Mapping of OES Security Requirements to Specific Sectors

DECEMBER 2017

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For queries in relation to this paper, please use resilience@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN 978-92-9204-232-5, DOI 10.2824/844702

Table of Contents

Executive Summary

According to the Directive (EU) 2016/1148 issued by the European Parliament and the Council, hereafter referred to as 'Network and Information Security (NIS) Directive', specific types of entities which provide essential services to the European internal market, shall be identified by the Member States. The business sectors for these entities are depicted in Annex II of the NIS Directive.

One of the main objectives of the NIS Directive is to enact security measures for operators of essential services (OES) across the European Union, in order to achieve a high common level of Security of Network and Information Systems.

The current report provides a substantial and comprehensive mapping of the security requirements for OES, as they have been agreed in the NISD Cooperation Group, to sector specific information security standards. Initially, ENISA conducted desktop research on international security standards, guidelines and good practices per sector. Finally, the security requirements for OES were mapped to international standards used by operators covering all business sectors under scope. This report is a living document that we will augment on a regular basis to keep it up to date with the latest developments.

1 Introduction

This report provides the mapping of security measures for OES to international standards used by operators in the business sectors mentioned in Annex II of the NIS Directive[1], namely energy, transport, banking, financial market infrastructures, health, drinking water supply & distribution and digital infrastructures.

The current report involves the security requirements for OES, as they have been defined in the specific work stream of the Cooperation Group of the NIS Directive, and they are presented in details in ENISA's deliverable "Baseline Security Requirements for OES". The mapping of security requirements for OES to specific sector standards contributes to achieving a common and converged level of security in network and information systems (Article 3 of the NIS Directive) at EU level. This report is a 'living document' that we will augment on a regular basis to keep it up to date with the latest developments.

It is important to note that the security measures described in this document derived from the work performed under the specific work stream of the NIS Directive Cooperation Group for the security measures for OES. The proposed security measures are not intended to replace existing standards, frameworks or good-practices in use by OES. However, operators could map the standards they use (internally) to the proposed security measures, and in this way assess their information security practices against the requirements adopted by the Cooperation Group.

1.1 Background

The NIS Directive was adopted by the European Parliament on the 6th of July, 2016 and entered into force in August 2016. Member States have 21 months to transpose the Directive into their national legislation and 6 more months to identify operators of essential services.

The ultimate goal of the NIS Directive is to ensure a culture of network and information systems security across sectors (i.e. energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure), vital for our society and economy and heavily dependent on ICT (Article 5 §2-b, NISD). The operators identified by the Member States as OES should take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations (Article 14 §1, NISD). Therefore, this mapping contributes to the establishment of a harmonised baseline security level of OES across EU.

1.2 Target Audience

The intended audience of this report consists of the OES as well as the public authorities for the following (sub)sectors:

- **Energy**
  - Electricity
  - Oil

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

    - Gas
- **Transport**
    - Air Transport
    - Rail Transport
    - Water Transport
    - Road Transport
- **Banking**
- **Financial Market Infrastructures**
- **Health**
- **Drinking Water Supply & Distribution**
- **Digital Infrastructures**

1.3 Goal and Scope of the report

The main goal of this report is to associate the security requirements for OES, adopted by the Cooperation Group, with information security standards applicable to the sectors of interest as mentioned above and referred to in the Annex II of the NIS Directive. In order to achieve a common, baseline, cross-sector (horizontal) framework of security measures for the OES at EU level, the security requirements for the OES are primarily mapped to the most frequently used international information security standards by operators in each of these sectors.

1.4 Methodology

Initially, ENISA conducted a desktop research of international information security standards, guidelines and good practices, relevant to security measures applicable by OES of the business sectors in scope. The final output of the desktop research is contained in the **tables [Table** 1**,Table** 2**,Table** 4**,Table** 6**,Table** 8**,Table** 9**, Table** 11**, Table** 12**, Table** 14**, Table 16 ,Table** 17 **]**, depicting the existing information security standards and good practices for each sector, as found in **section 2**.

The next step of the methodology was to map the identified and agreed by the Cooperation Group security measures for OES to the most commonly applicable sector specific standards by the operators of the business sectors.

Finally, the security measures were mapped to the three (3) most frequently used international standards, across all the sectors of interest, as found below:

- **ISO 27001**
  ISO/IEC 27001[2], part of the growing ISO/IEC 27000 family of standards, is an Information Security Management Systems (ISMS) standard published in October 2013 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO/IEC 27001 formally specifies a management system that is intended to bring information security under explicit management control.

[2] https://www.iso.org/isoiec-27001-information-security.html

- **ANSI ISA/IEC 62443**[3]
  ISA (International Society of Automation) and IEC have developed the IEC 62443[4] series of standards in order to address the need to design cybersecurity robustness and resilience into industrial automation control systems (IACS). The concept of industrial automation and control systems electronic security is applied in the broadest possible sense, encompassing all types of plants, facilities, and systems in all industries. IEC 62443 targets people, processes, systems, solutions and components/products.
- **NIST Framework for Improving Critical Infrastructure Cybersecurity**[5]
  This Framework[6] enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. The Framework provides structure to today's multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today. Moreover, because it references globally recognized standards for cybersecurity, the Framework can also be used by organizations located outside the United States and can serve as a model for international cooperation on strengthening critical infrastructure cybersecurity.

The above standards were selected according to:

- the results of the survey that was filled in by the representatives of EU Member States, in the Cooperation Group. The survey was launched on 6th March 2017 and it was active until 15th May 2017. More specifically, ISO 27001 was emerged by the survey as the most commonly followed standard.
- the input provided during phone interviews by EU operators in the sectors; referred to the NIS Directive. More specifically,
  - ANSI ISA/IEC 62443 is the most applicable international standard for IACS (Industrial Automation and Control Systems), as they constitute the core components of the OES;
  - NIST Cybersecurity Framework is followed by some European utilities which operate in U.S. and therefore they need a common denominator and ground policy.

[3] These documents were originally referred to as ANSI/ISA-99 or ISA99 standards, as they were created by the International Society for Automation (ISA) and publicly released as American National Standards Institute (ANSI) documents. In 2010, they were renumbered to be the ANSI/ISA-62443 series. This change was intended to align the ISA and ANSI document numbering with the corresponding International Electrotechnical Commission (IEC) standards https://en.wikipedia.org/wiki/Cyber_security_standards

[4] https://www.isa.org/store/ansi/isa-62443-3-3-990303-2013-security-for-industrial-automation-and-control-systems-part-3-3-system-security-requirements-and-security-levels/116785

[5] The Version 1.0 of the NIST Cybersecurity Framework was taken into account for the mapping it, as the newest version of the framework is still in draft status.

[6] https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

2 Mapping of Baseline Security Measures for OESs per sector

With the adoption of the Directive on security of Network and Information Systems (NIS) in 2016, a baseline level of security in network and information systems is aimed to be achieved at EU level. This will support the broader vision of the EU Digital Single Market[7], whilst protecting the interests of the European society and the provision of essential services to European citizens.

The following subsections present the mapping of the proposed security measures by the NIS Directive Cooperation Group to industry specific standards that are usually applied by operators covering the sectors under scope.

2.1 Energy

The European Union's prosperity and security hinges on a stable and abundant supply of energy. As energy is a vital part of Europe's economy and of modern lifestyles, European citizens expect uninterrupted flows of energy and access to energy sources. Numerous policies have been introduced to secure and create a European sustainable energy network, like the NIS Directive. The NIS Directive distinguishes the subsectors of Electricity, Oil and Gas for the Energy sector.

Table 1 below, lists international standards and good practices applicable across all the Energy subsectors of interest. It is the outcome of the conducted desktop research and it is not an all-inclusive table, as it is mainly based on bibliography.

STANDARDS	GOOD PRACTICES
• **ISO 27001** Information technology — Security techniques — Information security management systems — Requirements • **ANSI/ISA, Series "ISA-62443**: Security for industrial automation and control system" • **NIST Framework for Improving Critical Infrastructure Cybersecurity**	• Detailed Measures – Cybersecurity for Industrial Control Systems – ANSSI (France) • Good Practice Guide Process Control and SCADA Security – CPNI • AMI System Security Requirements updated – UCAIUG: AMI-SEC-ASAP • BDEW whitepaper – Requirements for secure controls and telecommunications systems – Bundesverband der energie un Wasserwirtschaft • Information security baseline requirements for process control, safety and support ICT systems – OLF • Twenty Critical Controls for Effective Cyber Defence: Consensus Audit Guidelines • Catalog of Control Systems Security: Recommendations for Standards Developers – USA DHS • 21 Steps to Improve Cyber Security of SCADA Networks – US DOE

Table 1: International standards and good practices applicable across the Energy sector.

According to feedback provided by Energy operators, the most frequently applicable standards for the energy sector, in its entirety, are ISO 27001 and ISA/IEC 62443. The mapping of the security measures to the above listed standards is depicted in **section 3**, **Table 22.**

[7] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN

In the following subsections, electricity, oil and gas specific standards and good practices along with the mapping to the security measures are presented.

2.1.1 Electricity

Table 2 below, lists international standards and good practices applicable across the Electricity subsector.

SUB-SECTOR	STANDARDS	GOOD PRACTICES
Electricity	• **NIST SP800-82** Guide to Industrial Control Systems (ICS) Security • **ISO 27019** -- Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry • **NERC CIP Series** "Critical Infrastructure Protection Cyber Security": CIP–002 to CIP-011. • IEEE STANDARD 1402-2000 - IEEE Guide for Electric Power Substation Physical and Electronic Security • IEC 61850 - Power Utility Automation	• Cybersecurity model electricity subsector cybersecurity capability maturity model (es-c2m2) - U.S. Department of Energy • NISTR 7628 - Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements • ENISA Appropriate security measures for Smart Grids - ENISA • Best practices for handling smart grid cyber security - California Energy Commission

Table 2: International standards and good practices applicable across the Electricity subsector

Table 3 illustrates the mapping of security measures with Electricity specific standards, such as:

- **NIST SP 800-82 Rev. 2** (Guide to Industrial Control Systems (ICS) Security) [8] provides guidance on how to secure Industrial Control Systems (ICS) and is usually followed by EU operators as a good practice;
- **ISO 27019** is the information security management guidelines[9] based on ISO/IEC 27002 for process control systems specific to the energy utility industry;
- **NERC CIP** (North American Electric Reliability Corporation Critical Infrastructure Protection) [10] is a set of requirements for North America's bulk electric system. Nevertheless, it is followed as well by EU operators that extend their business in U.S.

