WHITE PAPER

Combined Approach to Information Security Based on ISO 27001/2 and IEC 62443-2-1

Adelina-Elena Voicu

Secura
A BUREAU VERITAS COMPANY

Table of Contents

Combined approach to Information Security based on ISO 27001/2 and IEC 62443-2-1

The convergence and integration of information technology (IT) and operational technology (OT) take place at an accelerated pace. As the line between IT and OT is blurring, it has become imperative to reassess the way organizations approach Information Security in OT environments. The time to act is now.

1. Introduction

1.1 BRIDGING THE GAP – IT AND OT

Historically, OT systems were isolated from networks that ran IT systems; IT and OT cybersecurity were treated as separate issues. Recently, organizations have proceeded to integrate IT and OT infrastructure. This integration is driven by benefits such as richer real-time information sharing, constant monitoring of performance, improved uptime and a comprehensive overview of the industrial ecosystem. Nonetheless, traditional OT systems continue to leverage legacy technologies, can be rarely updated, have a long life cycle and often lack basic cybersecurity features.

Within industrial environments, many critical business processes depend on OT. Networks with Industrial Controls Systems (ICS) such as DCS, PLC and SCADA systems manage and automate critical processes. Still, IT services are just as necessary for daily operations. Moreover, due to the convergence of IT and OT, the dependency between these two environments is also increasing. Ultimately, a successful business depends on reliable systems in both IT and OT.

1.2 BUILDING A BUSINESS CASE FOR A TWO-PART APPROACH TO CYBERSECURITY IN OT ENVIRONMENTS

Cyber risks are increasingly important for organizations: a data breach, hack or even a ransomware attack can have a considerable impact. Companies often do not have a good overview of their information systems and the cyber resilience within their organization. To address this issue, organizations can choose to strengthen information security by establishing policies and procedures based on ISO/IEC 27001/2 standards, which cover both IT and OT. In certain cases, organizations can either choose to address their OT infrastructure under the same management system, based on ISO/IEC 27001/2 or to build their own CSMS based on ISA/IEC 62443-2-1. Nevertheless, the two standards, ISA/IEC 62443-2-1 and ISO/IEC 27001/2, address complementary parts of information security, hence they can work perfectly well once combined. Even though ISA/IEC 62443-2-1 is inspired from ISO/IEC 27001, there might exist topics that are not covered by ISA/IEC62443-2-1 but are still relevant within the management systems of OT-oriented organizations.

