DIGITAL SECURITY
AUTHORITY

NIS Directive Security Measures

Version 0.5 – DRAFT FOR PUBLIC CONSULTATION

21/01/2019

Digital Security Authority

1. DOCUMENT CONTROL

Document owner:	Digital Security Authority
Master copy storage location:	

Version	Reviewed by	Approved by	Approver's position	Date approved

Version	Updated by	Date	Description of changes
0.5	DSA	21/01/2019	Draft for Public Consultation

2. ABSTRACT

This document provides a catalogue of information security controls for operators of essential services and critical information infrastructures within Cyprus. The information security controls in this framework are to be established, implemented and maintained within an information security risk management system, which serves as a continuous process for identifying, analysing, evaluating and treating threats, vulnerabilities and risks with respect to the confidentiality, integrity, availability, authenticity and resilience of network and information systems. The Digital Security Authority has the mandate to enforce this framework upon operators of essential services and critical information infrastructures in Cyprus in order to enhance the national cyber security posture of Cyprus, implement part of the National Cybersecurity Strategy, and contribute to and support European cyber security efforts in context of the Directive on Network and Information Security (NIS Directive).

3. TABLE OF CONTENTS

4. PREAMBLE

On 6 July 2016, the European Parliament has adopted the Directive on the security of network and information systems (hereafter referred to as the *"NIS Directive"*). The NIS Directive entered into force in August 2016 and the Member States had up until 9 May 2018 to transpose the Directive into national legislation.

With respect to Article 8 – National competent authorities and single points of contacts – Cyprus has established the Digital Security Authority (hereafter referred to as the *"DSA"*). The DSA has been tasked with, amongst others, the implementation of the NIS Directive into national legislation and thereby effectively acting as the national competent authority for network and information security within Cyprus, including the role of Single Point of Contact (SPOC). The DSA also incorporates the National CSIRT for Cyprus (CRIST-CY).

Article 14 – Security requirements and incident notification for operators of essential services - of the NIS Directive, requires Cyprus to ensure that operators of essential services (OES) take appropriate and proportionate technical and organisational measures to manage risks posed to the security of network and information security, which they use in their operations. The objective of this provision is to enhance network and information security of entities critical and vital to the economy and functioning of the Member States and Europe as a whole.

In this context, the DSA has developed this NIS Cyber Security Framework (hereafter referred to as *"the Framework")* and supporting security measures in collaboration with operators of essential services and critical information infrastructure (CII) within Cyprus. The Framework has been designed taking into account the specifics and particularities of network and information security with respect to Cyprus operators of essential services and critical information infrastructure by consulting with the key stakeholders in the community. Stakeholder consultation included stakeholder interviews, targeted questionnaires, and Public Consultation prior to publication, in order to tailor the Framework and supporting measures to the needs and expectations of operators of essential services and critical information infrastructure within Cyprus.

Taking into account the specific context and conditions of Cyprus operators of essential services and critical information infrastructure, the DSA has consulted with international organisations, and providers of best practices and cyber security advisory services, in order to ensure alignment with international standards and guidelines with respect to network and information security. The DSA has taken into account network and information security guidelines and standards published by, amongst others, the International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) [e.g. ISO/IEC 27001:2017, ISO/IEC 27032:2012], the US National Institute of Standards and Technology (NIST) [e.g. SP800-53, SP800-82, Cybersecurity Framework], and International Society of Automation (ISA) [e.g. ISA99]. In addition, the DSA has consulted and analysed the guidelines and publications of the European Agency for Network and Information Security (ENISA) related to protecting critical infrastructures and services.

The DSA has established this security measures framework in alignment with the reference document on security measures for Operators of Essential Services (CG Publication 01/2018) published by the NIS Cooperation Group. This document is the result of a pan-European discussion amongst representatives of all Member States concerning achieving a high level of common security within Europe in context of the NIS Directive. This document sets forth the foundational pillars for a good cyber security posture in relation to the security requirements in the NIS Directive. This framework has been aligned with this guideline, and combined with other best practices found in international standards and frameworks.

5. EXECUTIVE SUMMARY

The Framework and supporting measures focus on strengthening the security posture of operators of essential services and critical information infrastructure providers in Cyprus by adopting adequate information security controls supported by risk management processes, including the following building blocks.

PREPARE requirements, which aim to ensure operators of essential services and critical information infrastructure providers are taking into account information security risks in day-to-day operations and ensure top-level management commitment to address information security threats, vulnerabilities and risks.

This first building block contains controls relating to the development of an information security strategy, information security governance (i.e. the definition of information security roles and responsibilities; compliance with legal and regulatory requirements; creation of information security policies, standards, guidelines and procedures), risk management (i.e. the establishment of the organisation's risk management methodology and surrounding processes); information security training and awareness, and third party and supplier management.

PROTECT and DETECT requirements, which aim at protecting organisational assets from unauthorised processing by ensuring that operators of essential services and critical information infrastructure providers establish, implement and maintain adequate information security measures appropriate to their risk exposure.

