University of Piraeus

School of Information and Communication Technologies

Department of Digital Systems

Postgraduate Program of Studies

Digital Systems Security

Master Thesis: *“Security Controls and Security Standards: Correlations and Synergies”*

Διπλωματική Εργασία*: “Βιβλιοθήκες Σημείων Ελέγχου (Security Controls) και Πρότυπα Ασφάλειας: Συσχετίσεις και Συνέργειες”*

Supervisor Professor: Konstantinos Lambrinoudakis

Name-Surname	E-mail	Student ID.
Christos Venizelos	x.venizelos@ssl-unipi.gr	MTE2002

Piraeus

13/08/2022

Acknowledgments

I would firstly like to express my gratitude to my supervisor Professor Mr. Konstantinos Lambrinoudakis, for his contribution by providing me with assistance and helpful guidelines during the development of this thesis.

In addition, I would like to thank my family and friends for their continuous support and understanding throughout this effort.

Table of Contents

Table of Tables

Table of Figures

Abbreviations and Acronyms

CER	Critical Entities Resilience
CG	Cooperation Group
CIS	Critical Security Control
CSIRT	Computer Security Incident Response Team
DORA	Digital Operational Resilience Act
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSP	Digital Service Provider
ENISA	European Union Agency for Network and Information Security
ESAs	European Supervisory Authorities
EU	European Union
GDPR	General Data Protection Regulation
ICS	Industrial Control Systems
ICT	Information And Communications Technology
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISSP	Information System Security Policy
NIS Directive	Network and Information Security Directive
OES	Operators of Essential Service
SPOC	Single Points of Contact

Abstract

The digital transformation of organisations continuously increases their exposure to malicious threats, vulnerabilities and attacks. Given this, organisations are required to establish, implement and enforce multiple controls from different regulatory and frameworks such as ISO/IEC 27001, NIS Directive and GDPR. Therefore, this thesis aims to explain, analyze and correlate these regulatory and frameworks. Initially, Chapter 1 defines what an Information Security Management System (ISMS) is, why it is considered important, and what are its benefits. In addition, it is provided an analysis of the updated and revised controls of ISO/IEC 27002. Chapter 2 defines and analyzes the NIS Directive 2016/1148 (NIS Directive) and its updated version of the NIS 2 Directive. Furthermore, Chapter 3 addresses the General Data Protection Regulation (GDPR) and the mapping of its Articles to appropriate domains. Finally, Chapter 4 has been carried out a mapping of the controls of ISO/IEC 27002:2013, ISO/IEC 27002:2022, NIS Directive and GDPR.

Keywords: ISO/IEC 27001, Information Security Management System, ISO/IEC 27002:2013, ISO/IEC 27002:2022, NIS 1 Directive, NIS 2 Directive, General Data Protection Regulation.

Περίληψη

Ο ψηφιακός μετασχηματισμός των οργανισμών συνεχώς αυξάνει την έκθεση του σε κακόβουλές απειλές, ευπάθειες και επιθέσεις. Δεδομένου αυτού, οι οργανισμοί καλούνται να εγκαθιδρύσουν, να εφαρμόσουν και να υλοποιήσουν πολλαπλά σημεία ελέγχου από διαφορετικά κανονιστικά πλαίσια και πλαίσια ελέγχων όπως το ISO/IEC 27001, την Οδηγία 2016/1148 (NIS Directive). και τον ΓΚΠΔ. Ως εκ τούτου, η παρούσα διπλωματική έχει ως στόχο να ορίσει, να αναλύσει και να συσχετίσει αυτές τις κανονιστικές ρυθμίσεις και τα πλαίσια. Αρχικά, το Κεφάλαιο 1 ορίζει τι είναι το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ), γιατί θεωρείται σημαντικό, καθώς και ποια θεωρούνται τα πλεονεκτήματα του. Επιπρόσθετα, γίνεται ανάλυση στα επικαιροποιημένα σημεία ελέγχου του ISO/IEC 27002. Το Κεφάλαιο 2, ορίζει και αναλύει την Οδηγία 2016/1148 (NIS Directive) και την επικαιροποιμένη της έκδοση της Οδηγίας 2 (NIS 2 Directive). Επιπρόσθετα, το Κεφάλαιο 3 αναφέρεται στο Γενικό Κανόνα Προστασίας Δεδομένων (ΓΚΠΔ) και στην αντιστοίχιση των άρθρων του σε κατάλληλες ενότητες. Τέλος, στο Κεφάλαιο 4 έχει πραγματοποιηθεί η συσχέτιση των σημείων ελέγχου ανάμεσα στο ISO/IEC 27002:2013, στο ISO/IEC 27002:2022, στην Οδηγία 2016/1148 και στο ΓΚΠΔ.

Λέξεις Κλειδιά: ISO/IEC 27001, Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών, ISO/IEC 27002:2013, ISO/IEC 27002:2022, Οδηγία 2016/1148, Οδηγία 2 2016/1148, Γενικός κανονισμός για την Προστασία Δεδομένων.

Introduction

During the last decades, the e-services, new technologies, information systems and networks have become embedded in our daily lives, increasing the deliberated incidents causing disruption of IT services and critical infrastructures constitute a serious threat to their operation and consequently to the functioning of the Internal Market and the Union. This risk, combined with the fact that existing counter-measures in terms of security tools and procedures are not sufficiently developed in the European Union (EU), and certainly not common in all Member States, has made the need for a comprehensive approach at the Union level, concerning the security of network and information systems, unquestionable [1].

Likewise, nowadays, the coronavirus pandemic has triggered an unforeseen acceleration in the digital transformation of societies around the world. Furthermore, it has exacerbated existing problems, such as the digital divide, and contributed to a global rise in cybersecurity incidents. During this unprecedented situation, there has been an increase in malicious cyber-activity across Member States, as revealed by a recent Europol report. Cybersecurity issues are becoming a day-to-day struggle for the EU. Therefore, cyber-attacks growing in scale, cost and sophistication and also it is considered among the fastest-growing form of crime worldwide. For instance, in 2017, Cybersecurity Ventures forecast that global ransomware damage costs would reach US$20 billion by 2021, 57 times more than the amount in 2015. It also predicted that companies would be suffering a ransomware attack every 11 seconds by 2021, up from every 40 seconds in 2016 [2].

The first step towards the creation and development of an EU cybersecurity ecosystem was the adoption of a cybersecurity strategy in 2013. The strategy identified the achievement of cyber resilience and the development of industrial and technological resources for cybersecurity as its key objectives. The Directive on Security of Network and Information Systems across the EU (the NIS Directive), which had to be transposed by 27 Member States by 9 May 2018, represents the first piece of EU-wide legislation on cybersecurity and its specific aim was to achieve a high common level of cybersecurity across the Member States [2]. The NIS Directive aims to address this need by putting forward "the measures with a view to achieving a high common level of security of network and information systems within the functioning of the internal market" [3]. While it increased the Member States' cybersecurity capabilities, its implementation proved difficult, resulting in fragmentation at different levels across the internal market. To respond to the growing threats posed with digitalization and the surge in cyber-attacks, the Commission has submitted a proposal to replace the NIS Directive and thereby strengthen the security requirements, address the security of supply chains, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonized sanctions across the EU. The proposed expansion of the scope covered by NIS 2 Directive, by effectively obliging more entities and sectors to take measures, would assist in increasing the level of cybersecurity in Europe in the longer term.

Furthermore, on 27 April 2016, the EU Commission received an additional General Data Protection Regulation (GDPR) that would have a full impact on 25 May 2018, removing all EU member states' surrounding national data security rules even in the context of the DPD (Commission, 2015). The latest guidance includes numerous basic concepts and aims to easily introduce and recognize relations within the EU. Among the most important news in GDPR was that it was a new guideline to submit another fining framework. This framework states that any corporation that does not meet the new directive could be punished up to 4% of its annual global profit, making this a real challenge. Also, organizations and companies as must be GDPR-compliant quickly as possible (EC 2015) [3].

Last but not least, another leading international standard focused on information security, published by the International Organization for Standardization (ISO), in partnership with the International Electrotechnical Commission (IEC) is considered the ISO/IEC 27001. The full name of ISO 27001 is “ISO/IEC 27001 – Information technology — Security techniques — Information security management systems — Requirements.” In addition, ISO/IEC 27001 is part of a set of standards developed to handle information security and particularly the ISO/IEC 27000 series. The basic goal of ISO/IEC 27001 is to protect three (3) aspects of information and particularly

- Confidentiality: only the authorized persons have the right to access information.
- Integrity: only the authorized persons can change the information.
- Availability: the information must be accessible to authorized persons whenever it is needed

In addition, ISO/IEC 27001 Annex A provides a detailed list of 93 controls (also known as safeguards) that should be implemented to reduce risks to an acceptable levels. These controls are organized in the following four (4) sections [4]:

- Organizational controls, including 37 controls.
- People controls, including 8 controls
- Physical controls, including 14 controls.
- Technological controls, including 34 controls

Chapter 1: ISO/IEC 27001

1.1 Information Security Management Systems (ISMS)

An Information Security Management System (ISMS) consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security program to achieve business objectives. It is based upon risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks. Analyzing requirements for the protection of information assets and applying appropriate controls to ensure the protection of these information assets, as required, contributes to the successful implementation of an ISMS. The following fundamental principles also contribute to the successful implementation of an ISMS [5]:

- Awareness of the need for information security.
- Assignment of responsibility for information security.
- Incorporating management commitment and the interests of stakeholders.
- Enhancing societal values.
- Risk assessments determining appropriate controls to reach acceptable levels of risk.
- Security incorporated as an essential element of information networks and systems.
- Active prevention and detection of information security incidents.
- Ensuring a comprehensive approach to information security management and
- Continual reassessment of information security and making of modifications as appropriate.