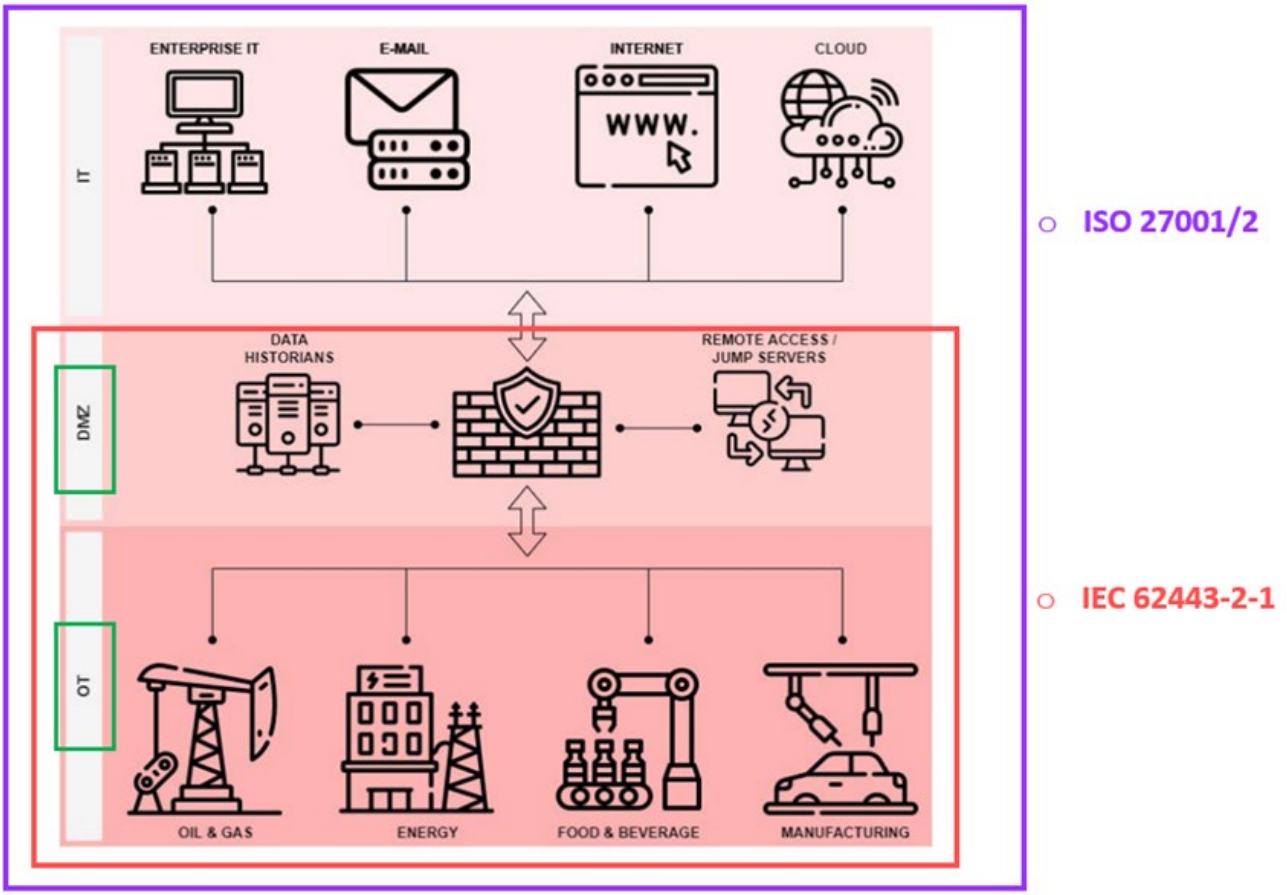


Figure 1: Two-part approach to information security

Consider, for example, a company with IT and OT infrastructures of operating facilities. Moreover, suppose said company undergoes an assessment to evaluate its cybersecurity maturity and resilience with a focus on assessing the security of the production environment and facilities. Let's imagine that during this assessment, an assessor made an observation where printed papers containing sensitive information were found in the printer. This printer was located in the area that guests can access unattended, meaning they can easily get access to sensitive information without the need to perform any technical attacks. An assessment based on the best practice industry standard for OT (ISA/IEC 62443-2-1), does not have any questions regarding this part, and as such, the risk remains undetected. However, an approach based on the combination of ISA/IEC 62443-2-1 and ISO/IEC 27001/2 addresses this issue within the clear desk and clear screen policy control in ISO/IEC 27001/2. At the same time, performing two separate assessments, one for ISO/IEC 27001/2 and one for ISA/IEC 62443-2-1, entails evaluating similar controls and as such, requires more time and effort. This finding, thus, highlights the importance of conducting a coordinated approach in selecting relevant controls and ensuring compliance by combining ISO/IEC 27001/2 and ISA/IEC 62443-2-1 requirements and controls.

2. Background

2.1 PRELIMINARIES

2.1.1 Information technology

Information Technology (IT) refers to "any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency" **[1]**.

2.1.1 Information technology

Operational Technology (OT) encompasses "a broad range of programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment)" **[2]**.

2.1.3 Different technologies, different needs

	Information Technology (IT)	Operational Technology (OT)
Information security property	Confidentiality – protect data from unauthorized access	Availability – performance, uptime 24/7/365
Focus	Data and flow of digital information	Industrial operations and machinery used to execute physical processes
Data/ assets [3]	Desktop and laptop computers, keyboards, printers, smartphones, data/ email servers	SCADA, PLC, DCS, I/O Hardened PCs
Scanning and Patching	Regularly	Rarely
Antivirus	Common	Uncommon
Upgrades	Automatically done, scheduled during uptime	Must be planned and tested, scheduled during downtime
Access control [4]	Strict network authentication	Strict physical access
Lifecycle	3-5 years	Decades
Operation environment [5]	Office, server room air-conditioned, dust-protected	Outside, weather, dirt, vibrations

2.1.4 Middle ground - IT/OT DMZ

An IT/OT DMZ separates the enterprise IT network and the OT network. Often, this level consists of generic IT components, but it could also contain specific OT-related applications, including specific OT communication protocols, like Modbus, OPC, or OPC-UA. Examples include remote access servers, patch update distribution servers, and data historian servers. It is often a crucial layer as this is one of the first layers of defense of the underlying OT systems.

2.2 STANDARDS

2.2.1 ISO 27001/2 provides requirements for establishing, implementing, maintaining and improving an ISMS

The ISO/IEC 27000 family of standards, also known as the ISO 27000 series currently consists of individual standards developed and maintained jointly by the international standards bodies: ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). The family of standards is broad in scope and enables organizations of all types, sizes or nature to manage their information security.

ISO/IEC 27001 provides requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS) as well as a list of commonly accepted controls to be used as a reference for establishing security requirements **[6]**. The second edition of the standard, published in 2013, revises the previous edition published in 2005. In addition, ISO/IEC 27002:2017 provides detailed guidance on implementing the information security controls listed in ISO/IEC 27001, Annex A. A new edition of this standard, ISO/IE 27002:2022, which revises the ISO/IEC 27002:2017 edition, was published in March 2022. Both ISO/IEC 27001:2013 and ISO/IEC 27002:2022 are the reference standards organizations employ to achieve certification. In the remainder of this document, we will refer to the two standards as ISO 27001 and ISO 27002.