D/N	DOMAIN NAME	SECURITY MEASURE	NIST SP-800-82	ISO 27019	NERC CIP
Part 1 – Governance and Ecosystem					
1.1	**Information System Security Governance & Risk Management**	Information system security risk analysis	3. ICS Risk Management and Assessment 4.5 Implement an ICS Security Risk	14.1.4 Business continuity planning framework	CIP-002-3 Critical Cyber Asset Identification

[8] https://csrc.nist.gov/csrc/media/publications/sp/800-82/rev-2/final/documents/sp800_82_r2_second_draft.pdf
[9] https://www.iso.org/standard/43759.html
[10] http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

D/N	DOMAIN NAME	SECURITY MEASURE	NIST SP-800-82	ISO 27019	NERC CIP
			Management Framework 6.1 Executing the Risk Management Framework Tasks for Industrial Control Systems 6.2.14 Risk Assessment	6.2.1 Identification of risks related to external parties	CIP-002-5 BES Cyber System Categorization CIP-010-2Table R3 – Vulnerability Assessments
		Information system security policy	3.3.1 Policy and Procedure Vulnerabilities	5. Security policy	CIP-003-6 Cyber Security - Security Management Controls CIP-011-2Table R1 – Information Protection
		Information system security accreditation	6.1.1 Security Assessment and Authorization	–	–
		Information system security indicators	3.3 Potential ICS Vulnerabilities	–	–
		Information system security audit	6.2.3 Audit and Accountability	10.10.1 Audit logging 15.3 Information systems audit considerations	CIP-003-6—Cyber Security —Security Management Controls, Compliance Monitoring Process
		Human resource security	6.2.1 Personnel Security	8. Human resource security	CIP-004 Cyber Security - Personnel & Training CIP-004-6 Table R1 – Security Awareness Program CIP-004-6Table R3– Personnel Risk Assessment Program
		Asset Management	#6.2.7 Media Protection	8. Asset Management	CIP-002-5.1a Cyber Security — BES Cyber System Categorization
1.2	**Ecosystem Management**	Ecosystem mapping	–	6.2 External parties	–

D/N	DOMAIN NAME	SECURITY MEASURE	NIST SP-800-82	ISO 27019	NERC CIP
		Ecosystem relations	–	6.2.2 Addressing security when dealing with customers 6.2.3 Addressing security in third-party agreements	–
Part 2 – Protection					
2.1	**IT Security Architecture**	Systems configuration	6.2.4 Configuration Management	11.4.4 Remote diagnostic and configuration port protection	CIP-007-6Table R1–Ports and Services CIP-010-2Table R1 – Configuration Change Management
		System segregation	5.1 Network Segmentation and Segregation 5.5 Network Segregation	10.6 Network security management 11.4.5 Segregation in networks	CIP-005-5 Table R1 – Electronic Security Perimeter
		Traffic filtering	6.3.3 Audit and Accountability 6.1.1 Security Assessment and Authorization	10.10.2 Monitoring system use	–
		Cryptography	6.3.4.1 Encryption	12.3 Cryptographic controls 15.1.6 Regulation of cryptographic controls	CIP-011-2 Cyber Security - Information Protection
2.2	**IT Security Administration**	Administration accounts	6.3.1 Identification and Authentication	11.5 Operating system access control	CIP-007-6Table R5 – System Access Control CIP-004-6Table R4–Access Management Program
		Administration information systems	–	10.10.4 Administrator and operator logs	CIP-007-6Table R5 – System Access Control CIP-004-6Table R4–Access Management Program

D/N	DOMAIN NAME	SECURITY MEASURE	NIST SP-800-82	ISO 27019	NERC CIP
2.3	**Identity and access management**	Authentication and identification	6.3.2 Access Control 6.3.1 Identification and Authentication	11. Access control	CIP-007-6Table R5 – System Access Control CIP-004-6Table R4– Access Management Program
		Access rights	6.3.2 Access Control	11. Access control	CIP-007-6Table R5 – System Access Control CIP-004-6Table R4– Access Management Program CIP-004-6Table R5– Access Revocation
2.4	**IT security maintenance**	IT security maintenance procedure	6.2.9 Maintenance	9.2.4 Equipment maintenance 12 Information systems acquisition, development and maintenance	CIP-007-6Table R2 – Security Patch Management
		Remote access	6.3.2 Access Control 6.3.1 Identification and Authentication	11.4 Network access control 11.4.4 Remote diagnostic and configuration port protection	CIP-005-5 Table R2 – Interactive Remote Access Management
2.5	**Physical and environmental security**	Physical and environmental security	6.2.2 Physical and Environmental Protection 6.2.7 Media Protection	9. Physical and environmental security 9.2 Equipment security	CIP-006-6 Cyber Security - Physical Security of BES Cyber Systems CIP-014-1 Physical Security
Part 3 - Defence					
3.1	**Detection**	Detection	3.3 Potential ICS Vulnerabilities	–	CIP-007-6 Table R4 – Security Event Monitoring CIP-007-6 Table R3 – Malicious Code Prevention

D/N	DOMAIN NAME	SECURITY MEASURE	NIST SP-800-82	ISO 27019	NERC CIP
		Logging	5.16 Monitoring, Logging,and Auditing	11.5.1 Secure log-on procedures	CIP-007-6 Table R4 – Security Event Monitoring
		Logs correlation and analysis	5.16 Monitoring, Logging, and Auditing	10.2.2 Monitoring and review of third party services 10.10.2 Monitoring system use	CIP-007-6 Table R4 – Security Event Monitoring
3.2	**Computer security incident management**	Information system security incident response	5.17 Incident Detection, Response, and System Recovery	13 Information security incident management	CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing
		Incident report	6.2.8 Incident Response	13.1 Reporting information security events and weaknesses	CIP-008 Cyber Security - Incident Reporting and Response Planning CIP-001 Sabotage Reporting
		Communication with competent authorities	–	6.1.6 Contact with authorities 6.1.7 Contact with special interest groups	CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication
Part 4 - Resilience					
4.1	**Continuity of Operations**	Business continuity management	6.1.2 Planning 6.1.3 Risk Assessment 6.1.5 Program Management	14. Business continuity management	CIP-013-1 Cyber Security - Supply Chain Risk Management
		Disaster recovery management	6.2.3 Contingency Planning	14.1 Information security aspects of business continuity management	CIP-009-1 Cyber Security - Recovery Plans for Critical Cyber Assets CIP-009-5 Cyber Security - Recovery

D/N	DOMAIN NAME	SECURITY MEASURE	NIST SP-800-82	ISO 27019	NERC CIP
					Plans for BES Cyber Systems
4.2	**Crisis Management**	Crisis management organization	6.2.6 Contingency Planning	14.2 Essential emergency services	CIP-009-6Table R1 – Recovery Plan Specifications CIP-009-6Table R2 – Recovery Plan Implementation and Testing
		Crisis management process	6.2.6 Contingency Planning	14.2.1 Emergency communication	CIP-009-6Table R3 – Recovery Plan Review, Update and Communication

Table 3: Mapping of security measures with electricity subsector specific standards

2.1.2 Oil & Gas

Protection of the Oil and Gas subsector within EU, but also globally, is considered of highly strategic and economic importance in the light of emerging hybrid threats targeting energy utilities.

Table 4 below lists international standards and good practices applicable across the Oil and Gas sectors of interest.

SUB-SECTORS	STANDARDS	GOOD PRACTICES
Oil & Gas	• Chemical Facility Anti-Terrorism Standards (CFATS)	• **API STD 1164** - Pipeline SCADA Security • **Oil and Natural Gas subsector cybersecurity capability maturity model** - (ONG-C2M2) • GIE - Gas Infrastructure Europe Security Risk Assessment Methodology[11] • Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry - Interstate Natural Gas Association of America (INGAA)

Table 4: International standards and good practices applicable across the Oil and Gas subsectors

The most known security framework related to the Oil and Gas subsector is the Chemical Facility Anti-Terrorism Standards (CFATS) program, which is a risk-based performance program that sets the standards for security at the United States highest risk chemical facilities.

The CFATS program covers equally both subsectors, while it identifies and regulates ensuring that high-risk chemical facilities have in place security measures to reduce the risks posed against these chemicals. However, the CFATS program does not consider cybersecurity, but safety.

[11] http://www.gie.eu/index.php/publications/gie/cat_view/2-gie-publications#

Table 5 illustrates the mapping of security measures with Oil and Gas specific good practices, such as:

- **API STD 1164** - Pipeline SCADA Security good practice[12] provides guidance to the operators of oil and gas liquids pipeline systems for managing SCADA system integrity and security.
- **ONG-C2M2** good practice assist oil and natural gas[13] organizations of all types to evaluate and make improvements to their cybersecurity programs.