1.1.1 Why an ISMS is important

Risks associated with an organization's information asset need to be addressed. Achieving information security requires the management of risk, and encompasses risks from physical, human and technology related threats associated with all forms of information within or used by the organization. The adoption of an ISMS is expected to be strategic decisions for an organization and it is necessary that this decision is seamlessly integrated, scaled and updated in accordance with the needs of the organization. The design and implementation of an organization's ISMS is influenced by the need and objectives of the organizations, security requirements, the business processes employed and the size and structures of the organization. The design and operation of an ISMS needs to reflect the interests and information security requirement of all of the organization's stakeholders including customers, suppliers, business partners, shareholders and other relevant third parties [5].

In an interconnected world, information and related processes, systems, and networks constitute critical business assets. Organizations and their information systems and networks face security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire and flood. Damage to information systems and networks caused by malicious code, computer hacking, and denial of service attacks have become more common, more ambitious, and increasingly sophisticated [5].

An ISMS is important to both public and private sector businesses. In any industry, an ISMS is an enabler that support e-business and is essential for risk management activities. The interconnection of public and private networks and the sharing of information assets increase the difficulty of controlling access to and handling of information. In addition, the distribution of mobile storage devices containing information assets weaken the effectiveness of traditional controls. When organizations adopt the ISMS family of standards, the ability to apply consistent and mutually-recognizable information security principles can be demonstrated to business partners and other interested parties [5].

Information security is not always taken into account in the design and development of information systems. Further, information security is often thought of as being a technical solution. However, the information security that can be achieved through technical means is limited and can be ineffective without being supported by appropriate management and procedures within the context of an ISMS. Integrating security into functionally complete information system can be difficult and costly. An ISMS involves identifying which controls are in place and requires careful planning and attention to detail. As an example, access controls, which can be technical (logical), physical, administrative (managerial) or a combination, provide a means to ensure that access to information assets is authorized and restricted based on the business and information security requirements. The successful adoption of an ISMS is important to protect information assets allowing an organization to [5]:

- achieve greater assurance that its information assets are adequately protected against threats on a continual basis,
- maintain a structured and comprehensive framework for identifying and assessing information security risks, selecting and applying applicable controls and measuring and improving their effectiveness,
- continually improve its control environment, and
- effectively achieve legal and regulatory compliance.

1.1.2 Benefits of the ISMS family of standards

The benefits of implementing an ISMS primarily result from a reduction in information security risks (i.e., reducing the probability of and/or impact caused by information security incidents). Specifically, benefits realized for an organization to achieve sustainable success from the adoption of the ISMS family of standards include the following [5]:

- a structured framework supporting the process of specifying, implementing, operating and maintaining a comprehensive, cost-effective, value creating, integrated and aligned ISMS that meets the organization's need across different operations and sites,
- assistance for management in consistently managing and operating in a responsible manner their approach towards information security management, within the context of corporate risk management and governance, including educating and training business and system owners on the holistic management of information security,

- promotion of globally accepted, good information security practices in a non-prescriptive manner, giving organizations the latitude to adopt and improve relevant controls that suit their specific circumstances and to maintain them in the face of internal and external changes,
- provision of a common language and conceptual basis for information security, making it easier to place confidence in business partners with a compliant ISMS, especially if they require certification against ISO/IEC 27001 by an accredited certification body,
- increase in stakeholder trust in the organization,
- satisfying societal needs and expectations,
- more effective economic management of information security investments.

1.2 ISMS family standards

The ISMS family of standards consists of inter-related standards, already published or under development, and contains a number of significant structural components. These components are focused on [5]:

- standards describing ISMS requirements (ISO/IEC 27001) and
- certification body requirements (ISO/IEC 27006) for those certifying conformity with ISO/IEC 27001.
- additional requirement framework for sector-specific implementation of the ISMS (ISO/IEC 27009)

Other standards provide guidance for various aspects of an ISMS implementation, addressing a generic process, control-related guidelines as well as sector-specific guidance. Relationships between the ISMS family of standards are the following [5]:

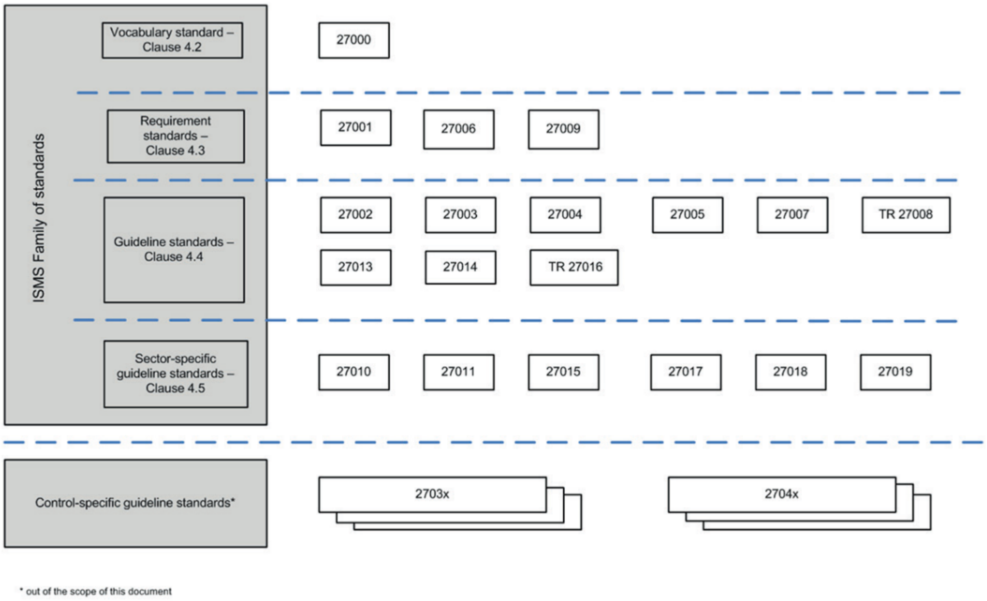
ISMS Family of standards
Vocabulary standard – Clause 4.2
27000
Requirement standards – Clause 4.3
27001
27006
27009
Guideline standards – Clause 4.4
27002
27003
27004
27005
27007
TR 27008
27013
27014
TR 27016
Sector-specific guideline standards – Clause 4.5
27010
27011
27015
27017
27018
27019
Control-specific guideline standards*
2703x
2704x
* out of the scope of this document

Figure 1: ISMS family of standards relationship

Each of the ISMS family standards is described below by its type (or role) within the ISMS family of standards and its reference number. In the below table, it is presented some example of the ISO 27000 family of standards [5]:

Example of ISO/IEC 27000 Family			
Number	**Title**	**Scope**	**Purpose**
ISO/IEC 27000	Information technology — Security techniques — Information security management systems — Overview and vocabulary	Scope: This document provides to organizations and individuals: a) an overview of the ISMS family of standards; b) an introduction to information security management systems; and	This document describes the fundamentals of information security management systems, which form the subject of the ISMS family of

		c) terms and definitions used throughout the ISMS family of standards.	standards and defines related terms,
ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements	This document specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving formalized information security management systems (ISMS) within the context of the organization's overall business risks. It specifies requirements for the implementation of information security controls customized to the needs of individual organizations or parts thereof. This document can be used by all organizations, regardless of type, size and nature	ISO/IEC 27001 provides normative requirements for the development and operation Of an ISMS, including a set of controls for the control and mitigation of the risks associated with the information assets which the organization seeks to protect by operating its ISMS. Organizations operating an ISMS may have its conformity audited and certified. The control objectives and controls from ISO/IEC 27001, Annex A shall be selected as part of this ISMS process as appropriate to cover the identified requirements. The control objectives and controls listed in ISO/IEC 27000, Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002, Clauses 5 to 8.
ISO/IEC 27002	Information technology — Security techniques — Code of practice for information security controls	This document provides a list Of commonly accepted control Objectives and best practice controls to be used as implementation guidance when selecting and implementing controls for achieving information security.	ISO/IEC 27002 provides guidance on the implementation Of information security controls. Specifically, Clauses 5 to 8 provide specific implementation advice and guidance on best practice in support of the controls specified ISO/IEC 27001 5 to 8.
ISO/IEC 27005	Information technology — Security techniques — Information security risk management	This document provides guidelines for information security risk management, The approach described within this document supports the general concepts specified in ISO/IEC 27001.	ISO/IEC 27005 provides guidance implementing a process-oriented risk management approach to assist in satisfactorily implementing and fulfilling the information security risk management requirements of ISO/IEC 27001.
ISO/IEC 27017	Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services	ISO/IEC 27017 gives guidelines for information security controls applicable to the provision and use of cloud services by providing: • additional implementation guidance for relevant controls specified in ISO/IEC 27002,	This document provides controls and implementation guidance for both cloud service providers and cloud service customers.

		• additional controls with implementation guidance that specifically relate to cloud services.	