ISO 27001 comprises of ten sections, known as clauses. The first three clauses (Scope, Normative references, Terms and definition) are introductory, whereas the following clauses, four to ten, are mandatory for any organization seeking certification.

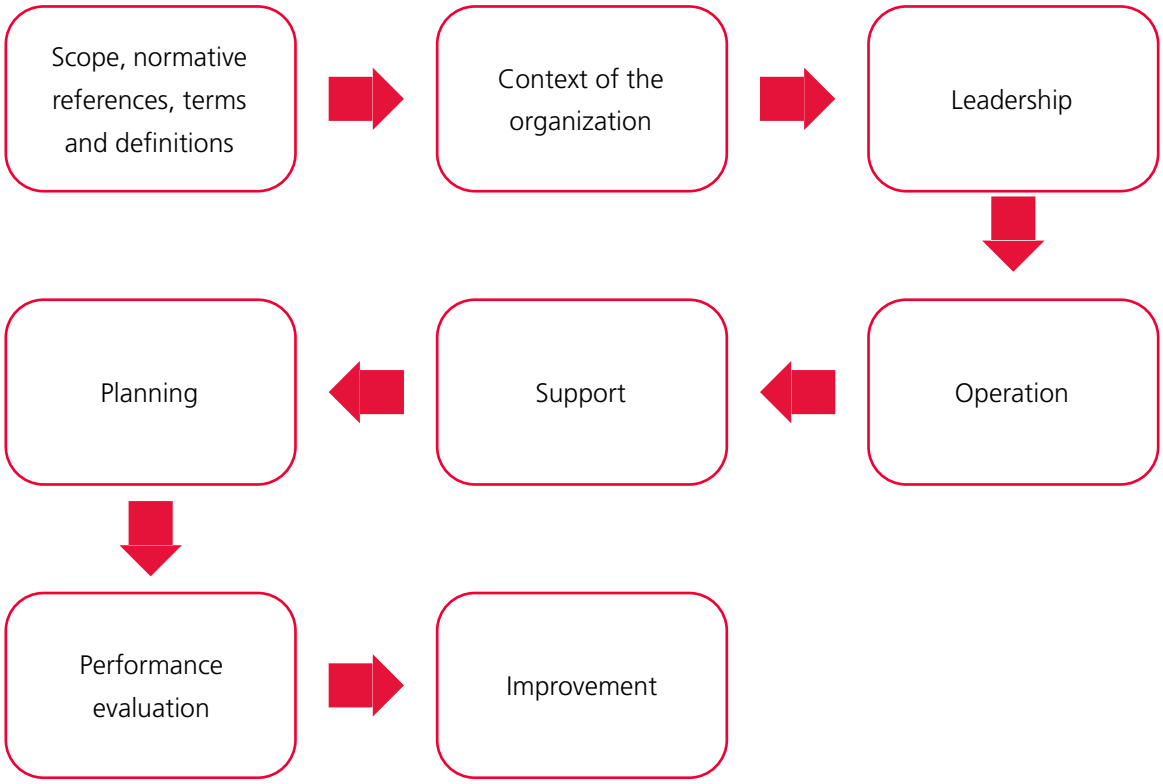


Figure 2: ISO 27001 structure

In February 2022, ISO 27002:2013 was withdrawn and revised by ISO 27002:2022 Information security, cybersecurity and privacy protection — Information security controls **[7]**. The latest version contains all controls listed in ISO 27001, Annex A, however, some controls have been merged and several new controls have been introduced. The latest version of the standard comprises eight clauses and two annexes, as depicted in Figure 2.