D/N	DOMAIN NAME	SECURITY MEASURE	API STD 1164	ONG-C2M2
Part 1 – Governance and Ecosystem				
1.1	**Information System Security Governance & Risk Management**	Information system security risk analysis	3.4 Risk and Vulnerability Assessment 3.8 Asset Inventory/Categorizing/Tracking	Risk Management Threat and Vulnerability Management
		Information system security policy	1.3 Roles and Responsibilities 3.1 Security Plan 3.3 Security Policies	Cybersecurity Program Management
		Information system security accreditation	–	–
		Information system security indicators	–	–
		Information system security audit	7.2.2.6 File Audit and Control	–
		Human resource security	3.2 Personnel 5.12 Personnel Administration	Workforce Management
		Asset Management	3.8 Asset Inventory/ Categorizing/Tracking	Asset, Change, and Configuration Management Situational Awareness
1.2	**Ecosystem Management**	Ecosystem mapping	7.3.4 Connections to Third Parties for Support	Supply Chain and External Dependencies Management
		Ecosystem relations	3.11 Procurement 7.3.4 Connections to Third Parties for Support	Supply Chain and External Dependencies Management

[12] https://global.ihs.com/doc_detail.cfm?document_name=API%20STD%201164
[13] https://energy.gov/sites/prod/files/2014/03/f13/ONG-C2M2-v1-1_cor.pdf

D/N	DOMAIN NAME	SECURITY MEASURE	API STD 1164	ONG-C2M2
Part 2 – Protection				
2.1	**IT Security Architecture**	Systems configuration	3.9 Change Management 3.10.1 System Hardening 3.10.2 Software Patching and Updates 3.10.3 Proper Disposal of Equipment and Media. 5.9 Disabled Non-Required Services 5.10 Operating System Tools 7.1.6 Defense in Depth 7.2.2.4 White Listing 7.2.2.5 Host/Endpoint Security 7.2.2.6 File Audit and Control 8.2.1 Network Protocols	Asset, Change, and Configuration Management
		System segregation	7 Network Design/Security and Data Interchange 7.1 Network Design 7.1.1 Interconnected Business and SCADA Networks 7.1.2 Communication Demarcation Points 7.1.3 Firewalls 7.1.4 Demilitarized Zone (DMZ) 7.1.5 Dual-Homed Computers 7.1.7 Firewall Management 7.1.8 Virtualization 7.1.8.2 Hypervisor and Virtual Machine Services 7.1.8.3 Networking 7.1.8.4 Resource Allocation 7.2 Network Management 7.3.1 Connections Between the SCADA Control Center Operational Facilities, Data Center, and Telecommunications Center	–

D/N	DOMAIN NAME	SECURITY MEASURE	API STD 1164	ONG-C2M2
			7.3.2 Connections Between the SCADA System and Business Networks 7.3.3 Connections Between the SCADA System and Business Partners SCADA Systems 7.3.5 Internet and Business Network Access 7.3.6 Voice Over IP/IP telephony (VoIP/IPT) 7.3.7 Instant Messaging (IM) 7.3.8 Wireless Networking 7.3.9 Audio/Video Conferencing 7.3.10 Video Surveillance 7.3.11 Cloud Computing 8 Field Communication 8.1 Field Device Technology	
		Traffic filtering	7.1.7 Firewall Management 7.1.8.3 Networking 7.3 Data Interchange	–
		Cryptography	7 Network Design/Security and Data Interchange 7.3 Data Interchange 8.2.2 Encryption of Data on Accessible Paths	–
2.2	**IT Security Administration**	Administration accounts	5.3 User Accounts 5.4 Operating System Accounts 5.5 SCADA Accounts	Identity and Access Management
		Administration information systems	5.4 Operating System Accounts 5.5 SCADA Accounts	–
2.3	**Identity and access management**	Authentication and identification	5.3 User Accounts 5.6 Password Controls 5.7 Multi-factor Authentication 5.8 Biometrics	Identity and Access Management
		Access rights	5.1 Restricted Access	Identity and Access Management

D/N	DOMAIN NAME	SECURITY MEASURE	API STD 1164	ONG-C2M2
			5.2 Logical Access Control to Control Systems and Control Networks 5.11 Device Access 7.1.8.1 Permissions 7.2 Network Management 8.2 System Access 8.2.3 Casual User Access to Network	
2.4	**IT security maintenance**	IT security maintenance procedure	3.5 New or Replacement System Security Design 3.10 Operating System and Application Updates 3.10.2 Software Patching and Updates 3.10.3 Proper Disposal of Equipment and Media. 9 Annual Review, Reassessment, and Update	–
		Remote access	5.1 Restricted Access 5.2 Logical Access Control to Control Systems and Control Networks 5.11 Device Access 7.2 Network Management 7.3.4 Connections to Third Parties for Support 8.2.4 Remote Access to SCADA Components 8.2.5 Dial-up Modem Access for Maintenance	–
2.5	**Physical and environmental security**	Physical and environmental security	4 Physical Security	–
Part 3 - Defence				
3.1	**Detection**	Detection	7.2.2 Network Security 7.2.2.1 Intrusion Detection and Prevention Systems (IDPS)	Situational Awareness

D/N	DOMAIN NAME	SECURITY MEASURE	API STD 1164	ONG-C2M2
			7.2.2.2 Malware Detection and Avoidance	
		Logging	7.2.1 Network Monitoring & Advanced Threat Protection 7.2.2 Network Security	Situational Awareness
		Logs correlation and analysis	7.2.2 Network Security 7.2.2.1 Intrusion Detection and Prevention Systems (IDPS) 7.2.2.3 Security Information and Event Management (SIEM)	–
3.2	**Computer security incident management**	Information system security incident response	3.7 Incident Response Plan (IRP)	Event and Incident Response, Continuity of Operations
		Incident report	–	Event and Incident Response, Continuity of Operations
		Communication with competent authorities	6 Information Distribution 6.1 Confidential 6.2 Restricted 6.3 Internal Use Only 6.4 Public	Information Sharing and Communications
Part 4 - Resilience				
4.1	**Continuity of Operations**	Business continuity management	3.6 Business Continuity Plan (BCP)	Event and Incident Response, Continuity of Operations
		Disaster recovery management	–	–
4.2	**Crisis Management**	Crisis management organization	–	–
		Crisis management process	–	–

Table 5: Mapping of security measures with Oil and Gas subsector specific standards

Finally, according to the input gathered by Oil and Gas operators in EU, the most applicable information security standards are ISO 27001, the NIST Cybersecurity Framework and ISA/IEC 62443. The mapping of security measures to these standards is presented in **section 3, Table 22**.

2.2 Transport

According to the NIS Directive, the Transport sector is divided in the following subsectors:

- Air Transport;
- Rail Transport;
- Water Transport;
- Road Transport.

Due to a great range of threats, cyber security and physical safety of the transport sector can no longer be treated separately[14]. Among the good practices for the transport sector, the "Roadmap to Secure Control Systems in the Transportation Sector" [15] is included, while there are no specific cybersecurity standards.

Therefore, risk management methodologies and security standards usually incorporate measures of both natures, cyber and physical as well. Besides ISO 27001 and ISA/IEC 62443 standards that are mainly followed by transport operators, in the following sections, the mapping of security measures to specific subsector standards is presented respectively.

2.2.1 Air Transport

Table 6 lists international standards and good practices applicable across the Air Transport sector.

SUB-SECTOR	STANDARDS	GOOD PRACTICES
Air Transport	• **ICAO Aviation Security Manual - Document 8973 (Restricted Access)** • ARINC 811 Commercial aircraft information security concepts of operations and process framework • EUROCAE ED-201 – 204 Aeronautical Information System Security (AISS) Framework • RTCA DO-326 Airworthiness security process specifications	• **AIAA (The American Institute of Aeronautics and Astronautics) The Connectivity Challenge: Protecting Critical Assets in a Networked World** • Information Security Certification and Accreditation (C&A) Handbook – FAA • FAA Issue Paper, Aircraft Electronic Systems Security Protection from Unauthorized External Access • FAA Aircraft systems information security protection overview

Table 6: International standards and good practices applicable across the Air Transport sector

Airports, Airlines and Air Navigation Service providers mainly use a risk based approach to security and rely on international information security standards, such as ISO27001 and NIST Cybersecurity Framework.

Table 7 illustrates the mapping of security measures to Air transport specific standards and good practices, such as:

- **ICAO Aviation Security Manual** - Document 8973 (Restricted Access)[16] gives a layout on cyber threats to critical aviation information and communication technology systems. Guidance material on areas such as unpredictability, behaviour detection techniques, landside security, and screening of persons other than passengers have been incorporated in the latest version.
- **AIAA (The American Institute of Aeronautics and Astronautics)** The Connectivity Challenge: Protecting Critical Assets in a Networked World[17] outlines a framework for helping the aviation

[14] https://www.enisa.europa.eu/publications/good-practices-recommendations
[15] https://ics-cert.us-cert.gov/sites/default/files/documents/TransportationRoadmap20120831.pdf
[16] http://www.icao.int/Security/SFP/Pages/SecurityManual.aspx
[17] https://www.hklaw.com/publications/Coast-Guard-DHS-Mandate-Cybersecurity-Reporting-Move-to-Require-Maritime-Cybersecurity-Programs-07-20-2017/

community build a roadmap for ensuring that aviation's critical infrastructure is secure and able to withstand and rapidly recover from the evolving threats. This framework addresses all security levels including know, prevent, detect, respond and recover.

D/N	DOMAIN NAME	SECURITY MEASURE	ICAO	AIAA
Part 1 – Governance and Ecosystem				
1.1	**Information System Security Governance & Risk Management**	Information system security risk analysis	#3 Security Measures for Infrastructure	#3 Define Operational Principals
		Information system security policy	#3 Security Measures for Infrastructure	#3 Define Operational Principals
		Information system security accreditation	#3 Security Measures for Infrastructure	#5 Establish common cyber standards for aviation systems
		Information system security indicators	–	–
		Information system security audit	–	–
		Human resource security	–	#6 Establish a Cybersecurity Culture
		Asset Management	#4 Define Design Principals	#4 Define Design Principals
1.2	**Ecosystem Management**	Ecosystem mapping	#1 Supply Chain Security for Hardware and Software	#7 Strengthen the defensive system
		Ecosystem relations	#1 Supply Chain Security for Hardware and Software	#7 Strengthen the defensive system
Part 2 – Protection				
2.1	**IT Security Architecture**	Systems configuration	#1 Supply Chain Security for Hardware and Software	–
		System segregation	#3 Security Measures for Infrastructure	#4 Define Design Principals
		Traffic filtering	#3 Security Measures for Infrastructure	#7 Strengthen the defensive system
		Cryptography	#3 Security Measures for Infrastructure	#7 Strengthen the defensive system
2.2	**IT Security Administration**	Administration accounts	–	#7 Strengthen the defensive system