This second building block entails preventive, detective and reactive measures from a technological, administrative and physical perspective in the following sub-categories: data security, change management, asset management, identity and access management, vulnerability and patch management, network security, system security, human resources security, and physical security.

RESPONSE requirements, of which the objective is to ensure that operators of essential services and critical information infrastructure providers are able to respond to information security events and incidents that could affect the confidentiality, integrity, availability or authenticity of information. The aim of these controls is to ensure that organisations can detect, analyse, contain and adequately recover from security events. One of the main objectives is to ensure that the organisation has a plan in place to maintain continuity of its critical business processes in case of a security incident.

This third building block entails the adoption of operational resilience and business continuity measures of the following sub-categories: event and incident management, and business continuity and resilience.

6. NIS CYBER SECURITY FRAMEWORK

The NIS Directive requires operators of essential services and critical information infrastructure providers to implement appropriate technical and organisational measures to manage the risks posed towards the security of their network and information systems, which support the delivery of essential and critical services. The NIS Cyber Security Framework aims to assist operators of essential services and critical information infrastructure providers in Cyprus to comply with these obligations under the NIS Directive.

The NIS Cyber Security Framework contains a general risk management provision, which imposes the obligation on operators of essential services and critical information infrastructure providers to establish, implement and maintain a risk management process. Next to the general provision, the framework includes specific information security measures to be implemented based on the outcome of the risk assessment carried out by operators of essential services and critical information infrastructure providers.

The risk management process and specific measures are detailed in the sections below.

6.1 Risk Management

This Framework is supported by information security measures as defined in section 7 of this document. The purpose of these measures is to enable operators of essential services to reduce security risks identified by the risk management processes. In order to identify adequate technical and organisational measures to reduce such risks, this framework introduces specific controls to mitigate various risk domains. Operators of essential services and critical information infrastructure providers should select and implement controls based on the outcome of their risk management processes (as described in the general risk management provision of the Framework) in order to ensure appropriate risk treatment of the specific risks posed to their organisational assets.

1. Taking into account the state of the art, the costs of implementation and the risk of varying likelihood and impact on the confidentiality, integrity, availability and authenticity of information, the operator of essential services or critical information infrastructure provider shall establish, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The organisation shall implement the information security measures in order to reduce risk to an acceptable level and to ensure appropriate risk treatment, unless the controls are inadequate with regards to the organisation's specific situation based, among others, on its risk management processes. If the organisation considers the controls to be inadequate, or it has to consider additional obligations (e.g. from another legal framework), then the organisation must decide how to appropriately treat the risks that it has identified.

2. In order to assess the appropriate level of security, the organisation shall establish, implement and maintain a process for information security risk management, including as appropriate:
   a) Determination of the organisational context including the criteria to assess and mitigate information security risks, including roles and responsibilities, risk owners, risk assessment criteria for impact and likelihood, risk score scales, risk evaluation criteria and risk appetite/risk tolerance.
   b) Identification of information security risks taking into account various threat, threat scenarios and vulnerabilities with regards to the confidentiality, integrity, availability and authenticity of information.
   c) Analysis of information security risks taking into account the risk assessment criteria impact, likelihood, and other relevant criteria in order to determine a risk score.
   d) Evaluation of information security risks taking into account the risk evaluation criteria and risk appetite in order to determine appropriate risk treatment strategies.
   e) Treatment of information security risks taking into account inter alia, risk retention/acceptance, risk transfer, risk avoidance or risk reduction.

3. In assessing the appropriate level of security, account shall be taken in particular of the risks resulting from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to information transmitted, stored or otherwise processed.

4. In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented that could have a potential impact on vital economical and societal functions and services provided by the operator of essential services or critical information infrastructure provider.

5. The Digital Security Authority shall have the right to obtain access to the risk management process and the risk treatment plan established by the operator of essential services or critical information infrastructure provider. If the Digital Security Authority is judges that the risk management process and the risk treatment plan do not appropriately address the risk identified by the operator of essential services or critical information infrastructure provider, the Digital Security Authority shall have the power to impose and enforce corrective actions by the operator of essential services or critical information infrastructure provider.

6.2 Network and information (NIS) officer

Achieving the information security objectives detailed in this framework requires the allocation of roles and responsibilities for network and information security within the organisation. More specifically, accountability and responsibility are key prerequisites in order to achieve reliable and effective information security governance. Therefore, this framework requires critical information infrastructures and operators of essential services to designate an information security officer, and ensure that he or she is appropriately resourced and trained in order to be able to deliver on the relevant responsibilities.

[Designation of the information security officer]

1. The operator of essential services or critical information infrastructure provider shall designate an information security officer, whereas:
   a) the information security officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of network and information security and the ability to fulfil the tasks referred to in [Article on minimum responsibilities of the information security officer]
   b) the information security officer shall be a dedicated resource. For very small organisations, the information security officer may fulfil other tasks and duties, which do not however result in a conflict of interest, subject to the approval of the DSA.
   c) the operator of essential services or critical information infrastructure provider shall publish the contact details of the information security officer and communicate them to the supervisory authority.
   d) the operator of essential services or critical information infrastructure provider shall ensure candidates for the position of information security officer are adequately screened in order to ensure this person delivers due diligently on its responsibilities.