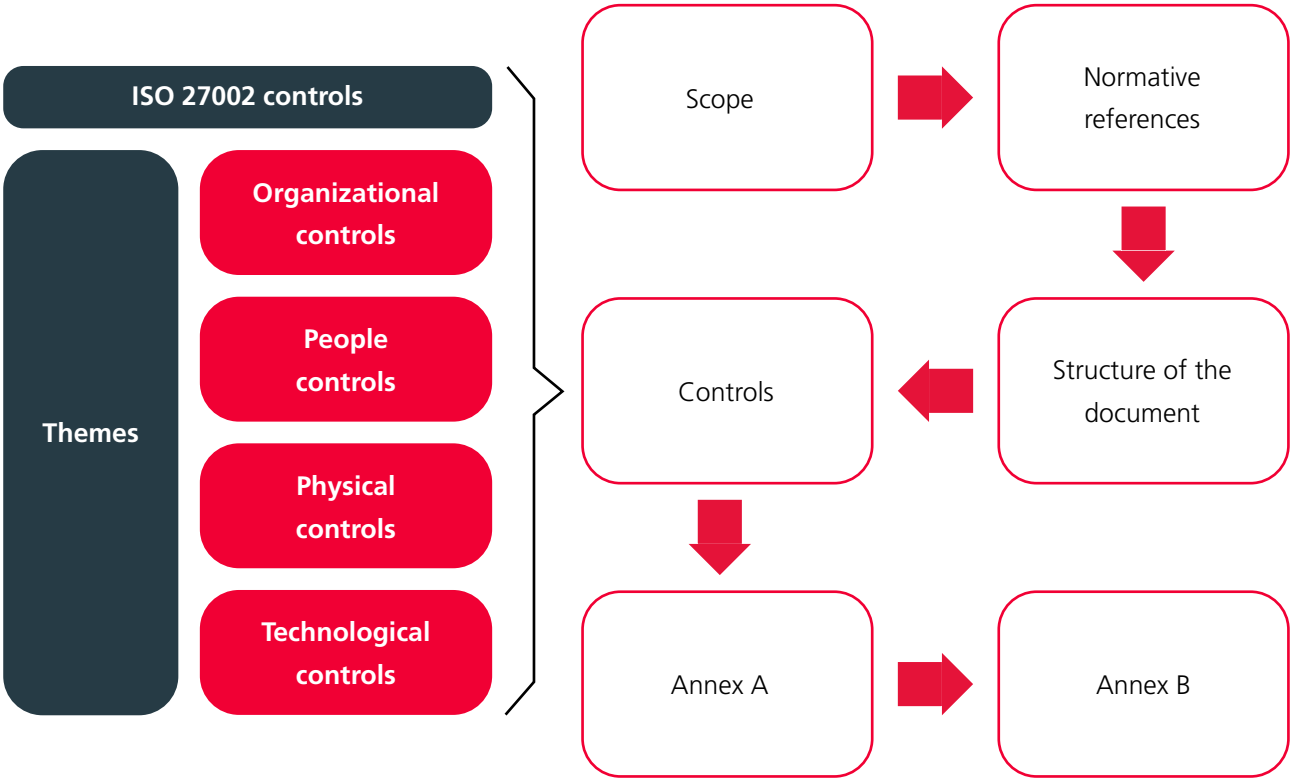


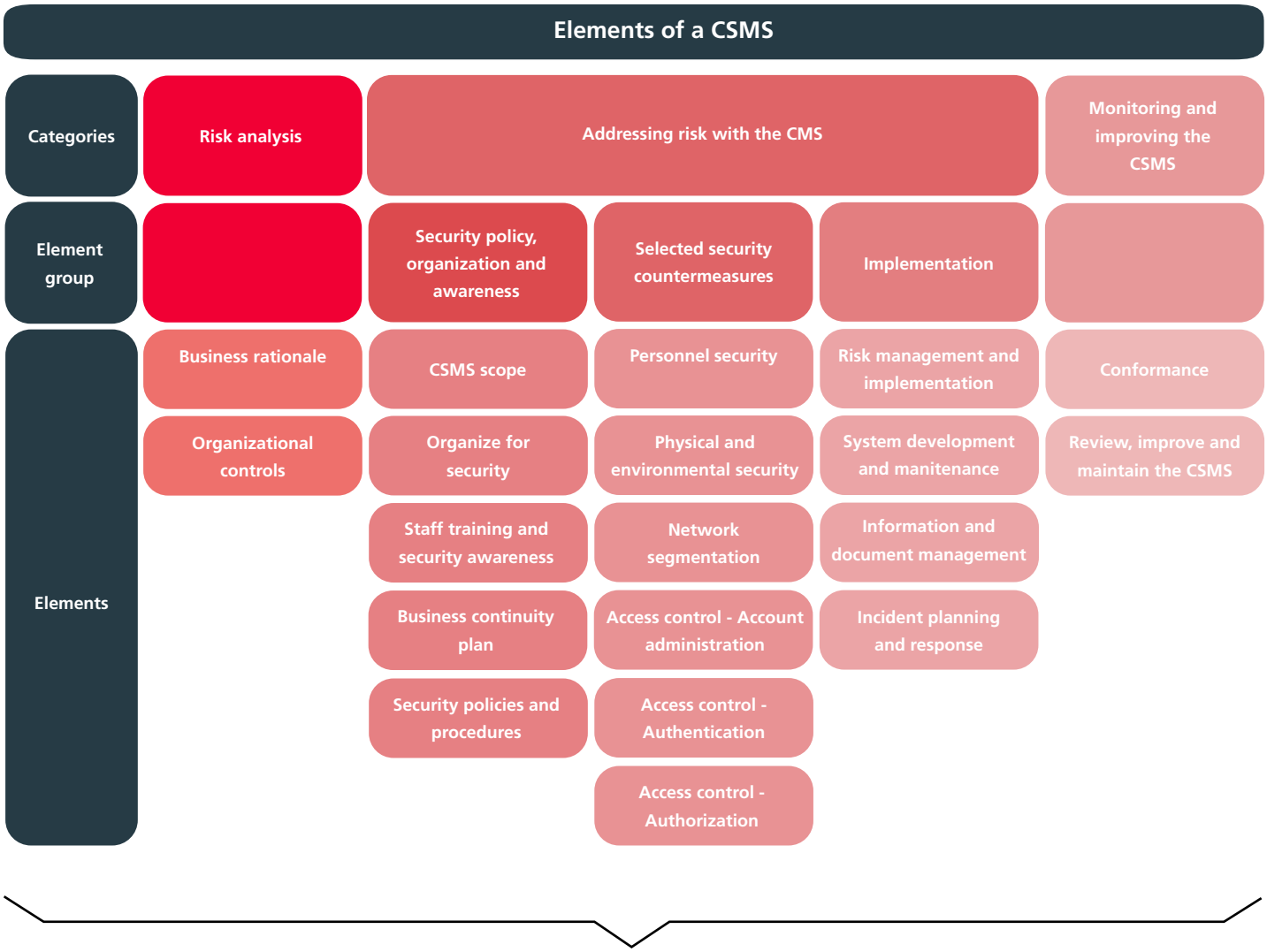
Figure 3: ISO 27002 structure

Clauses five to eight detail 93 controls, organized in four themes: people, physical, technology and organizational. Annex A explains how an organization can use attributes to create its own views based on the control attributes defined in this document or of its own creation, whereas Annex B presents the correspondence between the controls in this edition of ISO 27002 and the previous edition.

2.2.2 IEC 62443-2-1 addresses asset owners responsible for establishing security programs

The ISA/IEC 62443 series of standards, also known as the IEC 62443 series, consists of standards developed jointly by the International Electrotechnical Commission (IEC) and the ISA99 to address and mitigate security vulnerabilities in Industrial Automation and Control Systems (IACS) **[8]**. The series is structured in four layers entitled: General, Policies and procedures, System and Component **[9]**.