D/N	DOMAIN NAME	SECURITY MEASURE	ICAO	AIAA
		Administration information systems	–	–
2.3	**Identity and access management**	Authentication and identification	#3 Security Measures for Infrastructure	–
		Access rights	#3 Security Measures for Infrastructure	–
2.4	**IT security maintenance**	IT security maintenance procedure	#3 Security Measures for Infrastructure	–
		Remote access	#3 Security Measures for Infrastructure	–
2.5	**Physical and environmental security**	Physical and environmental security	–	–
Part 3 - Defence				
3.1	**Detection**	Detection	#2 Cyber Attack Incident Records	#7 Strengthen the defensive system
		Logging	–	#7 Strengthen the defensive system
		Logs correlation and analysis	–	#7 Strengthen the defensive system
3.2	**Computer security incident management**	Information system security incident response	#2 Cyber Attack Incident Records	#2 Provide incident response
		Incident report	#2 Cyber Attack Incident Records	#2 Provide incident response
		Communication with competent authorities	#2 Cyber Attack Incident Records	#2 Provide incident response
Part 4 - Resilience				
4.1	**Continuity of Operations**	Business continuity management	#3 Security Measures for Infrastructure	–
		Disaster recovery management	#3 Security Measures for Infrastructure	–
4.2	**Crisis Management**	Crisis management organization	#3 Security Measures for Infrastructure	–

D/N	DOMAIN NAME	SECURITY MEASURE	ICAO	AIAA
		Crisis management process	#3 Security Measures for Infrastructure	–

Table 7: Mapping of security measures with the Air Transport sector specific standards

2.2.2 Rail Transport

The majority of security standards and frameworks in the domain of Rail Transport is dealing mainly with safety aspects, rather than cybersecurity challenges which may affect eventually the safety and security of modern signalling and train control systems.

Table 8 below, lists international information security standards and good practices applicable to the Rail Transport subsector.

SUB-SECTOR	STANDARDS	GOOD PRACTICES
Rail Transport	• ISO 27001 Information technology — Security techniques — Information security management systems — Requirements • ANSI/ISA, Series "ISA-62443: Security for industrial automation and control system"	• UK Rail Cyber Security Guidance to Industry

Table 8: International standards and good practices applicable across the Rail Transport subsector

According to the feedback taken by EU rail operators, the most commonly applicable standards regarding network and information systems security are ISO 27001 and ANSI ISA/IEC 62443. The mapping of the proposed security measures with the above mentioned standards is presented in **section 3, Table 22**.

2.2.3 Water Transport

ICT systems supporting maritime operations, extending from port management to ship communication, are generally highly complex and employ a variety of ICT technologies. There is lack of holistic consideration of cybersecurity in this particular working environment.

Table 9 lists some international standards and good practices applicable in the Water Transport subsector taking into account security and mainly safety aspect.

SUB-SECTOR	STANDARDS	GOOD PRACTICES
Water Transport	• International Safety Management (ISM) Code)[18] • IMO interim guidelines on maritime cyber risk management • International Ship and Port Facility Security (ISPS) Code • ISO 27001— Information security management systems • ANSI/ISA, Series "ISA-62443: Security for industrial automation and control system	• **BIMCO Guidelines on Cyber Security on board Ships - The Guidelines on Cyber security on board ships** • DNVGL-RP-0496 (DNV-GL, 2016) Cyber security resilience management for ships and mobile offshore units in operation

[18] http://www.imo.org/en/Publications/PublishingImages/PagesfromEB117E.pdf & http://www.imo.org/en/OurWork/humanelement/safetymanagement/pages/ismcode.aspx

	• IEC 62351:2017 SER - Power systems management and associated information exchange - Data and communications security • IEC 61162 - Digital interfaces for navigational equipment within a ship • ISO 13613:2011 - Ships and marine technology -- Maintenance and testing to reduce losses in critical systems for propulsion • ISO 14885:2014 - Large yachts -- Diesel engines for main propulsion and essential auxiliaries -- Safety requirements	• Cyber-enabled ships: ShipRight procedure – autonomous ships • Cyber-enabled ships: Deploying information and communications technology in shipping – Lloyd's Register's approach to assurance • United States coast guard – Cyber Strategy Draft guidelines on maritime cyber risk management • The Tanker Management and Self Assessment (TMSA) is a best practice guide for ship operators whose latest version (TMSA 3) includes a new element about cybersecurity for both vessels and onshore

Table 9: International standards and good practices applicable in the Water Transport subsector

In the current regulatory context for the water transport subsector, either at regional or national level, there is very little consideration given to cyber security elements[19].

According to the input taken by Water Transport operators, **Table 10** illustrates the mapping of security measures to Water transport specific standards and good practices, such as:

- **Cybersecurity On-board Ships** is a guideline for cybersecurity on board [20]and it is made by the cooperation of BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.

D/N	DOMAIN NAME	SECURITY MEASURE	CYBERSECURITY ONBOARD SHIPS (BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF AND IUMI)
Part 1 – Governance and Ecosystem			
1.1	**Information System Security Governance & Risk Management**	Information system security risk analysis	# 2.1 Determination of vulnerability # 2.2 Risk assessment made by the company
		Information system security policy	–
		Information system security accreditation	–
		Information system security indicators	–

[19] https://www.hklaw.com/publications/Coast-Guard-DHS-Mandate-Cybersecurity-Reporting-Move-to-Require-Maritime-Cybersecurity-Programs-07-20-2017/ & http://www.ubak.gov.tr/BLSM_WIYS/DISGM/tr/HTML/20130304_142647_66968_1_67502.pdf

[20] The Guidelines on Cybersecurity onboard ships refer exclusively to cybersecurity for vessels | http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16

D/N	DOMAIN NAME	SECURITY MEASURE	CYBERSECURITY ONBOARD SHIPS (BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF AND IUMI)
		Information system security audit	–
		Human resource security	# 3.2.1 Training and awareness
		Asset Management	#1.1 Plans and procedures #3.1 Ship to shore interface
1.2	**Ecosystem Management**	Ecosystem mapping	# 2.3 Third party risk assessments
		Ecosystem relations	# 2.3 Third party risk assessments
Part 2 – Protection			
2.1	**IT Security Architecture**	Systems configuration	# 3.1.1 Limitation to and control of network ports, protocols and services # 3.1.2 Configuration of network devices such as firewalls, routers and switches # 3.1.3 Secure configuration for hardware and software # 3.1.4 Email and web browser protection # 3.1.10 Secure network design
		System segregation	# 3.1.10 Secure network design
		Traffic filtering	# 3.1.5 Satellite and radio communication
		Cryptography	–
2.2	**IT Security Administration**	Administration accounts	# 3.1.3 Secure configuration for hardware and software # 3.2.4 Use of administrator privileges
		Administration information systems	# 3.1.3 Secure configuration for hardware and software
2.3	**Identity and access management**	Authentication and identification	# 3.1.12 Boundary defence
		Access rights	–
2.4	**IT security maintenance**	IT security maintenance procedure	# 3.1.9 Application software security # 3.2.2 Upgrades and software maintenance # 3.2.3 Anti-virus and anti-malware tool updates
		Remote access	# 3.1.8 Wireless access control
2.5	**Physical and environmental security**	Physical and environmental security	# 3.1.11 Physical security # 3.1.12 Boundary defence
Part 3 - Defence			

D/N	DOMAIN NAME	SECURITY MEASURE	CYBERSECURITY ONBOARD SHIPS (BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF AND IUMI)
3.1	Detection	Detection	# 3.1.6 Malware defences
		Logging	–
		Logs correlation and analysis	–
3.2	Computer security incident management	Information system security incident response	–
		Incident report	–
		Communication with competent authorities	# 4.3 Investigate cyber incidents
Part 4 - Resilience			
4.1	Continuity of Operations	Business continuity management	# 3.1.7 Data recovery capability # 4.1 Response Plan
		Disaster recovery management	# 4.2 Recovery
4.2	Crisis Management	Crisis management organization	# 3.2.7 Obtaining support from ashore and contingency plans
		Crisis management process	# 4.2 Recovery

Table 10: Mapping of security measures with the Water Transport sector specific standard

ISO 27001 and ANSI ISA/IEC 62443 are among the most applicable standards for network and information systems security in the domain. The mapping with these standards is provided below in **section 3, Table 22**.

2.2.4 Road Transport

Several initiatives[21] led to defining guidelines or rules to implement security in the automotive industry[22], and other initiatives asked for collaboration on the security topics from the automotive industry[23]. Although some of them are well under development, like ISO/AWI 21434 (Road Vehicles -- Automotive Security

[21] https://www.automotiveisac.com/best-practices/
[22] https://wiki.unece.org/download/attachments/40009763/%28ITS_AD-10-11-Rev1%29%20Revised%20draft%20of%20guideline%20on%20cybersecurity%20and%20data%20protection.pdf?api=v2
[23] https://www.iamthecavalry.org/domains/automotive/5star/

Engineering)[24], safety and security considerations are currently handled by the TC22/SC3/WG16 committee under the development of ISO 26262[25].

Table 11 lists international standards and good practices applicable across the Road Transport subsector.

SUB-SECTOR	STANDARDS	GOOD PRACTICES
Road Transport	• SAE J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems • SAE J3101 Requirements for Hardware-Protected Security for Ground Vehicle Applications (WiP) • ISO 15031 Road Vehicles - Communication between. vehicle and external equipment for emissions-related diagnostics. Part 7: Data link security • ISO 15764 Road Vehicles - Extended data link security • ISO/AWI 21434 - Road Vehicles -- Automotive Security Engineering • ISO 26262-1:2011 - Road vehicles -- Functional safety • TS 102 940 Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management • TS 103 096-1 to TS 103 096-3: Intelligent Transport Systems (ITS); • TR 103 061-6 Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 6: Validation report	• ENISA Cyber Security and Resilience of smart cars – ENISA • Auto ISAC, Automotive Information Sharing and Analysis Center, Best Practices • Five Star Automotive Cyber Safety Program, I Am The Cavalry • Guideline on cybersecurity and data protection of connected vehicles and vehicles with ADT – UNECE

Table 11: International standards and good practices applicable across the Road Transport subsector

According to the input taken by EU road transport operators, SAE J3061 - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems has a predominant position, as it describes a cybersecurity process framework according to which an organization can develop an internal process for designing and building cybersecurity in-vehicle systems. As this standard is not publicly available, the mapping of security measures to this standard is not presented.