Table 1: Example of ISO/IEC 27000 Family standards

1.3 ISO/IEC 27001 Standard

ISO/IEC 27001 is widely known, providing requirements for an Information Security Management System (ISMS), though there are more than a dozen standards in the ISO/IEC 27000 family [6]. This report focuses on ISO/IEC 27001 which is the series of best practices to help organisations to improve their information security and ISO/IEC 27002 which is a supplementary standard that provides an overview of information security controls that organisations should choose to implement. The controls are outlined in Annex A of ISO 27001, but whereas this is essentially a quick rundown, ISO/IEC 27002 contains a more comprehensive overview, explaining how each control works, what its purpose is and how you can implement it. ISO/IEC 27001 is published by ISO (the International Organization for Standardization) and the IEC (International Electrotechnical Commission), the series explains how to implement best-practice information security practices [7]. ISO/IEC 27001 contains the following clauses [8]:

- Clause 1 - Scope,
- Clause 2 - Normative references,
- Clause 3 - Terms and definitions,
- Clause 4 - Context,
- Clause 5 - Leadership,
- Clause 6 - Planning and risk management
- Clause 7 - Support,
- Clause 8 - Operations,
- Clause 9 - Performance evaluation,
- Clause 10 - Improvement
- Annex A – Reference control objectives and controls

1.3.1 ISO/IEC 27002:2013 vs ISO/IEC 27002:2022

On 15 February 2022, ISO/IEC publishes the revised edition of the ISO/IEC 27002:2022. It has been eight (8) years since the last revision of ISO/IEC 27002 (particularly in 2013). Therefore, the new edition includes major changes not only about controls but also how to organize and use them. Below, it is presented the changes in comparison ISO/IEC 27002:2013 [9]:

- ISO 27001 Clauses 4 to 10 remain the same with minor wording updates for clarification purposes,
- The security controls contained in Annex A have been updated (the number of controls decreased from 114 to 93),
- Controls are now grouped into four (4) main domains (instead of the previous 14) and are tagged for easier reference and use. The 4 main domains are:
  i. Organizational controls, including 37 controls.
  ii. People controls, including 8 controls
  iii. Physical controls, including 14 controls.
  iv. Technological controls, including 34 controls

- Eleven (11) new controls have been introduced, whilst none of the controls was deleted, many controls were merged together, thereby reducing the overall number. The 11 controls now include:
  i. Physical security monitoring
  ii. Threat intelligence
  iii. Configuration management
  iv. Information deletion
  v. Data masking
  vi. Data leakage prevention
  vii. Monitoring activities
  viii. Information security for use of cloud services
  ix. Web filtering
  x. Secure coding
  xi. ICT readiness for business continuity
- The controls now also have five types of attribute to make them easier to categorize:
  i. Control type (preventive, detective, corrective)
  ii. Information security properties (confidentiality, integrity, availability)
  iii. Cybersecurity concepts (identify, protect, detect, respond, recover)
  iv. Operational capabilities (governance, asset management, etc.)
  v. Security domains (governance and ecosystem, protection, defence, resilience)

Below, it is presented the new controls of ISO/IEC 27002:2022 in comparison with the ISO/IEC 27002:2013 [10]:

ISO/IEC 27002:2022		ISO/IEC 27002:2013
5	**Organizational controls**	
5.1	Policies for information security	• A.5.1.1 Policies for information security • A.5.1.2 Review of the policies for information security
5.2	Information security roles and responsibilities	• A.6.1.1 Information security roles and responsibilities
5.3	Segregation of duties	• A.6.1.2 Segregation of duties
5.4	Management responsibilities	• A.7.2.1 Management responsibilities
5.5	Contact with authorities	• A.6.1.3 Contact with authorities
5.6	Contact with special interest groups	• A.6.1.4 Contact with special interest groups
5.7	Threat intelligence	-
5.8	Information security in project management	• A.6.1.5 Information security in project management • A.14.1.1 Information security requirements analysis and specification
5.9	Inventory of information and other associated assets	• A.8.1.1 Inventory of assets • A.8.1.2 Ownership of assets
5.10	Acceptable use of information and other associated assets	• A.8.1.3 Acceptable use of assets • A.8.2.3 Handling of assets
5.11	Return of assets	• A.8.1.4 Return of assets

5.12	Classification of information	• A.8.2.1 Classification of information
5.13	Labelling of information	• A.8.2.2 Labelling of information
5.14	Information transfer	• A.13.2.1 Information transfer policies and procedures • A.13.2.2 Agreements on information transfer • A.13.2.3 Electronic messaging
5.15	Access control	• A.9.1.1 Access control policy • A.9.1.2 Access to networks and network services
5.16	Identity management	• A.9.2.1 User registration and de-registration
5.17	Authentication information	• A.9.2.4 Management of secret authentication information of users • A.9.3.1 Use of secret authentication information • A.9.4.3 Password management system
5.18	Access rights	• A.9.2.2 User access provisioning • A.9.2.5 Review of user access rights • A.9.2.6 Removal or adjustment of access rights
5.19	Information security in supplier relationships	• A.15.1.1 Information security policy for supplier relationships
5.20	Addressing information security within supplier agreements	• A.15.1.2 Addressing security within supplier agreements
5.21	Managing information security in the ICT supply chain	• A.15.1.3 Information and communication technology supply chain
5.22	Monitoring, review and change management of supplier services	• A.15.2.1 Monitoring and review of supplier services • A.15.2.2 Managing changes to supplier services
5.23	Information security for use of cloud services	-
5.24	Information security incident management planning and preparation	• A.16.1.1 Responsibilities and procedures
5.25	Assessment and decision on information security events	• A.16.1.4 Assessment of and decision on information security events
5.26	Response to information security incidents	• A.16.1.5 Response to information security incidents
5.27	Learning from information security incidents	• A.16.1.6 Learning from information security incidents
5.28	Collection of evidence	• A.16.1.7 Collection of evidence
5.29	Information security during disruption	• A.17.1.1 Planning information security continuity • A.17.1.2 Implementing information security continuity • A.17.1.3 Verify, review and evaluate information security continuity
5.30	ICT readiness for business continuity	-
5.31	Identification of legal, statutory, regulatory and contractual requirements	• A.18.1.1 Identification of applicable legislation and contractual requirements

		• A.18.1.5 Regulation of cryptographic controls
5.32	Intellectual property rights	• A.18.1.2 Intellectual property rights
5.33	Protection of records	• A.18.1.3 Protection of records
5.34	Privacy and protection of PII	• A.18.1.4 Privacy and protection of personally identifiable information
5.35	Independent review of information security	• A.18.2.1 Independent review of information security
5.36	Compliance with policies and standards for information security	• A.18.2.2 Compliance with security policies and standards • A.18.2.3 Technical compliance review
5.37	Documented operating procedures	• A.12.1.1 Documented operating procedures
6	**People controls**	
6.1	Screening	• A.7.1.1 Screening
6.2	Terms and conditions of employment	• A.7.1.2 Terms and conditions of employment
6.3	Information security awareness, education and training	• A.7.2.2 Information security awareness, education and training
6.4	Disciplinary process	• A.7.2.3 Disciplinary process
6.5	Responsibilities after termination or change of employment	• A.7.3.1 Termination or change of employment responsibilities
6.6	Confidentiality or non-disclosure agreements	• A.13.2.4 Confidentiality or non-disclosure agreements
6.7	Remote working –	• A.6.2.2 Teleworking
6.8	Information security event reporting	• A.16.1.2 Reporting information security events • A.16.1.3 Reporting information security weaknesses
7	**Physical controls**	
7.1	Physical security perimeter	• A.11.1.1 Physical security perimeter
7.2	Physical entry controls	• A.11.1.2 Physical entry controls • & • A.11.1.6 Delivery and loading areas
7.3	Securing offices, rooms and facilities	• A.11.1.3 Securing offices, rooms and facilities
7.4	Physical security monitoring	-
7.5	Protecting against physical and environmental threats	• A.11.1.4 Protecting against external and environmental threats
7.6	Working in secure areas	• A.11.1.5 Working in secure areas
7.7	Clear desk and clear screen	• A.11.2.9 Clear desk and clear screen policy
7.8	Equipment siting and protection	• A.11.2.1 Equipment siting and protection
7.9	Security of assets off-premises	• A.11.2.6 Security of equipment and assets off-premises
7.10	Storage media	• A.8.3.1 Management of removable media • A.8.3.2 Disposal of media • A.8.3.3 Physical media transfer • A.11.2.5 Removal of assets
7.11	Supporting utilities	• A.11.2.2 Supporting utilities
7.12	Cabling security	• A.11.2.3 Cabling security
7.13	Equipment maintenance	• A.11.2.4 Equipment maintenance