IEC 62443-2-1 **[10]** belongs to the second part of the IEC 62443 family of standards, **Policies and procedures** and focuses on establishing an industrial automation and control system security program. IEC 62443-2-1 comprises four clauses and three annexes, as depicted in Figure 3. Inspired by ISO 27001, IEC 62443-2-1 only focuses on topics that differ within IT and OT environments but does not cover the whole set of requirements for Information Security Management System (ISMS) for companies.



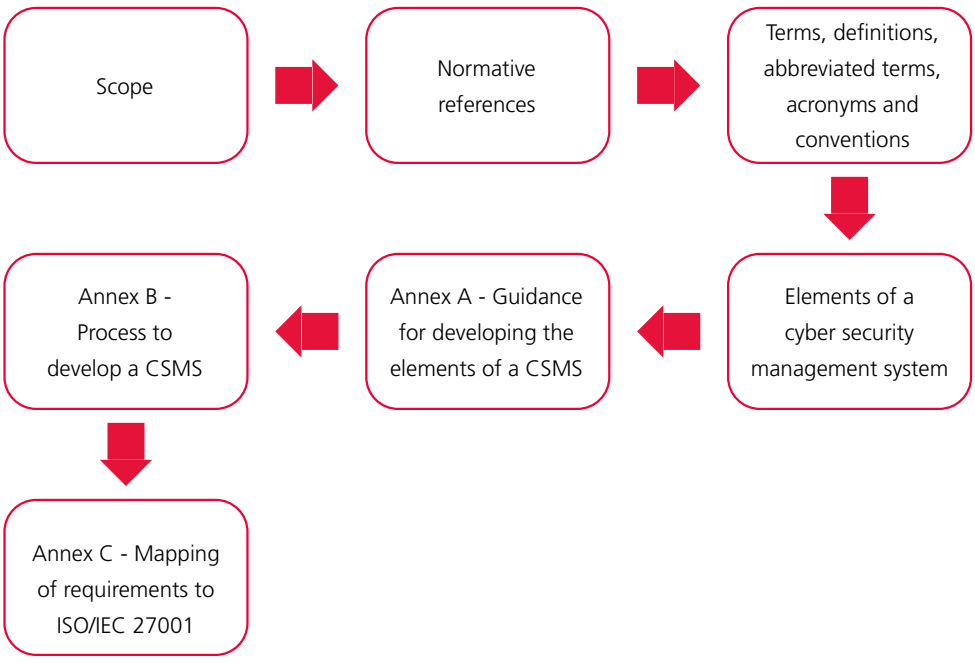


Figure 4: Elements of a CSMS

Clause 4, Elements of a cybersecurity management system, presents 126 requirements in three categories: risk analysis, addressing risk with the CSMS and monitoring and improving the CSMS. Each of the three categories is further divided into element groups and elements, with a total of nineteen elements and three element groups. The first category, risk analysis, consisting of two elements, defines an organization's cyber risk needs, identifies them and assesses their likelihood.