Nevertheless, ISO 27001 is the most applicable standard for both vehicle and road-side infrastructure, while ANSI ISA/IEC 62443 is usually applied in the road side infrastructure. The mapping of the security measures to these two standards is provided below in **section 3**, **Table 22**.

2.3 Financial and Banking

Table 12 lists international standards and good practices applicable across the Financial and Banking sector.

[24] https://www.iso.org/standard/70918.html
[25] https://www.iso.org/obp/ui/#iso:std:iso:26262:-1:en

SECTOR	STANDARDS	GOOD PRACTICES
Financial & Banking	• **ISO/TR 13569:2005** • **Gramm–Leach–Bliley Act** • **Sarbanes–Oxley Act** • **Payment services (PSD 2) - Directive (EU) 2015/2366** • EBA on the security of internet payments[26] • ISO/IEC 27015:2012 Information technology - Security techniques – Information security management guidelines for financial services • American National Standards Institute (ANSI) X9 series	• **Payment Card Industry Data Security Standard (PCI DSS)** • Basel II[27] • Draft Guidelines on the security measures for operational and security risks of payment services under PSD2[28] • CPMI-IOSCO Guidance on cyber resilience for financial market infrastructure[29] • SEC OCIE Cybersecurity[30]

Table 12: International standards and good practices applicable across the Financial and Banking sector

According to input taken by Financial and Banking institutions in EU, **Table 13**, illustrates the mapping of security measures to sector specific standards and good practices, such as:

- **ISO/TR 13569:2005 Financial services -- Information security guidelines**[31] provides guidelines on the development of an information security programme for institutions in the financial services industry. Considerations for the selection and implementation of security controls, and the elements required to manage information security risk within a modern financial services institution are discussed.
- **Gramm-Leach-Bliley Act** (GLB Act or GLBA)[32], also known as the Financial Modernization Act of 1999, is a federal law enacted in the United States to control the ways that financial institutions deal with the private information of individuals. It requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.
- **Sarbanes-Oxley Act** of 2002 (SOX)[33] is an act passed by U.S. Congress in 2002 to protect investors from the possibility of fraudulent accounting activities by corporations. The SOX Act mandated strict reforms to improve financial disclosures from corporations and prevent accounting fraud.

[26] http://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-the-security-of-internet-payments

[27] Basel II or International Convergence of Capital Measurement and Capital Standards is a set of recommendations issued by the Basel Committee on Banking Supervision. Basel II is considered by the Basel Committee to be instrumental in assessments of risk provided by banks' internal systems as inputs to capital calculations. Its relevance is complicated, since it is partially dependant on whether or not local governments have adopted it into their local regulations (or if Basel I has), and how this adoption has occurred. [https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/corporate-governance/basel-ii] The mapping to Basel II will be added in the next version of this document.

[28] http://www.eba.europa.eu/documents/10180/1836621/Consultation+Paper+on+the+security+measures+for+operational+and+security+risks+of+payment+services+under+PSD2+%28EBA-CP-2017-04%29.pdf

[29] http://www.bis.org/cpmi/publ/d146.pdf

[30] https://www.sec.gov/spotlight/cybersecurity

[31] https://www.iso.org/standard/37245.html

[32] https://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf

[33] http://www.ey.com/Publication/vwLUAssets/ey-the-sarbanes-oxley-act-at-15/$File/ey-the-sarbanes-oxley-act-at-15.pdf

- **Payment services (PSD 2) - Directive (EU) 2015/2366**[34] seeks to improve the existing EU rules for electronic payments. It takes into account emerging and innovative payment services, such as internet and mobile payments. It sets out rules concerning strict security requirements for electronic payments and the protection of consumers' financial data, guaranteeing safe authentication and reducing the risk of fraud; the transparency of conditions and information requirements for payment services; the rights and obligations of users and providers of payment services.
- **Payment Card Industry Data Security Standard (PCI DSS)** [35] is an information security standard for organizations that handle branded credit cards from the major card schemes. The PCI Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. The standard was created to increase controls around cardholder data to reduce credit card fraud.

[34] https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en

[35] https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf

D/N	DOMAIN NAME	SECURITY MEASURE	PSD2	PCI-DSS	ISO/TR 13569:2005	GLBA	SOX
Part 1 – Governance and Ecosystem							
1.1	**Information System Security Governance & Risk Management**	Information system security risk analysis	Guideline 1[36]: Governance Operational and security risk management framework	–	8.1 Processes 8.2 Risk assessment process 9.1 Risk mitigation	§ 314.1 (a) Purpose	–
		Information system security policy		Requirement 12 Maintain a policy that addresses information security for all personnel	5.1 Purpose 5.2 Legal and regulatory compliance 5.3 Development 5.4 Documentation hierarchy	§ 314.1 (b) Scope § 314.3 (a) Information Security Program	Information Security Policy Records Retention Policy and Procedures
		Information system security accreditation	Guideline 6: Testing of security measures	–	8.3 Security recommendations and risk acceptance	§ 314.3 (b) (1) Security of Customer Information	Acquisition and planning process Security Standards
		Information system security indicators	Guideline 7: Situational awareness and continuous learning	Requirement 11 Regularly test security systems and processes	13.2 Security compliance	§ 314.3 (a) Information Security Program	Policy and Procedure Compliance

[36] Taken from Art 95 Management of operational and Security risks

D/N	DOMAIN NAME	SECURITY MEASURE	PSD2	PCI-DSS	ISO/TR 13569:2005	GLBA	SOX
			Threat landscape and situational awareness				
		Information system security audit	Guideline 1: Governance Operational and security risk management framework	–	12.2 Audit	§ 314.1 (b) Scope	Post Implementation Reviews Review of Security Tests Policy and Procedure Compliance
		Human resource security	Guideline 2: Risk assessment Identification of functions, processes and assets	–	9.6 Information security awareness 9.7 Human factors	§ 314.1 (a) Purpose	–
		Asset Management	Guideline 2: Risk assessment Identification of functions, processes and assets	Requirement 6: Develop and maintain secure systems and applications			
1.2	**Ecosystem Management**	Ecosystem mapping	Guideline 2: Risk assessment • Identification of functions, processes and assets	–	12.4 External service providers	§ 314.1 (b) Scope § 314.2 (b) Customer Information § 314.2 (d) Service Provider	Monitoring Third Party Services Third Party Contracting Procedures Third Party Qualification

D/N	DOMAIN NAME	SECURITY MEASURE	PSD2	PCI-DSS	ISO/TR 13569:2005	GLBA	SOX
			• Classification of functions, processes and assets Risk assessments of functions, processes and assets				Vendor Management Policy Third Party Qualification
		Ecosystem relations		–	12.4 External service providers	§ 314.1 (b) Scope § 314.2 (b) Customer Information	Addressing Risks in Third Party Contracts
Part 2 – Protection							
2.1	**IT Security Architecture**	Systems configuration	Guideline 2: Risk assessment Identification of functions, processes and assets	Requirement 1 Install and maintain a firewall configuration to protect cardholder data Requirement 6 Develop and maintain secure systems and applications	10.1 Protecting IT systems 10.3 Software systems security 10.4 Network and network systems controls	§ 314.3 (a) Information Security Program	–
		System segregation	Guideline 3: Protection Data and Systems Integrity and Confidentiality	–	10.4 Network and network systems controls	§ 314.3 (a) Information Security Program	–
		Traffic filtering	Guideline 3: Protection	–	12.2 Audit	§ 314.3 (a) Information Security Program	–

D/N	DOMAIN NAME	SECURITY MEASURE	PSD2	PCI-DSS	ISO/TR 13569:2005	GLBA	SOX
		Cryptography	–	Requirement 4 Encrypt transmission of cardholder data across open, public networks	12.6 Cryptographic operations 12.7 Key management 12.8 Privacy	§ 314.3 (b) (2) Protect against Threats or hazards	–
2.2	**IT Security Administration**	Administration accounts	Guideline 3: Protection	Requirement 2 Do not use vendor-supplied defaults for system passwords and other security parameters	9.3 Logical access control	§ 314.3 (b) (1) Security of Customer Information § 314.3 (b) (3) Protect against Unauthorized Access	–
		Administration information systems	Guideline 3: Protection	–	9.3 Logical access control	§ 314.3 (b) (1) Security of Customer Information § 314.3 (b) (3) Protect against Unauthorized Access	–
2.3	**Identity and access management**	Authentication and identification	Guideline 3: Protection Access control	Requirement 8 Identify and authenticate access to system components	9.3 Logical access control	§ 314.1 (b) Scope § 314.3 (b) (3) Protect against Unauthorized Access	–
		Access rights		Requirement 3 Protect stored cardholder data Requirement 7 Restrict access to cardholder	9.3 Logical access control	§ 314.1 (b) Scope	Review of Access Rights

D/N	DOMAIN NAME	SECURITY MEASURE	PSD2	PCI-DSS	ISO/TR 13569:2005	GLBA	SOX
				data by business need to know		§ 314.3 (b) (3) Protect against Unauthorized Access	
2.4	**IT security maintenance**	IT security maintenance procedure	Guideline 2: Risk assessment Risk assessments of functions, processes and assets	Requirement 5 Protect all systems against malware and regularly update anti-virus software or programs	9.5 Change control 13.1 Maintenance	§ 314.2 (c) Information Security Program	–
		Remote access	Guideline 3: Protection	–	–	–	–
2.5	**Physical and environmental security**	Physical and environmental security	Guideline 3: Protection Physical Protection	Requirement 9 Restrict physical access to cardholder data	11.1 Financial transaction cards	§ 314.1 (a) Purpose § 314.1 (b) Scope § 314.2 (c) Information Security Program	–
Part 3 – Defense							
3.1	**Detection**	Detection	Guideline 2: Risk assessment Classification of functions, processes and assets	–	8.1 Detection	13.3 Monitoring	§ 314.3 (a) Information Security Program
		Logging		Requirement 10 Track and monitor all access to network resources and cardholder data	8.2 Logging	9.4 Audit journals	§ 314.1 (b) Scope § 314.3 (a) Information Security Program