7.14	Secure disposal or re-use of equipment	• A.11.2.7 Secure disposal or reuse of equipment
8	**Technological controls**	
8.1	User endpoint devices	• A.6.2.1 Mobile device policy • A.11.2.8 Unattended user equipment
8.2	Privileged access rights	• A.9.2.3 Management of privileged access rights
8.3	Information access restriction	• A.9.4.1 Information access restriction
8.4	Access to source code	• A.9.4.5 Access control to program source code
8.5	Secure authentication	• A.9.4.2 Secure log-on procedures
8.6	Capacity management	• A.12.1.3 Capacity management
8.7	Protection against malware	• A.12.2.1 Controls against malware
8.8	Management of technical vulnerabilities	• A.12.6.1 Management of technical vulnerabilities • A.18.2.3 Technical compliance review
8.9	Configuration management	-
8.10	Information deletion	-
8.11	Data masking	-
8.12	Data leakage prevention	-
8.13	Information backup	• A.12.3.1 Information backup
8.14	Redundancy of information processing facilities	• A.17.2.1 Availability of information processing facilities
8.15	Logging	• A.12.4.1 Event logging • A.12.4.2 Protection of log information • A.12.4.3 Administrator and operator logs
8.16	Monitoring activities	-
8.17	Clock synchronization	• A.12.4.4 Clock synchronization
8.18	Use of privileged utility programs	• A.9.4.4 Use of privileged utility programs
8.19	Installation of software on operational systems	• A.12.5.1 Installation of software on operational systems • A.12.6.2 Restrictions on software installation
8.20	Network controls	• A.13.1.1 Network controls
8.21	Security of network services	• A.13.1.2 Security of network services
8.22	Web filtering	• A.13.1.3 Segregation in networks
8.23	Segregation in networks	-
8.24	Use of cryptography	• A.10.1.1 Policy on the use of cryptographic controls • A.10.1.2 Key management
8.25	Secure development lifecycle	• A.14.2.1 Secure development policy
8.26	Application security requirements	• A.14.1.2 Securing application services on public networks • A.14.1.3 Protecting application services transactions
8.27	Secure system architecture and engineering principles	• A.14.2.5 Secure system engineering principles
8.28	Secure coding	-

8.29	Security testing in development and acceptance	• A.14.2.8 System security testing • A.14.2.9 System acceptance testing
8.30	Outsourced development	• A.14.2.7 Outsourced development
8.31	Separation of development, test and production environments	• A.12.1.4 Separation of development, testing and operational environments • A.14.2.6 Secure development environment
8.32	Change management	• A.12.1.2 Change management • A.14.2.2 System change control procedures • A.14.2.3 Technical review of applications after operating platform changes • A.14.2.4 Restrictions on changes to software packages
8.33	Test information	• A.14.3.1 Protection of test data
8.34	Protection of information systems during audit and testing	• A.12.7.1 Information systems audit controls

Table 2: ISO/IEC 27002:2022 controls in comparison with ISO/IEC 27002:2013

Chapter 2: From NIS 1 Directive to NIS 2 Directive

2.1 NIS 1 Directive

Directive 2016/11481 on security of network and information systems (the NIS Directive) is the first horizontal legislation undertaken at EU level for the protection of network and information systems across the Union. The goal was to enhance cybersecurity across the EU [1].

The NIS Directive was published in July 2016, however the EU has been addressing cyber security issues in a comprehensive manner since 2004, when ENISA a new specialized EU agency, was founded. The NIS Directive itself has its roots in the Commission's Communication of 2009, which focuses on prevention and awareness and defines a plan of immediate action to strengthen security and trust in the information society. This was followed, in 2013, by a joint Communication released by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy on the Cybersecurity Strategy of the EU. From 2013 to 2015 the Commission, the Council and the Parliament discussed the draft put forward by the Commission intensely and these discussions resulted in the NIS Directive that entered into force in August 2016 [1].

The NIS Directive was adopted in 2016 and subsequently, because it is an EU directive, every EU member state has started to adopt national legislation, which follows or 'transposes' the directive. EU directives give EU countries some level of flexibility to take into account national circumstances, for example to re-use existing organizational structures or to align with existing national legislation. The national transposition by the EU member states happened on 9 May 2018 [11].

The NIS Directive is divided into three (3) parts [11]:

1. **National capabilities:** EU Member States must have certain national cybersecurity capabilities of the individual EU countries, e.g., they must have a national CSIRT, perform cyber exercises, etc.
2. **Cross-border collaboration:** Cross-border collaboration between EU countries, e.g., the operational EU CSIRT network, the strategic NIS cooperation group, etc.
3. **National supervision of critical sectors:** EU Member states have to supervise the cybersecurity of critical market operators in their country: Ex-ante supervision in critical sectors (energy, transport, water, health, digital infrastructure and finance sector), ex-post supervision for critical digital service providers (online market places, cloud and online search engines)

The NIS Directive consists of 27 Articles. Articles 1–6 set its scope and main definitions, including a further clarification regarding the identification of Operators of Essential Services (Article 5), as well as the meaning of significant disruptive effect (Article 6). Articles 7–10 describe the national frameworks that need to be adopted by each Member State on the security of network and information systems. These frameworks include, among others, Member States' obligation to introduce a national strategy and to designate national competent authorities (including a single point of contract and the Computer Security Incident Response Teams (CSIRTs), as well as the creation of the Cooperation Group. The cooperation mechanism is provided in Chapter III and more specifically in Articles 11–13. The Articles that follow (14–18) define the security requirements and incident notification for operators of essential services and digital service providers, respectively. The adoption of standards and the process of voluntary notification are dealt with in Articles 19 and 20. Finally Articles 21–27 include the Directive's final provisions [1].

Furthermore, the NIS Directive affects two categories of undertakings, under an admittedly differentiated approach in terms of obligations placed upon each one of them [1] [12]:

1. Operators of Essential Services (OESs) means a public or private entity that activates in specific sectors such as the sector of energy, transport, banking and health, and which at the same time meets some essential criteria that qualify it as an entity of such type.
2. Digital Service Providers (DSPs) includes any legal person that provides a digital service and more specifically an online market place, an online search engine or a cloud computing service. More precisely, these three (3) types of digital service providers are:
    i. An online marketplace denotes a digital service that allows consumers and/or traders to conclude online services or service contracts with traders.
    ii. An online search engine is described as a digital service that allows users to perform searches of websites on the basis of a query on any subject.
    iii. Finally, cloud computing service means, a digital service that enables access to a scalable and elastic pool of shareable computing resources.

Each Member state must adopt a national framework in order to succeed compliance with the provisions of the NIS Directive. The national framework includes the national strategy on the security of network and information systems and the designation of the authorities that shall be responsible for monitoring the implementation of the NIS Directive. As far as the first parameter is concerned, Article 7 of the Directive sets the obligation of each Member State to adopt a national strategy on the security of network and information systems in order to achieve a high level of security of such networks. This national strategy must address a list of issues, as described in Article 7(1), including, among others, a risk assessment plan, a governance framework to achieve the objectives of the national strategy, the identification of measures relating to preparedness, response and recovery etc. Member States may turn to ENISA for advice and assistance when developing their national strategies. As per Article 7(3) Member States ought to communicate their national strategies to the Commission within three months from their adoption [1] [12].

In addition, Articles 8, 9, 11 and 12 of the NIS Directive specify the authorities and other bodies that shall be tasked with the role of monitoring its application at national and EU level. Each Member State ought to designate one or more national competent authorities on the security of network and information systems. These shall monitor the application of the NIS Directive at national level. Each Member State shall also designate a national Single Point of Contact to liaise and ensure cross-border cooperation with other Member States. Designated competent authorities and a single point of contact, as well as their tasks, should be notified to the Commission (Article 8). Member State are also asked to introduce one or more computer security incident response teams CSIRTs (Article 9). The CSIRTs role, as per Annex I of the Directive, is to monitor incidents at national level, provide early warning, alerts and information to relevant stakeholders about risks and incidents, respond to incidents, provide dynamic risk and incident analysis and increase situational awareness, as well as, to participate in a network of the CSIRTs across Europe. Another body which was established under the NIS Directive (Article 11) is the chairman of the CG is the Presidency of the Council of the European Union, including representatives from Member States, the Commission (acting as secretariat) and ENISA. Given the Cooperation Group ("CG"). importance of international cooperation on cybersecurity, the Group's role is to facilitate strategic cooperation and exchange of information among Member States and help develop trust and confidence. The Group's tasks are described in Article 11(3). Its functioning is further clarified by the Implementing Decision issued by the Commission, by virtue of Article 11(5) of the Directive. Finally, Article 12 establishes the creation of a network of the national CSIRT's. The CSIRTs network shall be composed of representatives of the Member States' CSIRTs and CERT-EU (the Computer Emergency Response Team for the EU institutions, agencies and bodies). Among the tasks that fall within the CSIRTs network's competencies is the exchange of information on CSIRTs' services, operations and cooperation capabilities, the exchange of information related to incidents and associated risks, identification of a coordinated response to an incident, and provision of support to Member States in addressing cross–border incidents. The Commission participates in the CSIRTs Network as an observer and ENISA provides secretariat services, actively supporting the cooperation among the CSIRTs. Two years after entry into force of the NIS Directive (by 9 August 2018), and every 18 months thereafter, the CSIRTs Network will produce a report assessing the benefits of operational cooperation, including conclusions and recommendations. The report will be sent to the Commission as a contribution to the review of the functioning of the Directive. It is essential to mention that the first recorded cyber security incident at EU level dates back to May 2017 and refers to the WannaCry Ransomware attack. The term ransomware has been around for decades but the WannaCry attack was the first global ransomware heist that impacted entire state hospital systems, international businesses and countries as a whole. Estimates of that time suggested that approximately 190,000 computers in over 150 countries were affected. This was a year in which the operational cooperation of the CSIRTs network was tested and proved its readiness and ability to cooperate during large scale security incidents. Despite its negative impact worldwide, this incident demonstrated the severity of large-scale cross border cyberattacks and triggered the need for international cooperation [1] [12].

