

For this purpose, it is necessary to identify existing gaps and, if necessary, to identify supplementary measures. Furthermore, based on ISO/IEC 27001 Chapter 6.1.3 d, it is necessary to adapt the SoA to the new structure and carry out checks regarding the applicability of the controls. To realize the mapping table, the following steps must first be performed:

The first step is to harmonize the two standards. This requires rewriting the SoA. The existing controls of ISO/IEC 27001:2013 must be mapped to the respective new controls of ISO/IEC 27001:2022. After mapping the two standards, the next step is to add the 11 new controls to the SoA and validate their applicability. This means that the mechanisms and measures already implemented must be compared in detail with the new ISO/IEC 27001:2022 and ISO/IEC 27002:2022 controls. New measures and controls must also be checked for applicability and may require additional measures to be taken (e.g., changes to the guidelines).

In order to use the SoA, the following operational steps must now be followed: The SoA ISO/IEC 27001:2022 artifact has already harmonized the two standards (2013 and 2022) (Figure 5). In order to determine the applicability, the applicability must first be defined as "Yes/No" in the "Status level" section under the "Applicability" column value. Here it is also possible to define the "Degree of Implementation" (Figure 6).

In the second step, the reasons why a control is implemented or not implemented must be listed under the heading "Reasons". The column value "Reasons for applicability / non-applicability" is followed by the entry of the existing documents, which can be recorded under the heading "document level".

In the last column, under the heading "Reasonability level", you can specify the owner of the control and the persons responsible for creating the documentation, updating and reviewing the assigned control (Figure 6). The following figures show the structure of the SoA ISO/IEC 27001:2022, which is linked and harmonized with the previous version 2013.

Confidentiality: Internal

Statement of Applicability ISO/IEC 27001:2022

	ISO/IEC 27001:2013	Control Level	ISO/IEC 27001:2022	Cause Assignment	Control Level
	Annex A nummeric	Control Name ISO/IEC 27001:2013	Annex A nummeric	Cause	Control Name ISO/IEC 27001:2022
A.5 Information security policies	A.5.1.1	Policies for information security	5.1	Organization Control	Policies for information security
	A.5.1.2	Review of the policies for information security			
A.6 Organization of information security	A.6.1.1	Information security roles and responsibilities	5.2	Organization Control	Information security roles and responsibilities
	A.6.1.2	Segregation of duties	5.3	Organization Control	Segregation of duties
	A.6.1.3	Contact with authorities	5.5	Organization Control	Contact with authorities
	A.6.1.4	Contact with special interest groups	5.6	Organization Control	Contact with special interest groups
	A.6.1.5	Information security in project management	5.8	Organization Control	Information security in project management
	A.6.2.1	Mobile device policy	8.1	Technological Control	User endpoint devices
	A.6.2.2	Teleworking	6.7	People Control	Remote working
A.7 Human resource security	A.7.1.1	Screening	6.1	People Control	Screening
	A.7.1.2	Terms and conditions of employment	6.2	People Control	Terms and conditions of employment
	A.7.2.1	Management responsibilities	5.4	Organization Control	Management responsibilities
	A.7.2.2	Information security awareness, education and training	6.3	People Control	Information security awareness, education and training
	A.7.2.3	Disciplinary process	6.4	People Control	Disciplinary process
	A.7.3.1	Termination or change of employment responsibilities	6.5	People Control	Responsibilities after termination or change of employment
A.8 Asset management	A.8.1.1	Inventory of assets	5.9	Organization Control	Inventory of information and other associated assets
	A.8.1.2	Ownership of assets	5.9	Organization Control	Inventory of information and other associated assets
	A.8.1.3	Acceptable use of assets	5.10	Organization Control	Acceptable use of information and other associated assets
	A.8.1.4	Return of assets	5.11	Organization Control	Return of assets
	A.8.2.1	Classification of information	5.12	Organization Control	Classification of information
	A.8.2.2	Labelling of information	5.13	Organization Control	Labelling of information
	A.8.2.3	Handling of assets	5.10	Organization Control	Acceptable use of information and other associated assets
	A.8.3.1	Management of removable media	7.10	Physical Control	Storage media
	A.8.3.2	Disposal of media			
	A.8.3.3	Physical media transfer			
A. 9 Access control	A.9.1.1	Access control policy	5.15	Organization Control	Access control
	A.9.1.2	Access to networks and network services		Organization Control	

Fig. 5. Harmonized SOA ISO/IEC 27001:2013 with ISO/IEC 27001:2022 Part I

Status Level		Reasons	Document level	Reasonability level	
Applicability	Degree of implementation	Reasons for applicability / non-applicability	Reference document	Responsible	Process owner
Please select an element	Please select an element				
Please select an element	Please select an element				
Please select an element	Please select an element				
Please select an element	Please select an element				
Please select an element	Please select an element				
Please select an element	Please select an element				
Please select an element	Please select an element				
Please select an element	Please select an element				
Please select an element	Please select an element				
Please select an element	Please select an element				
Please select an element	Please select an element				
Please select an element	Please select an element				
Please select an element	Please select an element				
Please select an element	Please select an element				
Please select an element	Please select an element				
Please select an element	Please select an element				
Please select an element	Please select an element				
Please select an element	Please select an element				
Please select an element	Please select an element				
Please select an element	Please select an element				
Please select an element	Please select an element				
Please select an element	Please select an element				
Please select an element	Please select an element				
Please select an element	Please select an element				
Please select an element	Please select an element				