D/N	DOMAIN NAME	SECURITY MEASURE	PSD2	PCI-DSS	ISO/TR 13569:2005	GLBA	SOX
		Logs correlation and analysis		–	8.3 Logs correlation and analysis	–	§ 314.3 (a) Information Security Program
3.2	**Computer security incident management**	Information system security incident response	Article 96 (Incident Reporting)	–	14.1 Managing Events 14.3 Incident handling 14.4 Emergency problems	§ 314.3 (b) (2) Protect against Threats or hazards	Security Incident Response
		Incident report		–	14.2 Investigations and forensics	§ 314.3 (b) (2) Protect against Threats or hazards	Security Incident Response
		Communication with competent authorities		–	14.3 Incident handling	§ 314.3 (b) (2) Protect against Threats or hazards § 314.2 (c) Information Security Program	Security Incident Response
Part 4 – Resilience							
4.1	Continuity of Operations	Business continuity management	Guideline 5: Business continuity Business continuity management	–	–	§ 314.3 (b) (2) Protect against Threats or hazards § 314.3 (b) (1) Security of Customer Information	–

D/N	DOMAIN NAME	SECURITY MEASURE	PSD2	PCI-DSS	ISO/TR 13569:2005	GLBA	SOX
		Disaster recovery management		–	12.3 Disaster recovery planning	§ 314.3 (b) (2) Protect against Threats or hazards	–
4.2	Crisis Management	Crisis management organization	Guideline 5: Business continuity Business continuity management Incident management and crisis communication	–	6.5 Incident management	§ 314.3 (b) (2) Protect against Threats or hazards	–
		Crisis management process		–	6.5 Incident management	§ 314.3 (b) (2) Protect against Threats or hazards	–

Table 13: Mapping with the security measures of the Financial and Banking sector specific standards

2.4 Healthcare

Table 14 lists international standards and good practices applicable across healthcare sector.

SECTOR	STANDARDS	GOOD PRACTICES
Healthcare	• ISO 27799:2008 Health informatics - Information security management in health using ISO/IEC 27002 • Health Insurance Portability and Accountability Act (HIPPA) • ISO 13485:2003 Medical devices -- Quality management systems – Requirements for regulatory purposes • ISO 80001-1:2010 Application of risk management for IT networks incorporating medical devices • ETSI eHealth Standard TR 102 764 eHEALTH; Architecture; Analysis of user service models, technologies and applications supporting eHealth[37] • Digital Imaging and Communications in Medicine (DICOM) • EC Medical Devices Regulation (text agreed by EP and Council – in adoption process) • NIST SP 800-66 An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Guide	• Royal Australian College of General Practitioners (RACGP) Computer Information Security Standards (CISS)

Table 14: International standards and good practices applicable across Healthcare sector

According to input taken by healthcare operators in EU, **Table 15**, illustrates the mapping of security measures to sector specific standards and good practices, such as:

- **ISO 27799:2016**[38] gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s). It defines guidelines to support the interpretation and implementation in health informatics of ISO/IEC 27002 and is a companion to that International Standard.
- **Health Insurance Portability and Accountability Act of 1996 (HIPAA)** [39] required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information. The *Security Standards for the Protection of Electronic Protected Health Information* (the Security Rule) [40] establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule[41] by addressing the technical and non-technical safeguards that organizations called “covered entities” must put in place to secure individuals’ “electronic protected health information” (e-PHI).

[37] http://www.etsi.org/technologies-clusters/technologies/ehealth
[38] https://www.iso.org/standard/62777.html
[39] https://www.hhs.gov/hipaa/for-professionals/security/index.html?language=es
[40] https://www.hhs.gov/hipaa/for-professionals/privacy/index.html?language=es
[41] https://www.awwa.org/store/productdetail.aspx?productid=20779

D/N	DOMAIN NAME	SECURITY MEASURE	ISO 27799	HIPAA
Part 1 – Governance and Ecosystem				
1.1	**Information System Security Governance & Risk Management**	Information system security risk analysis	5.1 Management direction for information security 6.1 Internal organization	Assigned Security Responsibility Information Security Activity Review Assigned Security Responsibility Risk analysis Risk management
		Information system security policy	5.1 Management direction for information security 6.1 Internal organization	Assigned Security Responsibility Information Security Activity Review Assigned Security Responsibility
		Information system security accreditation	5.1 Management direction for information security 6.1 Internal organization 8.1 Responsibility for assets 8.2 Information classification	Assigned Security Responsibility Information Security Activity Review Assigned Security Responsibility Risk analysis Risk management
		Information system security indicators	5.1 Management direction for information security 6.1 Internal organization 18.1 Compliance with legal and contractual requirements 18.2 Information security reviews	Assigned Security Responsibility Information Security Activity Review Assigned Security Responsibility Sanction policy Evaluation
		Information system security audit	5.1 Management direction for information security 6.1 Internal organization 7.1 Prior to employment 7.2 During employment 7.3 Termination and change of employment	Assigned Security Responsibility Information Security Activity Review Assigned Security Responsibility
		Human resource security	5.1 Management direction for information security 6.1 Internal organization 7.1 Prior to employment 7.2 During employment	Assigned Security Responsibility Information Security Activity Review Workforce clearance procedure Termination procedures

D/N	DOMAIN NAME	SECURITY MEASURE	ISO 27799	HIPAA
			7.3 Termination and change of employment 15.2 Supplier service delivery management 18.1 Compliance with legal and contractual requirements	Sanction policy Security Training Response and reporting Protection from malicious software Written Contract or Other Arrangement
		Asset Management	8.1 Responsibility for assets 8.2 Information classification 8.3 Media Handling	Integrity Controls Mechanism to Authenticate Electronic Protected Health Information Accountability Device and Media Controls Disposal Encryption and Decryption Encryption
1.2	**Ecosystem Management**	Ecosystem mapping	15.1 Information security in supplier relationships 15.2 Supplier service delivery management	–
		Ecosystem relations	15.1 Information security in supplier relationships 15.2 Supplier service delivery management	–
Part 2 – Protection				
2.1	**IT Security Architecture**	Systems configuration	13.1 Network security management 13.2 Information transfer	–
		System segregation	13.1 Network security management 13.2 Information transfer	–
		Traffic filtering	13.1 Network security management 13.2 Information transfer	–
		Cryptography	13.1 Network security management	–

D/N	DOMAIN NAME	SECURITY MEASURE	ISO 27799	HIPAA
			13.2 Information transfer	
2.2	**IT Security Administration**	Administration accounts	–	–
		Administration information systems	–	–
2.3	**Identity and access management**	Authentication and identification	9.1 Business requirements of access control 9.2 User access management 9.3 User responsibilities 9.4 System and application access control	Access authorization Termination Procedures Unique User Identification Access Establishment and Modification Authorization and/or supervision Unique User Identification Person or Entity Authentication Automatic Logoff Workstation use
		Access rights	9.1 Business requirements of access control 9.2 User access management 9.3 User responsibilities 9.4 System and application access control	Access authorization Termination Procedures Unique User Identification Access Establishment and Modification Authorization and/or supervision Unique User Identification Person or Entity Authentication Automatic Logoff Workstation use
2.4	**IT security maintenance**	IT security maintenance procedure	12.5 Control of operational software 12.6 Technical vulnerability management	Integrity Controls Mechanism to Authenticate Electronic Protected Health Information
		Remote access	13.1 Network security management 13.2 Information transfer	Person or Entity Authentication
2.5	**Physical and environmental security**	Physical and environmental security	11.1 Secure areas 11.2 Equipment	Physical Safeguards Access Control and Validation Procedures

D/N	DOMAIN NAME	SECURITY MEASURE	ISO 27799	HIPAA
				Authorization and/or supervision Workstation Use Workstation Security Disposal Media Re-use Accountability
Part 3 - Defence				
3.1	**Detection**	Detection	12.4 Logging and monitoring	Information Security Activity Review
		Logging	12.4 Logging and monitoring 12.7 Information systems audit considerations	Audit controls
		Logs correlation and analysis	12.4 Logging and monitoring 12.7 Information systems audit considerations	Audit controls
3.2	**Computer security incident management**	Information system security incident response	16.1 Management of information security incidents and improvements	Information Security Activity Review Protection Against Malicious Software Data Backup Plan Testing and Revision Procedures
		Incident report	16.1 Management of information security incidents and improvements	Information Security Activity Review
		Communication with competent authorities	–	–
Part 4 - Resilience				
4.1	**Continuity of Operations**	Business continuity management	17.1 Information security continuity 17.2 Redundancies	Contingency Plan Testing and Revision Procedures Disaster Recovery Plan Applications and Data Criticality Analysis
		Disaster recovery management	17.1 Information security continuity	Disaster Recovery Plan

D/N	DOMAIN NAME	SECURITY MEASURE	ISO 27799	HIPAA
			17.2 Redundancies	
4.2	**Crisis Management**	Crisis management organization	17.1 Information security continuity 17.2 Redundancies	Contingency Plan Testing and Revision Procedures Disaster Recovery Plan Applications and Data Criticality Analysis
		Crisis management process	17.1 Information security continuity 17.2 Redundancies	Contingency Plan Testing and Revision Procedures Disaster Recovery Plan Applications and Data Criticality Analysis

Table 15: Mapping of security measures with Healthcare sector specific standards

2.5 Drinking Water Supply & Distribution

Table 16 below, lists international information security standards and good practices applicable to the Drinking Water Supply and Distribution sector.

SECTOR	STANDARDS	GOOD PRACTICES
Drinking Water Supply and Distribution	• ISO 27001 Information technology — Security techniques — Information security management systems — Requirements • ANSI/ISA, Series "ISA-62443: Security for industrial automation and control system"	• ANSI/AWWA G430-09/"Security Practices for Operations and Management"

Table 16: International standards and good practices specific to the Drinking Water Supply & Distribution sector

According to the input by EU drinking water operators, the most applicable standards for this sector are ISO-27001 and ISA/IEC62443, for which the mapping with the security measures is presented in **section 3**, **Table 22**.