As mentioned above, ENISA has a vital role under the NIS Directive, as it should assist Member States and the Commission by providing expertise whereas both Member States and the Commission should be able to consult ENISA. Also, ENISA is responsible for assisting the Cooperation Group and be involved in the development of guidelines. Last but not least, the Commission should consult ENISA when adopting implementing acts. Furthermore, ENISA launches a tool which maps security measures for Operators of Essential Services (OES) to international standards. This tool is available through an online platform (you can click here) dedicated to operators in the sectors of [1] [12] [13]:

1. Energy, with the following sub-sectors [12]:
   i. Electricity,
   ii. Oil, and
   iii. Gas.
2. Transport, with the following sub-sectors:
   i. Air transport,
   ii. Rail transport,
   iii. Water transport, and
   iv. Road transport.
3. Banking,
4. Financial market infrastructures,
5. Health, with the following sub-sector:

i. Health care settings (including hospitals and private clinics).

6. Drinking water supply & distribution,
7. Digital infrastructures.

This tool provides the mapping of security measures for OESs to international standards used by operators in the business sectors (namely energy, transport, banking, financial market infrastructures, health, drinking water supply & distribution and digital infrastructures). It also helps to assess their use in the Member States and in various NIS Directive sectors [13] [14]:

- Operators can use this tool to map their own standards to the proposed security measures, enabling the assessment of their information security practices against the requirements adopted by the Cooperation Group.
- The Member States can use this tool to identify issues and look for solutions when assessing the security measures of their national OES and possibly identify a mapping to corresponding national security measures of other Member States.

Below, it is presented a table with the relevant minimum security measures for Operators of Essentials Services and their corresponding domain and sub-domain [13].

NIS Directive				
ID	**Security Measure**	**Domain**	**Sub-domain**	**Description**
1	Incident Report	Defense	Computer Security Incident Management	The operator creates and keeps up-to-date and implements procedures for incidents' reporting.
2	Communication with competent authorities and CSIRTs	Defence	Computer Security Incident Management	The operator implements a service that enables it to take note, without undue delay, of information sent out by its national competent authority concerning incidents, vulnerabilities, threats and relevant mappings (up-to-date inventory of CIS, interconnections of CIS with third-party networks, etc.). It implements a procedure for handling the information received, and, where appropriate, for taking the security measures required to protect its CIS. The operator provides its national competent authority with up to date contact details (department name, telephone number, and e-mail address) for this service. The operator is encouraged to connect its incident management with relevant Computer Security Incident Response Teams (CSIRTs).
3	Logging	Defence	Detection	The operator sets up a logging system on each CIS in order to record events relating, at least, to user authentication, management of accounts and access rights, modifications to security rules, and the functioning of the CIS and which covers application servers that support critical activities; system infrastructure servers;

				network infrastructure servers; security equipments; engineering and maintenance stations of industrial systems; network equipments; administrative workstations. The operator records through the logging system events with time and date-stamping using synchronized time sources and centralizes archives for at least half-a-year.
4	Logs Correlation And Analysis	Defence	Detection	The operator creates a log correlation and analysis system that mines the events recorded by the logging system installed on each of the CIS in order to detect events that affects CIS security. The log correlation and analysis system is installed and operated by the operator (or the service provider appointed to that effect) via a dedicated information system used only to detect events that are likely to affect the security of information systems.
5	Detection	Defence	Detection	The operator sets up a security incident detection system of the “analysis probe for files and protocols” type. The analysis probes for files and protocols analyses the data flows transiting through those probes in order to seek out events likely to affect the security of CIS. They are positioned so that they can analyse all flows exchanged between the CIS and third-party information systems.
6	Information System Security Incident Response	Defence	Computer Security Incident Management	The operator creates and keeps up-to-date and implements a procedure for handling, response to and analyses of incidents that affect the functioning or the security of its CIS, in accordance with its ISSP. The operator puts in place a dedicated information system to handle incidents, in order inter alia to store the technical records of incident analysis. The operator segregates the system from the CIS affected by the incident and stores the related technical records for a period of at least half-a-year. The operator takes into account, when designing the system, the confidentiality level of stored documents.
7	Human Resource Security	Governance and Ecosystem	Information System Security Governance & Risk Management	The operator ensures that, first, employees and contractors understand and demonstrate their responsibilities and are suitable for the roles for which they are considered and, second, commit to their roles. The established information system security policies sets up a CIS security awareness raising program for all staff and a security training program for employees with CIS related responsibilities.

8	Information System Security Indicators	Governance and Ecosystem	Information System Security Governance & Risk Management	For each CIS and according to a number of indicators and assessment methods, the operator evaluates its compliance with its ISSP. Indicators may relate to the risk management organization's performance, the maintaining of resources in secure conditions, users' access rights, authenticating access to resources, and resource administration.
9	Information System Security Risk Analysis	Governance and Ecosystem	Information System Security Governance & Risk Management	The operator conducts and regularly updates a risk analysis, identifying its Critical Information Systems (CIS) underpinning the provision of the essential services of OES and identifies the main risks to these CIS. This process is essential to build and maintain a robust risk management organization. The results of the updates should be implemented through a virtuous circle of continuous improvement.
10	Information System Security Audit	Governance and Ecosystem	Information System Security Governance & Risk Management	The operator establishes and updates a policy and procedures for performing information system security assessments and audits of critical assets and CIS, taking into account the regularly updated risks analysis.
11	Ecosystem Mapping	Governance and Ecosystem	Ecosystem Management	The operator establishes a mapping of its ecosystem, including internal and external stakeholders, including but not limited to suppliers, in particular those with access to or managing operator's critical assets.
12	Information System Security Accreditation	Governance and Ecosystem	Information System Security Governance & Risk Management	Building on the risk analysis and according to an accreditation process referred to in the ISSP, the operator accredits the CIS identified in its information system risk analysis, including inter alia the inventory and architecture of the administration components of the CIS. The purposes of the accreditation process for the operator are to integrate the CIS within the risk management organization and to formally accept the residual risks. As part of the accreditation process and depending on the risks analysis, a security audit of the CIS should be carried out. That audit should aim at checking the application and effectiveness of the security measures that apply to the CIS. The CIS accreditation decision should take into account the risk analysis, the security measures applied to the CIS, audit reports and the residual risks, and the reasons to justify their acceptance. The operator maintains an up-to-date map of its CIS.
13	Information System Security Policy	Governance and Ecosystem	Information system security policy	Building upon the risks analysis, the operator establishes, maintains up-to-date and implements an information system security policy (ISSP) and an information security

				management system (ISMS) approved by senior management, guaranteeing high level endorsement of the policy. The policy sets out strategic security objectives, describes the security governance (or risk management organization), and refers to all relevant specific information system security policies (e.g., on the security accreditation process, security audit, cryptography, security maintenance, incident handling, etc.).
14	Ecosystem Relations	Governance and Ecosystem	Ecosystem Management	The operator establishes a policy towards its relations with its ecosystem in order to mitigate the potential risks identified. This includes in particular interfaces between the CIS and third parties. Generally, security requirements must been taken into account for CIS-components operated by third parties. The operator ensures via service level agreements (SLA) and/or auditing mechanisms that his suppliers also establish adequate security measures.
15	Authentication and Identification	Protection	Identity and access management	For identification, the operator sets up unique accounts for users or for automated processes that need to access resources of its CIS. Unused or no longer needed accounts are to be deactivated. A regular review process should be established. For authentication, the operator protects access to resources of its CIS for users or automated processes using authentication mechanism. The operator defines the rules for the management of authentication credentials of its CIS.
16	IT security Maintenance Procedure	Protection	IT Security Maintenance	The operator develops and implements a procedure for security maintenance in accordance with its ISSP. To this purpose, the procedure defines the conditions enabling the minimum security level to be maintained for CIS resources.
17	System Segregation	Protection	IT Security Architecture	The operator segregates its systems in order to limit the propagation of IT security incidents within its systems or subsystems. To this aim, the operator segregates physically or logically each CIS from the operator's other information systems or from third party information system. In the case a CIS itself is composed of subsystems, the operator segregates these last physically or logically. The operator allows only interconnections - between CIS and other systems or between CIS subsystems - that are essential for the functioning and security of a CIS. The operator implements adequate security

				measures for unavoidable interfaces (e.g., interfaces to the IT of suppliers or customers).
18	Cryptography	Protection	IT Security Architecture	In its ISSP, the operator establishes and implements a policy and procedures related to cryptography, in view of ensuring adequate and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information in its CIS.
19	Industrial Control Systems	Protection	IT Security Maintenance	Many essential services depend on functioning and secure industrial control systems (ICS). If applicable, the operator takes the particular security requirements for ICS into account. For example, the classical information technology approach (which is focused on transfer of and access to information) could be replaced by an operational technology approach (hardware and software is used to cause or detect changes in a physical process).
20	Administration Accounts	Protection	IT Security Administration	The operator sets up specific accounts for the administration, to be used only for administrators that are carrying out administration operations (installation, configuration, management, maintenance, etc.) on its CIS. These accounts are kept on an up-to-date list, which can be done for non-administration accounts as well. To this aim, the permissions given to administrators are individualized and restricted as much as possible to the functional and technical perimeter of each administrator. The administrator accounts are only used to connect to administration information system. While these accounts are used for administration purposes only, administration operations are realized exclusively with the use of administrator accounts.
21	Physical and Environmental Security	Protection	Physical and environmental security	The operator prevents unauthorized physical access, damage and interference to the organization's information and information processing facilities.
22	Access Rights	Protection	Identity and access management	Among the rules defined in its systems security policy, the operator grants access rights to a user or an automated process only when that access is strictly necessary for the user to carry out their mission or for the automated process to carry out its technical operations.
23	Traffic Filtering	Protection	IT Security Architecture	The operator filters traffic flows circulating in its Critical Information Systems (CIS). The operator therefore forbids traffic flows that are not needed for the functioning of its systems and