The second category consists of three element groups, which comprise five, six and four elements, respectively. The category discusses the development of cyber security policies, including staff training and business continuity, how to select and implement security countermeasures: physical, personnel and network security, as well as access control.

The third and last category, monitoring and improving the CSMS, consists of two elements and its purpose is to ensure the employees adhere to the established policies and the CSMS operates as defined so that the organization meets its goals, policies and procedures.

Finally, each element in turn comprises: the objective of the element, a basic description of the element, a rationale to explain why the element is included and the requirements for that element. Further guidance on how to implement the requirements is provided in Annex A, detailing for each element: a description, element-specific information, supporting practices, baselines practices, additional practices and resources used.

3. ISO 27001/2 and IEC 62443-2-1 should be combined to ensure robust coverage of cyber risks in OT Environments

In recent years, the boundaries between IT and OT have been blurring. Threat actors have begun to leverage IT-based techniques to access OT systems. To address this issue, organizations need to employ a coordinated approach in selecting relevant controls to ensure cyber resilience.

Below, a high-level approach for combining ISO 27001/2 focusing on IT/OT and IEC 62443-2-1 focusing on OT is presented.

3.1 ESTABLISH A MANAGEMENT SYSTEM AND ADAPT IT FOR THE OT INFRASTRUCTURE

When the asset owner employs a formal ISMS to protect the IT system, the asset owner shall ensure that the security program of the IACS is coordinated with the ISMS to ensure a defense-in-depth strategy for the IACS **[11]**.

3.2 HOW TO APPLY ISO 27001/2 AND IEC 62443-2-1 IN OT ENVIRONMENTS

To combine ISO 27001/2 and IEC 62443-2-1, the following steps should be followed:

- Find the common controls in ISO 27001/2 and IEC 62443-2-1
- Find the controls in ISO 27001/2 which cannot be mapped to IEC 62443-2-1
- Find the requirements in IEC 62443-2-1 which cannot be mapped to ISO 27001/2
- Find the clauses in ISO 27001 which cannot be mapped to IEC 62443-2-1

3.2.1 Phase 1: Find the common controls in ISO 27001/2 and IEC 62443-2-1

One practical way to identify the common controls in ISO 27001/2 and IEC 62443-2-1 is to leverage the structure of IEC 62443-2-1. For each element in IEC 62443-2-1, the search for corresponding controls in ISO 27002 and corresponding clauses in ISO 27001 should be done at different levels of abstraction, including:

- the requirements listed for each element in IEC 62443-2-1;
- the subclauses providing detailed guidance specific to each element;
- the baseline practices listed per element;
- the additional practices listed per element.

To map the common controls, combined approach to Information security based on ISO 27001/2 and IEC 62443-2-1 considers requirements - title and text - and baseline practices. The methodology requires that for each element, the corresponding controls in ISO 27002 and clauses in ISO 27001 be identified based on keywords (nouns and verbs) and synonymous terminology.

Finally, the proposed approach recommends adding controls in ISO 27002 resulting from additional practices and detailed guidance in the information gap between ISO 27002 and IEC 2443-2-1 i.e., controls in ISO 27002 that cannot be mapped to IEC 62443-2-1.

3.2.2 Phase 2: Find the requirements in IEC 62443-2-1 which cannot be mapped to ISO 27001/2

Combined approach to Information Security based on ISO 27001/2 and IEC 62443-2-1 allows to simultaneously identify which requirements in IEC 62443-2-1 have a correspondence in ISO 27001/2 and which requirements in IEC 62443-2-1 cannot be mapped to ISO 27001/2. Based on the common controls identified in the previous step, the approach allows to further define a more granular correspondence by adding to each requirement the related controls and clauses. Although most of the controls in

ISO 27002 are related to one or more requirements, some can still be of general nature or can result from baseline practices. These shall still be listed as corresponding requirements and a motivation shall be provided. The requirements for which no security controls and clauses are listed form the information gap.

Although a correspondence between controls can be identified, the level of detail of one requirement may extend beyond the level of detail of the corresponding requirement in the other standard. This may simultaneously result in an overlap and in a coverage gap. Whenever a coverage gap arises, it shall be explained. Additionally, whenever the implementation of a corresponding control in ISO 27002 may conflict with OT considerations, the conflict shall be addressed.

3.2.3 Phase 3: Find the controls in ISO 27002 which cannot be mapped to IEC 62443-2-1

The Combined Approach to Information Security based on ISO 27001/2 and IEC 62443-2-1 recommends adding controls in ISO 27002 resulting from additional practices and detailed guidance in the information gap between ISO 27002 and IEC 2443-2-1 i.e., controls in ISO 27002 that cannot be mapped to IEC 62443-2-1. In addition, the methodology requires that for each control in ISO 27002, the corresponding elements identified in the first step be listed. The controls for which no element is listed form the information gap.