Nevertheless, it's worth mentioning the standard ANSI/AWWA G430-09/"Security Practices for Operations and Management" [42] published by the American Water Works Association which purpose is to define the minimum requirements for a protective security program for a water or wastewater utility, that will promote the protection of employee safety, public health, public safety, and public confidence. The ANSI/AWWA G430-09 standard is applied in United States and it is not publicly available.

2.6 Digital Infrastructures

Table 17 lists international standards and good practices specific to the Digital Infrastructures.

[42] https://www.iso.org/standard/43751.html

SECTOR	STANDARDS	GOOD PRACTICES
Digital Infrastructure	• ISO/IEC 27011:2008 Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	• Technical guidance on the security measures for Telcos in Article 13a, ENISA • Best Practices – IX-F

Table 17: International standards and good practices specific to the Digital Infrastructures sector

According to input taken by Digital Infrastructures operators in EU, **Table 18**, illustrates the mapping of security measures to sector specific standards, such as:

- **ISO/IEC 27011:2008**[43] which refers to Information security management guidelines for telecommunications organizations and it is based on ISO/IEC 27001:2013.

D/N	DOMAIN NAME	SECURITY MEASURE	ISO 27011
Part 1 – Governance and Ecosystem			
1.1	**Information System Security Governance & Risk Management**	Information system security risk analysis	–
		Information system security policy	# 4.2 Information security management systems in telecommunications business # 5. Security Policy
		Information system security accreditation	–
		Information system security indicators	–
		Information system security audit	–
		Human resource security	# 8.1 Prior to employment # 8.2 During employment # 8.3 Termination or change of employment
		Asset Management	7. Asset management
1.2	**Ecosystem Management**	Ecosystem mapping	# 6.1 Internal organization # 6.2 External Parties
		Ecosystem relations	# 6.2 External Parties # 10.2 Third party service delivery management
Part 2 – Protection			

[43] ISO/IEC 27011:2008 - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002; URL: https://www.iso.org/standard/43751.html

D/N	DOMAIN NAME	SECURITY MEASURE	ISO 27011
2.1	**IT Security Architecture**	Systems configuration	# 12.1 Security requirements of information systems # 12.2 Correct processing in applications
		System segregation	# 10.6 Network security management
		Traffic filtering	# 10.8 Exchange of information
		Cryptography	# 12.3 Cryptographic controls
2.2	**IT Security Administration**	Administration accounts	# 11.2 User access management
		Administration information systems	# 11.2 User access management
2.3	**Identity and access management**	Authentication and identification	# 11.1 Business requirement for access control # 11.4 Network access management # 11.5 Operating system access control # 11.6 Application and information access control
		Access rights	# 11.2 User access management # 11.3 User responsibilities
2.4	**IT security maintenance**	IT security maintenance procedure	–
		Remote access	# 11.7 Mobile Computing and teleworking
2.5	**Physical and environmental security**	Physical and environmental security	# 9.1 Secure areas # 9.2 Equipment security
Part 3 - Defence			
3.1	**Detection**	Detection	# 10.10 Monitoring
		Logging	# 10.10 Monitoring
		Logs correlation and analysis	# 10.10 Monitoring
3.2	**Computer security incident management**	Information system security incident response	# 13.2 Management of information security incidents and improvements
		Incident report	# 13.1 Reporting information security events and weaknesses

D/N	DOMAIN NAME	SECURITY MEASURE	ISO 27011
		Communication with competent authorities	–
Part 4 - Resilience			
4.1	**Continuity of Operations**	Business continuity management	# 14.1 Information security aspects of business continuity management
		Disaster recovery management	# 14.1 Information security aspects of business continuity management
4.2	**Crisis Management**	Crisis management organization	–
		Crisis management process	–

Table 18: Mapping of security measures with Digital Infrastructure sector specific standard

2.7 Matching of baseline security measures with sectors

Table 19 summarizes the matching of the proposed security measures with sector-specific international standards, regulations and well accepted good practices of Energy and Transport sector, that were presented in more details above.

DOMAIN NAMES	SECURITY MEASURES	ENERGY					TRANSPORT				
		ELECTRICITY			OIL & GAS		AIR		RAIL	WATER	ROAD
		NIST SP 800-82	ISO 27019	NERC CIP	API STD 1164	ONG-C2M2	ICAO	AIAA	(TABLE 22)	BIMCO	(TABLE 22)
Part 1 – Governance and Ecosystem											
Information System Security Governance & Risk Management	Information system security risk analysis	●	●	●	●	●	●	●	–	●	–
	Information system security policy	●	●	●	●	●	●	●	–	–	–
	Information system security accreditation	●	–	–	–	–	●	●	–	–	–
	Information system security indicators	●	–	–	–	–	–	–	–	–	–
	Information system security audit	●	●	●	●	–	–	–	–	–	–
	Human resource security	●	●	●	●	●	–	●	–	●	–

DOMAIN NAMES	SECURITY MEASURES	ENERGY					TRANSPORT				
		ELECTRICITY			OIL & GAS		AIR		RAIL	WATER	ROAD
		NIST SP 800-82	ISO 27019	NERC CIP	API STD 1164	ONG-C2M2	ICAO	AIAA	(TABLE 22)	BIMCO	(TABLE 22)
	Asset Management	●	●	●	●	●	●	●	–	●	–
Ecosystem Management	Ecosystem mapping	–	●	–	●	●	●	●	–	●	–
	Ecosystem relations	–	●	–	●	●	●	●	–	●	–
Part 2 – Protection											
IT Security Architecture	Systems configuration	●	●	●	●	●	●	–	–	●	–
	System segregation	●	●	●	●	–	●	●	–	●	–
	Traffic filtering	●	●	–	●	–	●	●	–	●	–
	Cryptography	●	●	●	●	–	●	●	–		–
IT Security Administration	Administration accounts	●	●	●	●	●	–	●	–	●	–
	Administration information systems	–	●	●	●	–	–	–	–	●	–

DOMAIN NAMES	SECURITY MEASURES	ENERGY					TRANSPORT				
		ELECTRICITY			OIL & GAS		AIR		RAIL	WATER	ROAD
		NIST SP 800-82	ISO 27019	NERC CIP	API STD 1164	ONG-C2M2	ICAO	AIAA	(TABLE 22)	BIMCO	(TABLE 22)
Identity and access management	Authentication and identification	●	●	●	●	●	●	–	–	●	–
	Access rights	●	●	●	●	●	●		–	–	–
IT security maintenance	IT security maintenance procedure	●	●	●	●	–	●	—	–	●	–
	Remote access	●	●	●	●	–	●	–	–	●	–
Physical and environmental security	Physical and environmental security	●	●	●	●	–	–	–	–	●	–
Part 3 - Defence											
Detection	Detection	●	–	●	●	●	●	●	–	●	–
	Logging	●	●	●	●	●		●	–	–	–
	Logs correlation and analysis	●	●	●	●	–		●	–	–	–
Computer security incident management	Information system security incident response	●	●	●	●	●	●	●	–	–	–

DOMAIN NAMES	SECURITY MEASURES	ENERGY					TRANSPORT				
		ELECTRICITY			OIL & GAS		AIR		RAIL	WATER	ROAD
		NIST SP 800-82	ISO 27019	NERC CIP	API STD 1164	ONG-C2M2	ICAO	AIAA	(TABLE 22)	BIMCO	(TABLE 22)
	Incident report	●	●	●	–	●	●	●	–	–	–
	Communication with competent authorities	–	●	●	●	●	●	●	–	●	–
Part 4 - Resilience											
Continuity of Operations	Business continuity management	●	●	●	●	●	●	–	–	●	–
	Disaster recovery management	●	●	●	–	–	●	–	–	●	–
Crisis Management	Crisis management organization	●	●	●	–	–	●	–	–	●	–
	Crisis management process	●	●	●	–	–	●	–	–	●	–

Table 19: **Overview of the proposed security measures with Energy and Transport sector-specific international standards, regulations and good-practices**

Table 20 summarizes the matching of the proposed security measures with sector-specific international standards, regulations and well accepted good practices of Financial & Banking, Healthcare, Drinking Water and Digital Infrastructures sectors, that were presented in more details above.

DOMAIN NAMES	SECURITY MEASURES	FINANCIAL AND BANKING					HEALTHCARE		DRINKING WATER SUPPLY AND DISTRIBUTION	DIGITAL INFRASTRUCTURES
		PSD2	PCI-DSS	ISO/TR 13569:2005	GLBA	SOX	ISO27799	HIPAA	(Table 22)	ISO 27011
Part 1 – Governance and Ecosystem										
Information System Security Governance & Risk Management	Information system security risk analysis	●	–	●	●	–	●	●	–	–
	Information system security policy	●	●	●	●	●	●	●	–	●
	Information system security accreditation	●	–	●	●	●	●	●	–	–
	Information system security indicators	●	●	●	●	●	●	●	–	–
	Information system security audit	●	–	●	●	●	●	●	–	–
	Human resource security	●	–	●	●	–	●	●	–	●
	Asset Management	●	●				●	●	–	●

Ecosystem Management	Ecosystem mapping	●	–	●	●	●	●	–	–	●
	Ecosystem relations	●	–	●	●	●	●	–	–	●
Part 2 - Protection										
IT Security Architecture	Systems configuration	●	●	●	●	–	●	–	–	●
	System segregation	●	–	●	●	–	●	–	–	●
	Traffic filtering	●	–	●	●	–	●	–	–	●
	Cryptography		●	●	●	–	●	–	–	●
IT Security Administration	Administration accounts	●	●	●	●	–	–	–	–	●
	Administration information systems	●	–	●	●	–	–	–	–	●
Identity and access management	Authentication and identification	●	●	●	●	–	●	●	–	●
	Access rights	●	●	●	●	●	●	●	–	●
IT security maintenance	IT security maintenance procedure	●	●	●	●	–	●	●	–	–
	Remote access	●	–	–	–	–	●	●	–	●

Physical and environmental security	Physical and environmental security	●	●	●	●	–	●	●	–	●
Part 3 - Defence										
Detection	Detection	●	–	●	●	●	●	●	–	●
	Logging	●	●	●	●	●	●	●	–	●
	Logs correlation and analysis	●	–	●	–	●	●	●	–	●
Computer security incident management	Information system security incident response	●	–	●	●	●	●	●	–	●
	Incident report	●	–	●	●	●	●	●	–	●
	Communication with competent authorities	●	–	●	●	●	–	–	–	–
Part 4 - Resilience										
Continuity of Operations	Business continuity management	●	–	–	●	–	●	●	–	●
	Disaster recovery management	●	–	●	●	–	●	●	–	●
Crisis Management	Crisis management organization	●	–	●	●	–	●	●	–	–

	Crisis management process	●	–	●	●	–	●	●	–	–

Table 20: Overview of the proposed security measures with Energy and Transport sector-specific international standards, regulations and good-practices

3 Mapping the Baseline Security Measures for OES to cross sector international standards

Table 21 lists international standards and good practices applicable across all the sectors referred to in the NIS Directive.