				that are likely to facilitate an attack. The operator defines and regularly updates the filtering rules (by network address, by port number, by protocol, etc.) in order to restrain traffic flows to flows needed for the functioning and the security of the CIS. The operator filters flows entering and existing CIS and flows between CIS subsystems at the level of their interconnection, therefore limiting the flows strictly necessary for the functioning and security of CIS.
24	Administration Information Systems	Protection	IT Security Administration	Hardware and software resources used for administration purposes are managed and configured by the operator, or, where appropriate, by the service provider that the operator has authorized to carry out administration operations. Administration information systems used for administration purposes only and to carry out administration operations and should not be mixed up with other operations. In particular administration accounts’ software environment is not used for access to web sites or messaging systems on the internet, and users do not connect to a system used for administration purposes through a software environment used for other functions than administration operations.
25	Systems Configuration	Protection	IT Security Architecture	The operator only installs services and functionalities or connects equipment which are essential for the functioning and the security of its CIS. If additional components are unavoidable (e.g., for economic reasons), they are analyzed according to the risk analysis. Those components should only be used to the necessary extent and with adequate security measures.
26	Disaster Recovery Management	Resilience	Continuity of Operations	In accordance with its ISSP, the operator defines objectives and strategic guidelines regarding disaster recovery management, in case of a severe IT security incident.
27	Crisis Management Organization	Resilience	Crisis management	The operator defines in its ISSP the organization for crisis management in case of IT security incidents and the continuity of organization’s activities.
28	Business Continuity Management	Resilience	Continuity of operations	In accordance with its ISSP, the operator defines objectives and strategic guidelines regarding business continuity management, in case of IT security incident.
29	Crisis Management Process	Resilience	Crisis management	The operator defines in its ISSP the processes for crisis management which the crisis management

				organization will implement in case of IT security incidents and the continuity of an organization's activities.

Table 3: Mapping of Security Measures for OES tool

2.1 NIS 2 Directive

According to NIS Directive and particularly Article 23, the European Commission should periodically review the functioning of this Directive and report to the European Parliament and to the Council. Therefore, the Commission announced in its 2020 work programme that it would be conducted this review by the end of 2020 [15].

On 25 June 2020, the Commission published a combined evaluation roadmap/ inception impact assessment (you can see here) on the revision of the NIS Directive, according to which it planned to 'evaluate the functioning of the NIS Directive based on the level of security of network and information systems in the Member States'. The Commission underlined that in addition to the requirement under Article 23 of the NIS Directive, the revision was 'further justified by the sudden increase in the dependence on information technology during the Covid-19 crisis'. The Commission stated that 'depending on the results from the evaluation of the functioning of the NIS Directive, an open public consultation and an impact assessment, the Commission might propose measures aimed at enhancing the level of cybersecurity within the Union'. The Commission evaluation analysed the NIS directive for its relevance, EU added value, coherence, effectiveness and efficiency. Its main findings were that the scope of the NIS Directive is too limited in terms of the sectors covered, mainly due to [2]:

i. increased digitalization in recent years and a higher degree of interconnectedness, and
ii. the scope of the NIS Directive no longer reflects all digitalized sectors providing key services to the economy and society as a whole.

Furthermore, the evaluation concluded that the NIS Directive does not provide sufficient clarity as regards the scope criteria for OESs or the national competence over digital service providers. This has led to a situation in which certain types of entities have not been identified in some Member States and are therefore not required to put in place security measures and report incidents. For example, certain major hospitals in a Member State do not fall within the scope of the NIS Directive and hence are not required to implement the resulting security measures, while in another Member State almost every single healthcare provider is covered by the NIS security requirements. The NIS Directive afforded Member States broad discretion when laying down security and incident reporting requirements for OESs. The evaluation shows that in some instances Member States have implemented these requirements in significantly different ways, creating an additional burden for companies operating in more than one Member State. The supervision and enforcement regime of the NIS Directive is ineffective. The financial and human resources set aside by Member States for fulfilling their tasks (such as OES identification or supervision), and consequently the different levels of proficiency in dealing with cybersecurity risks, vary greatly. This further exacerbates the differences in cyber-resilience among Member States. Member States do not share information systematically with one another, with negative consequences in particular for the effectiveness of the cybersecurity measures and the level of joint situational awareness at EU level. This is also the case for information-sharing among private entities and for the engagement between the EU level cooperation structures and private entities [2].

The Commission presented on 16 December 2020 a proposal for a directive on measures for a high common level of cybersecurity across the Union (NIS 2), which would repeal and replace the existing NIS Directive (NIS 1). The proposed directive aims to tackle the limitations of the current NIS 1 regime.

The legal basis for both NIS 1 and the proposed NIS 2 is Article 114 of the Treaty on the Functioning of the European Union, whose objective is the establishment and functioning of the internal market by enhancing measures for the approximation of national rules. The proposed expansion of the scope covered by NIS 2, which would effectively oblige more entities and sectors to take measures, would assist in increasing the level of cybersecurity in Europe in the longer term. Overall, the NIS 2 proposal sets itself three general objectives [2]:

- Increase the level of cyber-resilience of a comprehensive set of businesses operating in the European Union across all relevant sectors, by putting in place rules that ensure that all public and private entities across the internal market, which fulfil important functions for the economy and society as a whole, are required to take adequate cybersecurity measures. For instance, the proposal extends significantly the scope of the current directive by changing the “Operators of essential services” and “Digital service providers” categories into two new (2) categories, named “Essential entities” and “Important entities” corresponding, as presented in the table below with the corresponding sectors and subsectors [2] [16]:

NIS 2 Directive’s Sectors & Sub-sectors			
“Essential entities” Category		“Important entities” Category	
1. Energy	a. Electricity	1. Postal and courier services	-
	b. District heating and cooling	2. Waste management	-
	c. Oil	3. Manufacture, production and distribution of chemicals	-
	d. Gas	4. Food production, processing and distribution	-
	e. Hydrogen	5. Manufacturing	a. Manufacture of medical devices and in vitro diagnostic medical devices
2. Transport	a. Air		b. Manufacture of computer, electronic and optical products
	b. Rail		c. Manufacture of electrical equipment

	c. Water		d. Manufacture of machinery and equipment n.e.c.
	d. Road		e. Manufacture of motor vehicles, trailers and semi-trailers
3. Banking	-		f. Manufacture of other transport equipment
4. Financial market infrastructures	-	6. Digital providers	-
5. Health	-	-	-
6. Drinking water	-	-	-
7. Waste water	-	-	-
8. Digital Infrastructure	-	-	-
9. Public administration	-	-	-
10. Space	-	-	-

Table 4: NIS 2 Directive's sectors and sub-sectors

It establishes that all medium-sized and large entities active in the sectors covered by the NIS 2 framework would hence have to comply with the security rules put forward in the proposal and removes the possibility for Member States to tailor the requirements in certain cases (which had led to much fragmentation with NIS 1 implementation, see impact assessment). It removes the distinction made between OESs and digital DSPs, which currently fall into three categories: online marketplaces, search engines and cloud service providers. Finally, it addresses, for the first time, cybersecurity of the ICT supply chain (of special importance in the case of the IoT) [2].

- Reduce inconsistencies in resilience across the internal market in the sectors already covered by the directive, by further aligning [2]:

  i. the de facto scope,
  ii. the security and incident reporting requirements,
  iii. the provisions governing national supervision and enforcement, and
  iv. the capabilities of the Member States' relevant competent authorities.

The proposal includes a list of seven key elements that all companies must address or implement as part of the measures they take, including incident response, supply chain security, encryption and vulnerability disclosure. In addition, the proposal envisages a two-stage approach to incident reporting. Affected companies have 24 hours from when they first become aware of an incident to submit an initial report, followed by a final report no later than one month later. Regarding enforcement, it establishes a minimum list of administrative sanctions whenever entities breach the rules regarding cybersecurity risk management or their reporting obligations laid down in the NIS Directive. These sanctions include binding instructions, an order to implement the recommendations of a security audit, an order to bring security measures into line with NIS requirements, and administrative fines (up to €10 million or 2 % of the entities' total turnover worldwide, whichever is higher) [2].

- Improve the level of joint situational awareness and the collective capability to prepare and respond,

    i. by taking measures to increase the level of trust between competent authorities,
    ii. by sharing more information, and
    iii. setting rules and procedures in the event of a large-scale incident or crisis.

The proposed new rules improve the way the EU prevents, handles and responds to large-scale cybersecurity incidents and crises by introducing clear responsibilities, appropriate planning and more EU cooperation. The revised directive would establish an EU crisis management framework, requiring Member States to adopt a plan and designate national competent authorities responsible for participating in the response to cybersecurity incidents and crises at the EU level. The proposed directive would establish an EUCyber Crises Liaison Organization Network (EU-CyCLONe) to support the coordinated management of EU-wide cybersecurity incidents, as well as to ensure the regular exchange of information. The proposed directive would also strengthen the role of the NIS Cooperation Group in making decisions and increasing cooperation between Member States. Member States would still be required to adopt a national cybersecurity strategy and to designate one or more national competent authorities to supervise compliance with the directive; and to designate CSIRTs to handle incident notifications and single points of contact (SPOC) to act as a liaison point with other Member States [2].