Fig. 6. Harmonized SoA ISO/IEC 27001:2013 with ISO/IEC 27001:2022 Part II

3.5. *Mapping Table ISO/IEC 27002:2022 and ISO/IEC 27019:2018*

To implement the controls of ISO/IEC 27001:2022, schematic reference is now made to the industry-wide implementation instructions of ISO/IEC 27002:2022. However, as already explained, the two standards listed are mutually compatible. The players in the energy industry must, however, extend and supplement these cross-industry implementation instructions of ISO/IEC 27002:2022 to the specific requirements of ISO/IEC 27019:2018, so that they are able to guarantee the specific state of the art in terms of the information security requirements for the SCADA systems, process control systems and the associated logical and physical assets.

In order to eliminate the incompatibility of the two standards 27002:2022 and 2019:2018, the implementation notes are referenced directly or, where a direct link is not possible, indirectly via a thematic approach.

The following steps must be taken into account: If a direct referencing is specified thematically, the contents can be embedded and supplemented one-to-one. In case of indirect linking, the thematic approach corresponds to the additional notes from the section "Addition Information" should be taken into account and embedded operationally. The rest of the procedure remains in the analogy to SoA ISO/IEC 27001:2022.

The following Figure 7 shows the structure of the mapping table of ISO/IEC 27002:2022 and ISO/IEC 27019:2018.

Confidentiality: **Internal**

Mappingtable ISO/IEC 27002:2022 and ISO/IEC 27019:2018

ISO/IEC 27019:2018	Control-Level	Linking scheme		ISO/IEC 27002:2022	Control Level
Cause nummeric	Control Name ISO/IEC 27019:2018	Are directly linkable to the requirements of ISO/IEC 27002:2022	Semantic approach	Cause nummeric	Control Name ISO/IEC 27001:2022
6.1.1	Information security roles and responsibilities	x		5.2	Information security roles and responsibilities
6.1.2	Segregation of duties	x		5.3	Segregation of duties
6.1.3	Contact with authorities	x		5.5	Contact with authorities
6.1.4	Contact with special interest groups	x		5.6	Contact with special interest groups
6.1.5	Information security in project management	x		5.8	Information security in project management
6.1.6	ENR - Identification of risks related to external parties		x	5.19	Information security in supplier relationships
6.1.7	ENR - Adressing security when dealing with customers		x	5.19	Information security in supplier relationships
6.2.1	Mobile device policy		x	8.1	User endpoint devices
6.2.2	Teleworking		x	6.7	Remote working

Fig. 7. Mapping table ISO/IEC 27002:2022 with ISO/IEC 27019:2018

5. Conclusion

The amendment of the ISO/IEC 27001 and 27002 standards entail a restructuring and adaptation of the measures for the introduction and operation of an ISMS. A major challenge is to transfer the existing SoA of ISO/IEC 27001:2013 into the new structure of ISO/IEC 27001:2022 and to combine it with the energy-specific requirements of ISO/IEC 27019:2018.

Basically, in addition to the name change, an update of the measures was also carried out. The original 114 controls were consolidated to 93 by the update. However, this consolidation should not be underestimated from an effort perspective. Many of the measures were combined or newly introduced. In particular, the structural approach has been renewed.

The 14 thematic areas were categorised. According to the new standard, there are now four overarching areas. These include: Organisational measures, technological measures, physical measures, personnel measures.

For existing certifications, this now means that companies have to adapt their existing ISO structure and design their SoA to the new standard. The mapping table can be used here Initial certifications will now be based on the new standard.

Thus, stakeholders in the energy industry and also other CRITIS are encouraged to access the artifacts presented in this paper "SoA ISO/IEC 27001:2022" and "Mapping Table ISO/IEC 27002:2022 and ISO/IEC 27019: 2018" to increase their efficiency in restructuring their documentary processes, reporting and future auditing process with respect to ISMS based on ISO/IEC 27001:2022 and to avoid long inefficient process times, as in the case of harmonization and synchronisation of the old and new ISO/IEC 27001.

The authors also make their artefacts available to the professional audience on demand via e.g. a personal/E-Mail contact.

References

ISO/IEC 27001:2022-10 (2022), "Information security, cybersecurity and privacy protection — Information security management systems — Requirements," Beuth Verlag, Berlin, Germany, pp. 1-19.

ISO/IEC 27002:2022-08 (2022), "Information security, cybersecurity and privacy protection — Information security controls" Beuth Verlag, Berlin, Germany, pp. 1-368.

ISO/IEC 27000:2020-06 (2020), "Information technology - Security techniques - Information security management systems - Overview and vocabulary (ISO/IEC 27000:2018)", Beuth Verlag, Berlin, Germany, pp. 1-43.

ISO/IEC 27019:2018-08 (2018), "Information technology - Security techniques - Information security controls for the energy utility industry (ISO/IEC 27019:2017)" Beuth Verlag, Berlin, Germany, pp. 1-89.

ISO/IEC 27001:2013 (2013), "Information security management systems- Requirements," Beuth Verlag, Berlin, Germany, pp. 1-19.

National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity," April 16, 2018, pp. 1-48.