SECTOR	STANDARDS	GOOD PRACTICES
Cross sector	• **ANSI/ISA, Series "ISA-62443: Security for industrial automation and control system"** • **ISO 27001 Information Technology Security Techniques Information Security Management Systems Requirements** • **NIST Framework for Improving Critical Infrastructure Cybersecurity** • ISO/IEC 27002:2013: Code of practice for information security controls • ISO 27003 - Information technology -- Security techniques -- Information security management system implementation guidance • ISO/IEC 27004:2016 Information technology -- Security techniques -- Information security management -- Monitoring, measurement, analysis and evaluation • ISO/IEC 20000-1:2011 Information technology -- Service management -- Part 1: Service management system requirements • ISO/IEC 27010:2015 Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications • ISO/IEC 21827:2008 Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®) • ISO/IEC 10181-2:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Authentication framework • ISO/IEC 27013:2015 Information technology -- Security techniques -- Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 • ISO/IEC 27014:2013 Information technology — Security techniques — Governance of information security • ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cybersecurity • ISO/IEC 27033-1:2015 Information technology -- Security techniques -- Network security -- Part 1: Overview and concepts • ISO/IEC 27034-1:2011 Information technology -- Security techniques -- Application security -- Part 1: Overview and concepts • ISO/IEC TR 19791:2010 Information technology -- Security techniques -- Security assessment of operational systems	• The CIS Critical Security Controls for Effective Cyber Defence Version 6.1 • Organisation for Economic Co-operation and Development (OECD), Guidelines for the Security of Information Systems and Networks, 2002, • Generally Accepted Information Security Principles (GAISP) – ISSA • The Open Group Open Information Security Management Maturity Model (O-ISM3) • ISACA BMIS • IT Baseline Protection Manual Standard Security Measures – BSI • UK Cyber Essentials (CREST) • Cyber Defence Capability Assessment Tool (CDCAT®) – CESG • HMG Security Policy Framework (SPF) – CESG • NIST/NSA/DISA/DoD Security Technical Implementation Guides (STIGs) • Carnegie Melon Capability Maturity Model (CMM)

	• European Telecommunications Standards Institute (ETSI) Cybersecurity Standards TR 103 303 - TR 103 309 CYBER series • TR 103 331 CYBER; Structured threat information sharing • TR 103 369 CYBER; Design requirements ecosystem • TS 103 487 CYBER; Baseline security requirements regarding sensitive functions for NFV and related platforms • IT Infrastructure Library (ITIL) v3 • NIST SP 800-53 • Information Assurance for SMEs (IASME) • ISF Standard of Good Practice for Information Security • ITU X series : Information security management framework	

Table 21: International standards and good practices applicable across all the sectors

The **Table 22** depicts the mapping of the information security measures identified and agreed in the NIS Directive Cooperation Group to the international information security standards applied to all the sectors referred to in the NIS Directive.

The standards and good practices, that are usually applied by the operators of all the sectors referred to in the NIS Directive, were identified through the survey filled in by the Cooperation Group representatives, as well as by the feedback provided by EU operators, are:

- ISO 27001 Revision 2013, which is the most globally widespread standard covering all aspects of information security management systems across all the sectors.
- ISA/IEC 62443, which is a series of standards that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS). This guidance applies to end-users (i.e. asset owner), system integrators, security practitioners, and control systems manufacturers responsible for manufacturing, designing, implementing, or managing industrial automation and control systems.
- NIST Cybersecurity Framework, which despite the fact that is not compulsory even in the U.S., it is usually followed by EU operators that work beyond EU's territory as it is a good point of reference for cybersecurity requirements.

D/N	DOMAIN NAME	SECURITY MEASURE	ISO 27001:2013	NIST CYBER SECURITY FRAMEWORK	ISA/IEC 62443 3-3
Part 1 – Governance and Ecosystem					
1.1	**Information System Security Governance & Risk Management**	Information system security risk analysis	# 8.2 Information security risk assessment (ISO 27001) # 8.3 Information security risk treatment (ISO 27001)	ID.GV-4 ID.RA-1,2,3,4,5,6 D.RM-1,2,3 PR.AT-2	SR 5.2, 5.3,
		Information system security policy	# 5.1 Management direction for information security	ID.GV-1,2,3	–

D/N	DOMAIN NAME	SECURITY MEASURE	ISO 27001:2013	NIST CYBER SECURITY FRAMEWORK	ISA/IEC 62443 3-3
		Information system security accreditation	# 12.7.1 Information systems audit controls	–	SR 2.8, 2.9, 2.10, 2.12
		Information system security indicators	# 12.1.3.Capacity Management	–	SR 1.4, 3.9, 6.1
		Information system security audit	# 9.2 Internal Audit (ISO 27001)	PR.PT-1	SR 2.8, 2.9, 2.10, 2.11, 2.12, 3.9,
		Human resource security	# 7.1 Prior to employment # 7.2 During employment # 7.3 Termination and change of employment	PR.AT-1,2,3,4,5	SR 1.1
		Asset Management	A.8 Asset management	PE-20 Asset Monitoring and Tracking CM-8 Information System Component Inventory	SR 7.2 – Resource management
1.2	**Ecosystem Management**	Ecosystem mapping	# 15.1 Information security in supplier relationships	ID.BE-1,2	–
		Ecosystem relations	# 15.2 Supplier service delivery management	ID.BE-3,4 PR.AT-3	SR 1.1, 1.13, 2.6
Part 2 – Protection					
2.1	**IT Security Architecture**	Systems configuration	# 12.1.1 Documented operating procedures # 12.5 Control of operational software	PR.IP-1,3	SR 2.5, 2.6, 2.7, 3.4, 3.5, 3.6, 3.7, 7.6, 7.7
		System segregation	# 13.1 Network security management	PR.AC-5	
		Traffic filtering	# 12.5 Control of operational software # 12.6 Technical vulnerability management	–	SR 6.2, 7.1, 7,2
		Cryptography	# 10.1 Cryptographic controls	–	SR 1.8, 1.9,

D/N	DOMAIN NAME	SECURITY MEASURE	ISO 27001:2013	NIST CYBER SECURITY FRAMEWORK	ISA/IEC 62443 3-3
2.2	**IT Security Administration**	Administration accounts	# 9.2 User access management	PR.AT-2	SR 1.3, 1.4,
		Administration information systems	# 9.4 System and application access control	PR.AT-2	SR 2.1,
2.3	**Identity and access management**	Authentication and identification	# 9.1 Business requirements of access control	PR.AC-1	SR 1.1, 1.2, 1.5, 1.7, 1.10, 1.11
		Access rights	# 9.2 User access management	ID.AM-5,6 PR.AC-1,4	SR 2.1, 2.5,
2.4	**IT security maintenance**	IT security maintenance procedure	# 14.1 Security requirements of information systems # 14.2 Security in development and support processes	PR.IP-2 PR.MA-1,2	SR 3.3, 3.4, 3.7
		Remote access	# 6.2 Mobile devices and teleworking	PR.AC-3	SR 1.6, 1.13, 2.2, 2.6,
2.5	**Physical and environmental security**	Physical and environmental security	#11.1 Secure areas #11.2 Equipment	PR.AC-2 PR.IP-5	SR 1.1, 1.5
Part 3 - Defence					
3.1	**Detection**	Detection	# 12.4 Logging and monitoring	DE.AE-1 DE.CM-1,2,3,4,5,6,7,8 DE.DP-1,2,3,4,5	SR 3.1, 3.2
		Logging	# 12.4 Logging and monitoring	DE.CM-1	SR 6.1
		Logs correlation and analysis	# 12.4 Logging and monitoring	DE.CM-1	SR 6.1
3.2	**Computer security incident management**	Information system security incident response	# 16.1.4 Management of information security incidents and improvements # 16.1.5 Response to information security incidents	DE.AE-2,3,4,5 RS.AN-1,2,3,4 PR.IP-9 RS.RP-1 RS.CO-1 RS.MI-1,2,3	SR 6.1, 6.2

D/N	DOMAIN NAME	SECURITY MEASURE	ISO 27001:2013	NIST CYBER SECURITY FRAMEWORK	ISA/IEC 62443 3-3
		Incident report	# 16.1.5 Response to information security incidents	RS.CO-1,2,3,4,5	SR 6.2
		Communication with competent authorities	–	–	–
Part 4 - Resilience					
4.1	**Continuity of Operations**	Business continuity management	# 17.1 Information security continuity	ID.BE-5 PR.DS-4 PR.IP-4	SR 7.3, 7.4
		Disaster recovery management	# 17.2 Redundancies	PR.DS-4 PR.IP-10	SR 7.4, 7.5
4.2	**Crisis Management**	Crisis management organization	# 17.1 Information security continuity	PR.DS-4 PR.IP-10	SR 7.4, 7.5
		Crisis management process	# 17.1 Information security continuity	PR.DS-4	SR 7.4, 7.5

Table 22: Mapping of the information security measures to the international information security standards applied to all the sectors

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

Catalogue Number

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN 978-92-9204-232-5,
DOI 10.2824/844702