In order to ensure consistency and coherence with related EU legislation, the NIS Directive review in particular takes into account the following three Commission initiatives [2]:

- the review of the Resilience of Critical Entities (CER) Directive (you can see here), which was proposed alongside the NIS 2 proposal, with the objective of improving the resilience of critical entities against physical threats in a large number of sectors. The proposal expands both the scope and depth of the current 2008 directive, including the coverage of ten (10) sectors: energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, public administration and space,
- the initiative on a digital operational resilience act for the financial sector (DORA-you can see here),
- the initiative on a network code on cybersecurity with sector-specific rules for cross border electricity flows (you can see here)

As regards the financial sector, the DORA proposal would provide legal clarity on whether and how digital operational provisions apply, especially to cross-border financial entities, and it would eliminate the need for Member States to individually improve rules, standards and expectations regarding operational resilience and cybersecurity as a response to the current limited coverage of EU rules and the general nature of the NIS 1 Directive. At the same time, it is important to maintain a strong relationship for the exchange of information between the financial sector and the other sectors covered by NIS 2. To that end, under the DORA proposal, all financial supervisors, the European supervisory authorities (ESAs) for the financial sector and the financial sector-related national competent authorities would be able to participate in the discussions of the NIS Cooperation Group, and to exchange information and cooperate with the single points of contact and with the national CSIRTs under NIS 2. Moreover, Member States should continue to include the financial sector in their cybersecurity strategies, and national CSIRTs may cover the financial sector in their activities [2].

Furthermore, the Commission has aligned the scope in the NIS2 proposal with the proposal for a review of the CER Directive. As regards ENISA, it would see increased responsibilities within its existing mandate, which involves overseeing the implementation of the NIS. ENISA would be tasked to prepare a report every two years on the state of cybersecurity in the EU and to maintain a European vulnerability registry providing access to information on the vulnerabilities of ICT products and services disclosed on a voluntary basis by essential and important entities and their ICT suppliers. At the same time, ENISA would be required to create and maintain a registry, in which certain types of entities including domain name system service providers, top level domain name registries, cloud computing service providers, data centre service providers, content delivery network providers, as well as online marketplaces, online search engines and social networking platforms would notify where they are established in the EU. This is to ensure that such entities do not face a multitude of different legal requirements, given that they provide services across borders to a particularly high extent [2].

To address key supply chain risks and to assist entities in managing cybersecurity risks related to the ICT supply chain, the NIS Cooperation Group, together with the Commission and ENISA, would be tasked to carry out a coordinated risk assessment per sector of critical ICT services, systems, or products including relevant threats and vulnerabilities. The supply chain risk assessments would consider both technical factors (hardware- or software-related) and, where relevant, non-technical factors (such as suppliers being subject to interference by a non-EU country or state-backed players). This approach largely builds on the previous work of the Commission and the NIS Cooperation Group on the security of 5G networks. The Commission published on 29 January 2020 the 5G risk management toolbox (you can see here), which listed measures to mitigate the security threats associated with 5G networks. Among others, the EU 5G risk assessment identified security risks related to 5G networks and the 5G supply chain at the EU level. To ensure that entities comply with their obligations addressing ICT supply chain security, the new directive would enable Member States to require essential and important entities to certify specific ICT products, services and processes under the EU Cybersecurity Act. In this context, the draft directive would empower the Commission to lay down which categories of essential entities (due to their criticality) would be required to obtain certification [2].

Chapter 3: General Data Protection Regulation (GDPR)

The General Data Protection Regulation (ECU) 2016/679 was adopted on 27 April 2016 after year of dialog and preparations on the ECU Parliament and Council with a view to the processing of private data and the free circulation of such data. The regulation exists as a framework for laws across the continent and replaced the previous 1995 data protection Directive 95/46/EC. The General Data Protection Regulation (GDPR) became applicable on 25 May 2018, after the expiry of the two-year transitional period with the purpose to protect the individual's processing of personal data. Thus, the GDPR was directed at the reform and harmonization of EU data protection laws. The technological occurrence and the disruptive world demanded major changes in data privacy. For the business, GDPR inevitably means new responsibilities, structural changes and cost of compliance on the one hand, but most significantly, security; the elimination of barriers, and hence the responsibility of data transfers. The EU institutions recognize development through the implementation of the law, incorporate certain facets of the business system and lay the foundation for recent legislation which is compatible with the technologically advanced world [1] [3]

But what is GDPR exactly? GDPR can be considered as the world's strongest set of data protection rules, which enhance how people can access information about them and places limits on what organisations can do with personal data. GDPR applies to any organization operating within the EU, as well as any organisations outside of the EU which offer goods or services to customers or businesses in the EU. Furthermore, as mentioned before, GDPR is for personal data. Broadly, this is information that allows a living person to be directly, or indirectly, identified from data that's available. This can be something obvious, such as a person's name, location data, or a clear online username, or it can be something that may be less instantly apparent: IP addresses and cookie identifiers can be considered as personal data [17].

Under GDPR there's also a few special categories of sensitive personal data that are given greater protections. This personal data includes information about racial or ethnic origin, political opinions, religious beliefs, membership of trade unions, genetic and biometric data, health information and data around a person's sex life or orientation. The crucial thing about what constitutes personal data is that it allows a person to be identified – pseudonymized data can still fall under the definition of personal data. Personal data is so important under GDPR because individuals, organisations, and companies that are either 'controllers' or 'processors' of it are covered by the law. A controller is a "person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing of personal data", while the processor is a "person, public authority, agency or other body which processes personal data on behalf of the controller" [17] [18].

Moreover, under GDPR, the organization should make a notification to the relevant supervisory body about a breach within 72 hours of the organization first becoming aware of it. Meanwhile, if the breach is serious enough to mean customers or the public must be notified, GDPR legislation says customers must be made responsible without 'undue delay.' [17]

Another crucial aspect of GDPR is consist the fines and the penalties, as the failure to comply with GDPR can result in a fine ranging from 10 million euros to four per cent of the company's annual global turnover, a figure which for some could mean billions. Fines depend on the severity of the breach and on whether the company is deemed to have taken compliance and regulations around security in a serious enough manner. The maximum fine of 20 million euros or four percent of worldwide turnover - whichever is greater - is for infringements of the rights of the data subjects, unauthorized international transfer of personal data, and failure to put procedures in place for or ignoring subject access requests for their data. A lower fine of 10 million euros or two percent of worldwide turnover will be applied to companies that mishandle data in other ways. They include, but aren't limited to, failure to report a data breach, failure to build in privacy by design and ensure data protection is applied in the first stage of a project and be compliant by appointing a data protection officer - should the organization be one of those required to by GDPR [17]. Below, it presents some of the biggest GDPR fines for the last three years [19]:

1. Amazon - €746 million,
2. WhatsApp — €225 million,
3. Google Ireland — €90 million,
4. Facebook — €60 million,
5. Google LLC — €60 million
6. H&M — €35 million

Last but not least, it is presented below a table with the appropriate GDPR Articles under twelve (12) domains:

General Data Protection Regulation (GDPR)	
1. Maintain Governance Structure	
Article 27	Assign responsibility for the operational aspects of a privacy programme to a representative individual (i.e., Privacy officer) (Applicable for controllers or processors not established in EU)
Article 37	Designate a Data Protection Officer
Article 38	The Data Protection Officer's independence and funding must be ensured, as well as his/her direct reporting to the highest management level.
Article 38	The Data Protection Officer shall be an employee or Third Party expert in data protection law
Article 39	Privacy roles in an organization must be defined through job descriptions, by contract or other methods (i.e., DPO tasks: advise the Controller or Processor and its employees of data protection obligations, monitor compliance, assign responsibilities, training and audits, advising on & monitoring DPIAs, cooperating and contacting the supervisory authority as required and reviewing processing risk)
Article 38	Ensure regular communication between the privacy responsible and the supervisory authority as well as with the stakeholders of the Organization in order for the privacy responsible to be involved in all issues relating to the processing of personal data
Article 24 Article 39	The Controller is responsible to conduct an Enterprise Privacy Risk Assessment taking under consideration the nature, scope, context, and purposes of the processing as well as the risks of varying likelihood and severity for the rights and freedoms of individuals
2. Maintain Personal Data Inventory and Data Transfer Mechanisms	
Article 30	Appropriately maintain a Record of Processing Activities document.
Article 30	The Record of Processing Activities includes:

	the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer
	the purposes of the processing
	a description of the categories of data subjects and of the categories of personal data
	the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations
	where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, where applicable the documentation of suitable safeguards
	where possible, the envisaged time limits for erasure of the different categories of data
	where possible, a general description of the technical and organizational security measures implemented to ensure confidentiality, integrity and availability of Personal Data
Article 45, Article 46, Article 49	Records of the transfer mechanism used for cross-border data flows (e.g., standard contractual clauses, binding corporate rules, approvals from regulators) must be maintained
	Which of the following mechanisms are used when a third country (recipient of data) has not been assessed as providing an adequate level of data protection by the European Commission:
Article 46	a) Binding Corporate Rules
Article 46	b) Contracts
Article 46	c) Regulator's Approval
Article 45, Article 48, Article 49	d) Derogations from adequacy (i.e., data subject consent, performance of a contract, serve public interest)
Article 46	e) EU-US Privacy Shield
3. Maintain Data Privacy Policy	
Article 5, Article 24, Article 91	An organizational–level privacy policy must be developed and enforced in order to provide guidance to employees regarding the processing and protection of personal data to ensure that such processing aligns with the obligations of the GDPR
Article 6, Article 9, Article 10	The legal basis on which processing of personal data takes place must be determined and documented (i.e., legitimate purpose, lawfulness of processing etc.)
4. Embed Data Privacy Into Operations	
Article 9	Policies / Procedures must be established and enforced in order to ensure that special categories of personal data are processed only based on solid legal ground
Article 8, Article 12	Policies / Procedures must be established and enforced in order to ensure that consent is given or authorized by the holder of parental responsibility over the child when personal data of minors are being processed
Article 5	Specific technical and organizational measures must be implemented in order to ensure data quality (accuracy and up-to-date)
Article 89	Specific technical and organizational measures must be implemented in order to ensure respect for the principle of data minimization
Article 12, Article 22	Specific technical and organizational measures must be implemented in order to safeguard the data subject's rights and freedoms and legitimate interests