3.2.4 Phase 4: Find the clauses in ISO 27001 which cannot be mapped to IEC 62443-2-1

The proposed approach requires that for each control in ISO 27002, the corresponding elements identified in the first step be listed. The clauses (sub-clauses and sub-subclauses) for which no element is listed form the information gap.

3.3 ADAPT THE ADDITIONAL CONTROLS IN ISO 27001/2 FOR OT ENVIRONMENTS

After completion of Phase 3: Find which controls in ISO 27002 cannot be mapped to IEC 62443-2-1, the additional controls in ISO 27002 shall be examined. Areas of potential conflicts should be identified and addressed such that the controls apply to OT environments. In addition, concepts and terminology from both standards shall be used consistently **[11]**.

4. Outcome

Table 1 depicts how to find the common controls in ISO 27001/2 and IEC 62443-2-1 according to the first step in the proposed approach.

Category	Element group	Element	ISO 27001	ISO 27002
Risk analysis	->	Business rationale	6.2 Information security objectives and planning to achieve them	5.1 Policies for information security
Risk analysis	->	Risk identification, classification and assessment	6.1.2 Information security risk assessment 8.2 Information security risk assessment	5.9 Inventory of information and other associated assets 5.14 Information transfer 5.25 Assessment and decision on information security events 5.33 Protection of records 8.8 Management of technical vulnerabilities 8.19 Installation of software on operational systems 8.20 Networks security (ISO 27002) c) 5.12 Classification of information
Addressing risk with the CSMS	Selected security countermea-sures	Physical and environmental security	None	5.11 Return of assets 7.1 Physical security perimeters 7.2 Physical entry 7.3 Securing offices, rooms and facilities 7.4 Physical security monitoring 7.5 Protecting against physical and environmental threats **7.6 Working in secure areas[1]** 7.8 Equipment siting and protection **7.9 Security off-premises[2]** 7.10 Storage media 7.11 Supporting utilities 7.12 Cabling security 7.13 Equipment maintenance 7.14 Secure disposal or re-use of equipment

Table 1: Mapping of common controls

[1]Resulting from Physical and environmental security (additional practices and clauses)

[2]Resulting from Physical and environmental security (additional practices and clauses)

Table 2 illustrates how to find the controls which are present in IEC 62443-2-1, but not in ISO 27002. Note that the controls listed in the column "Subclauses and additional practices" are included for completeness, but form the information gap between ISO 27002 and IEC 62443-2-1.

Element	IEC 62443-2-1	ISO 27001	ISO 27002	Remarks	Subclauses and additional practices
Risk identification, classification and assessment	4.2.3.5 Develop simple network diagrams	-	8.20 Networks security	Guidance c) maintaining up to date documentation including network diagrams and configuration files of devices (e.g. routers, switches); page 111	
Personnel security	4.3.3.2.7 Segregate duties to maintain appropriate checks and balances	-	5.3 Segregation of duties	6.4 Disciplinary process and 6.6. Confidentiality or non-disclosure	
Physical and environmental security	4.3.3.3.10 Establish procedures for the interim protection of critical assets	-	No corresponding control/ clause	7.11 Supporting utilities based on A.3.3.3.3.1 Baseline practices b), d) -> corresponds to the element	7.6 Working in secure areas, 7.9 Security off-premises result from A.3.3.3.2.3 Security perimeter, A.3.3.3.2.13 Use of assets outside controlled environments
System development and maintenance	4.3.4.3.8 Establish and document antivirus/malware management procedure	-	8.7 Protection against malware		

Table 2: Information gap between IEC 62443-2-1 and ISO 27001/2

Table 3 exemplifies how to find the information gap between ISO 27002 and IEC 62443-2-1 i.e. the controls present in ISO 27002, but not in IEC 62443-2-1.

Category	Control #	Control title	Mapped/ Information gap	Element(s) in IEC 62443-2-1
Organizational controls	5.3	Segregation of duties	Yes	Personnel security, System development and maintenance
People controls	6.1	Screening	Yes	Personnel security
Physical controls	7.7	Clear desk and clear screen	Information gap	
Technological controls	8.17	Clock synchronization	Information gap	

Table 3: Information gap between ISO 27002 and IEC 62443-2-1

Finally, Table 4 illustrates how to find the information gap between ISO 27001 and IEC 62443- 2-1.