Article 6, Article 13, Article 14	Specific instructions must be defined in order to handle situations when the Organization wishes to use personal data beyond the primary purpose
Article 6, Article 7, Article 8	Specific technical and organizational measures must be implemented in order to ensure that consent is valid (i.e., freely given, specific and unambiguous)
Article 5	Specific technical and organizational measures must be implemented in order to ensure that Personal Data are not kept in a form that permits identification of data subjects for longer than is necessary for the purposes of collection (i.e., retention periods, anonymization, secure deletion)
Article 21	Appropriate mechanisms must be implemented in order to ensure that the Data Subject can object to the processing of his/her personal data
Article 21, Article 89	Specific technical and organizational measures must be implemented for research practices including processes to obtain personal data for research purposes, ensuring valid consents are obtained, de–identifying data where possible, and taking measures to ensure that research data maintained for scientific, historical or statistical research is safeguarded against improper use
5. Maintain Training and Awareness Program	
Article 39	Awareness–raising and training must be provided, on a regular basis, to staff involved in Personal Data processing operations and appropriate artefacts must be maintained
Article 39	The effectiveness of the training program should be evaluated
6. Manage Information Security Risk	
Article.32	Response will be derived by the outcome of the Security Compliance Assessment
7. Manage Third Party Risk	
Article 28, Article 29, Article 32	A processing contract must be signed with each processor, setting out aspects such as: duration, scope, purpose, documented processing instructions, prior authorization where a processor is engaged, provision of any documentation providing evidence of compliance with the GDPR, prompt notification of any data breach, etc
Article 28	The Organization must conduct due diligence around the data privacy and security posture of potential vendors/processors
Article 28	The Organization must conduct ongoing due diligence around the data privacy and security posture of vendors/processors
8. Maintain Notices	
Article 8, Article 13, Article 14, Article 21,	The Organization must maintain a data privacy notice that details the Personal Data handling practices (including when Personal Data are collected)
9. Manage Requests from Individuals	
Article 15	The Organization must establish and enforce procedures to respond to requests for access to personal data
Article 16, Article 19	The Organization must establish and enforce procedures to respond to requests and/or provide a mechanism for individuals to update or correct their Personal Data
Article 7, Article 18, Article 21	The Organization must establish and enforce procedures to respond to requests to opt–out of, restrict or object to processing

Article 20	The Organization must establish and enforce procedures to respond to requests for data portability
Article 17, Article 19	The Organization must establish and enforce procedures to respond to requests to be forgotten or for erasure of data
10. Monitor for New Operational Practices	
Article 25	The Organization must integrate Privacy by Design into system and product development frameworks
Article 5, Article 6, Article 26, Article 35	The Controller is responsible to conduct DPIAs in order to assess the impact of processing operations on the protection of personal data where the processing is likely to result in a high risk for the rights and freedoms of data subjects
Article 5, Article 6, Article 26, Article 35	The Controller is responsible to conduct DPIAs in order to assess the impact of processing operations on the protection of personal data where the processing is likely to result in a high risk for the rights and freedoms of data subjects
Article 36	The Organization must report DPIA results to relevant authorities (where required)
11. Maintain Data Privacy Breach Management Program	
Article 33, Article 34	The Organization must establish and enforce a Privacy Incident/Breach Management procedure and appropriate artefacts must be maintained
Article 12, Article 33, Article 34	The Organization must establish a notification mechanism in order to inform relevant authorities and affected individuals, where required, in case of a data breach
12. Monitor Data Handling Practices	
Article 5, Article 24, Article 39	The Controller is responsible to conduct self-assessments of privacy management and to maintain appropriate artefacts in order to demonstrate compliance and/or accountability
13. Track External Criteria	
Article 39	The DPO is responsible to conduct regular research in order to maintain expert knowledge with respect to privacy and data protection law and practices and to determine what, if any, changes to the privacy program need to be made as a result of any legal or regulatory developments

Table 5: General Data Protection Regulation (GDPR)

Chapter 4: Comparison among ISO 27002, NIS Directive and GDPR

In this Chapter, it has been carried out a comparison among the controls of ISO/IEC 27002:2013, ISO/IEC 27002:2022, NIS Directive and General Data Protection Regulation (GDPR), which is presented into the additional attached Microsoft Excel file “Mapping_ISO-NIS-GDPR.xlsx”.

Mapping_ISO-NIS-GD
PR.xlsx

Conclusion

Although ISO/IEC 27001, NIS Directive and GDPR are related to different types of data they overlap since security and data protection are related to each other. Moreover, these regulations and frameworks aim at protecting organization against cyber-attacks. Their adoptions from the organisations is often a challenging task as CISOs and DPOs face difficulties understanding their roles and design consistent cybersecurity frameworks inside their organisations, due to the regulations' requirements overlapping. To address this issue a mapping of ISO 27001, GDPR and NIS Directive requirements is presented that can help organisations to adopt properly to these regulations, help them to identify current potential security issues and structure new security plans.

References

[1] V. P. P. d. H. Dimitra Markopoulou, "ScienceDirect," July 2019. [Online]. Available: https://www.sciencedirect.com/science/Article/pii/S0267364919300512. [Accessed June 2022].

[2] N. A. M. D. Mar, "The NIS2 Directive: A high common level of cybersecurity in the EU," June 2022. [Online]. Available: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333. [Accessed June 2022].

[3] W. Z. L. M. Vasileios Germanos, "ResearchGate," June 2020. [Online]. Available: https://www.researchgate.net/publication/342170762_Mapping_of_the_Security_Requirements_of_GDPR_and_NIS. [Accessed June 2022].

[4] D. Kosutic, "Advisera," [Online]. Available: https://advisera.com/27001academy/what-is-iso-27001/?utm_source=%20how-iso-27001-can-help-eu-gdpr-compliance&utm_medium=downloaded-content&utm_content=lang-en&utm_campaign=free-knowledgebase-27001. [Accessed July 2022].

[5] ISO/IEC JTC 1/SC 27, "iso.org," February 2018. [Online]. Available: https://www.iso.org/standard/73906.html. [Accessed June 2022].

[6] "iso.org," ISO, [Online]. Available: https://www.iso.org/isoiec-27001-information-security.html. [Accessed June 2022].

[7] L. Irwin, "itgovernance.co.uk," 19 October 2020. [Online]. Available: https://www.itgovernance.co.uk/blog/what-is-the-iso-27000-series-of-standards#:~:text=The%20series%20consists%20of%2046,clarifying%20key%20terms%20and%20definitions.. [Accessed June 2022].

[8] "itgovernance.co.uk," [Online]. Available: https://www.itgovernance.co.uk/iso27001. [Accessed June 2022].

[9] "tgovernance.co.uk," [Online]. Available: https://www.itgovernance.co.uk/iso27001-and-iso27002-2022-updates. [Accessed June 2022].

[10] ISO/IEC JTC 1/SC 27, "iso.org," February 2022. [Online]. Available: https://www.iso.org/standard/75652.html. [Accessed June 2022].

[11] Enisa, "Enisa," [Online]. Available: https://www.enisa.europa.eu/topics/nis-directive. [Accessed June 2022].

[12] THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, "EUR-Lex," July 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN. [Accessed June 2022].

[13] ENISA, "ENISA-Minimum Security Measures for Operators of Essentials Services," [Online]. Available: https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services. [Accessed June 2022].

[14] ENISA, "ENISA-ENISA launches a tool which maps security measures for OES to international standards," November 2019. [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/enisa-launches-oes-tool-to-map-security-measures. [Accessed June 2022].

[15] "European Commission-NIS Directive," [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/nis-directive. [Accessed June 2022].

[16] T. E. P. A. O. T. COUNCIL, "EUR-Lex," December 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN. [Accessed June 2022].

[17] M. Burgess, "WIRED," March 2020. [Online]. Available: https://www.wired.co.uk/Article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018. [Accessed June 2022].

[18] THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,, "EUR-Lex," April 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj. [Accessed June 2022].

[19] "TESSIAN," May 2022. [Online]. Available: https://www.tessian.com/blog/biggest-gdpr-fines-2020/#:~:text=1.,bigger%20than%20the%20previous%20record.. [Accessed June 2022].