Clause	Subclause	Sub-subclause	Element in IEC 62443-2-1	Requirement in IEC 62443-2-1
4 Context of the organization	4.1 Understanding the organization and its context			
6 Planning	6.1 Actions to address risks and opportunities	6.1.2 Information security risk assessment	Risk identification, classification and assessment	4.2.3.1 Select a risk assessment methodology 4.2.3.3 Conduct a high-level risk assessment 4.2.3.6 Prioritize systems 4.2.3.7 Perform a detailed vulnerability assessment 4.2.3.8 Identify a detailed risk assessment methodology 4.2.3.9 Conduct a detailed risk assessment 4.2.3.11 Integrate physical, HSE and cyber security risk assessment results 4.2.3.12 Conduct risk assessments throughout the lifecycle of the IACS 4.2.3.13 Document the risk assessment
			Risk management and implementation	4.3.4.2.1 Manage IACS risk on an ongoing basis

Table 4: Information gap between ISO 27001 and IEC 62443-2-1

5. OT Security Maturity review extended

Secura defined two approaches to OT cybersecurity based on international standards IEC 62443-2-1 and ISO 2700/2. The approaches are applicable for asset owners and cover the establishment and implementation of a management system. The second approach, OT Security Maturity Review Extended is built on international standards IEC 62443-2-1 and ISO 27001/2 following the process described in this whitepaper. By including all requirements in IEC 62443-2-1 and in addition, controls that are not found in IEC 62443-2-1, but are fully applicable to IT and OT, the framework ensures a robust approach to information security. The outcome of this service is clear insight into the current maturity scoring and an indication of which control improvements help most raising the current maturity level to the desired level. These measures are formulated high level, with aim to report the most important to involved Senior Management. Recommendations are prioritized based on the risk profile and the maturity scoring.

More information can be found at: **secura.com**

6. Conclusion

To conclude, due to recent IT/OT convergence and integration developments organizations must employ a coordinated approach to ensure cyber resilience in OT environments. Combined Approach to Information Security based on ISO 27001/2 and IEC 62443-2-1 provides cyber risks coverage by highlighting both common controls and controls/guidance that are fully common to IT and OT and are not found in ISA/IEC 62443.

In addition, the proposed solution facilitates an understanding of when compliance with one standard can be extended to compliance with another and may be used to simplify the process of achieving certification for multiple standards.

7. References

[1] NIST Information Technology Laboratory Computer Security Resource Center. https://csrc.nist.gov/glossary/term/information_technology. Accessed on [14.04.2022]

[2] NIST Information Technology Laboratory Computer Security Resource Center. https://csrc.nist.gov/Projects/operational-technology-security. Accessed on [14.04.2022]

[3] 2020. Information Technology and Operations Technology: Beyond Convergence. International Society of Automation, p.2. Accessed on [24.06.2022]

[4] 2020. Information Technology and Operations Technology: Beyond Convergence. International Society of Automation, p.3. Accessed on [24.06.2022]

[5] Fluchs, S., 2020. Why OT has different needs than IT. [online] Medium. Available at: https://fluchsfriction.medium.com/why-ot-has-different-needs-than-it-18ba9baa36e7 [24.06.2022].

[6] Global Cybersecurity Alliance. 2021. Applying ISO/IEC 27001/2 and the ISA/IEC 62443 Series for Operational Technology Environments. Accessed on [22.01.2022]

[7] ICS>35>35.30. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. https://www.iso.org/standard/75652.html. Accessed on [29.04.2022]

[8] ISA. New ISA/IEC 62443 standard specifies security capabilities for control system components. https://www.isa.org/?aspxerrorpath=%2fintech-home%2f2018%2fseptember-+october%2fdepartments%2fnew-standard-specifies-security-capabilities-for-+c%3a+%3atext%3dThe+ISA%-2fIEC+62443+series&aspxerrorpath=and+control+systems+(IACSs)
Accessed on [09.05.2022]

[9] IEC 62443 Background. https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/iec-62443/ Accessed on [09.05.2022]

[10] IEC. 2010. IEC 62443-2-1. Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program. 1st ed. ISBN 978-2-88912-037-6. Accessed on [09.05.2022]

[11] ISA. Whitepaper. July 2021. Applying ISO/IEC 27001/2 and the ISA/IEC 62443 Series for Operational Technology Environments, p.6. Accessed on [14.04.2022]

About Secura

Secura has worked in information security and privacy for over two decades. This is why we uniquely understand the challenges that you face like no one else and would be delighted to help you address your information security matters efficiently and thoroughly. We work in the areas of people, processes and technology. For our customers we offer a range of security testing services varying in depth and scope.

Secura has the mission to support organizations with up-to-date knowledge to work toward a bright and safe future.

Keep updated with the latest insights on digital security and subscribe to our periodical newsletter.

Follow us on:

Contact us today at info@secura.com or visit secura.com for more information.

SUBSCRIBE

TO OUR NEWSLETTER

Secura
A BUREAU VERITAS COMPANY

BUREAU VERITAS
Shaping a World of Trust