[Minimum responsibilities]

1. The information security officer designated by operator of essential services or critical information infrastructure provider shall have at least the following tasks:
   a) to inform and advise the operator of essential services or critical information infrastructure provider and the employees who have access to network and information systems, of their obligations pursuant to this framework.
   b) to monitor compliance with this framework, with other national or European information security provisions and with the policies of the operator of essential services or critical information infrastructure provider in relation to the security of network and information systems.
   c) to provide advice as regards to information security management and monitor its performance pursuant to [ARTICLE X/Risk management provision (Section 6.1)].
   d) to cooperate with, and act as a single point of contact for the Digital Security Authority on topics related to the activities performed by the national competent authority as part of its official mandate, including providing support to external audit activities, pro-actively providing accountability documentation such as the risk treatment plan and risk register pursuant to [ARTICLEX/Accountability requirements].
   e) to report on information security threats, vulnerabilities and risks towards top-level management by the means of formal and recurrent reporting lines through appropriate governance bodies.

[Position of the information security officer]

1. The operator of essential services or critical information infrastructure provider shall ensure the information security officer is involved, properly, and in a timely manner, in all issues which relate to the security of network and information systems.
2. The operator of essential services or critical information infrastructure provider shall support the information security officer in performing the tasks referred to in [Article on minimum responsibilities of the information security officer] by providing resources necessary to carry out those responsibilities, and to maintain his or her expert knowledge by receiving appropriate training and engage in industry forums such as relevant conferences and workshops.
3. The operator of essential services or critical information infrastructure provider shall ensure that the information security officer does not receive any instructions conflicting with the exercise of those tasks. He or she shall not be dismissed or penalised by the operator of essential services or critical information infrastructure provider for due diligently performing his or her tasks.
4. The information security officer shall directly report to the highest management level of the operator of essential services or critical information infrastructure provider.
5. The information security officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with [National legislation on professional secrecy]

6.3 Accountability

This framework requires operators of essential services and critical information infrastructure providers to document all relevant information in relation to information security risk management and to provide this documentation to the Digital Security Authority upon request, in order to achieve the information security objectives as required by this framework.

The operator of essential services or critical information infrastructure provider shall be able to provide the following documentation to the Digital Security Authority, in order to demonstrate compliance with its responsibilities under this framework:

1. The risk management methodology, including risk assessment criteria for impact and likelihood, risk score scales, risk evaluation criteria and risk appetite/risk tolerance, pursuant to [ARTICLE X/Risk management provision (Section 6.1)].
2. The risk assessment, including the identification, analysis and evaluation of all information security risks within the organisation, pursuant to [ARTICLE X/Risk management provision (Section 6.1)];
3. The risk register, which provides an overview of the risk analysis and risk evaluation of all information security risks identified within the organisation;
4. The risk treatment plan, which specifies the remediation measures for all information security risks identified within the organisation, i.e. risk retention/acceptance, risk transfer, risk avoidance or risk reduction, pursuant to [ARTICLE X/Risk management provision (Section 6.1)];
5. The governance structure including internal roles and responsibilities with regards to network and information security, pursuant to [ARTICLE X/Information Security Officer (Section 6.2)];
6. The security policy and information security strategy;
7. The network and information security control implementation plan, which provides a control implementation tracker on an operational level;
8. The business continuity plan;
9. The disaster recovery plan.

6.4 Powers of the Digital Security Authority

In order to ensure the enforceability of this security measures framework, it is essential to confer investigative and corrective powers upon the Digital Security Authority. The Digital Security Authority should also have the power to issue opinions and guidelines in order to assist operators of essential services and critical information infrastructure providers to implement the security measures in the framework.

The Digital Security Authority shall have the investigative and corrective powers to

1. Order the operator of essential services or critical information infrastructure provider to provide all relevant documentation pursuant to [ARTICLE X/Accountability provision (Section 6.3)].
2. Issue guidelines and binding instructions to operators of essential services and critical information infrastructure providers regarding the format and provision of documentation and information to the Digital Security Authority.
3. Perform information security audits in order to assess whether the operator of essential services or critical information infrastructure provider complies with its obligations as described in this framework.
4. Issue guidelines and binding instructions with respect to operators of essential services and critical information infrastructure providers who fail to meet their obligations in this framework.

In addition, the Digital Security Authority shall have the power to issue official opinions and guidelines in order to help operators of essential services and critical information infrastructure providers with the implementation of specific controls in this framework.

6.5 NIS Security Measures

The DSA NIS Security Measures Framework consists of three main building blocks (PREPARE, PROTECT AND DETECT, and RESPOND) in order to establish, implement and maintain a layered-defence approach with respect to ensuring confidentiality, integrity, availability, authenticity resilience of network and information systems.

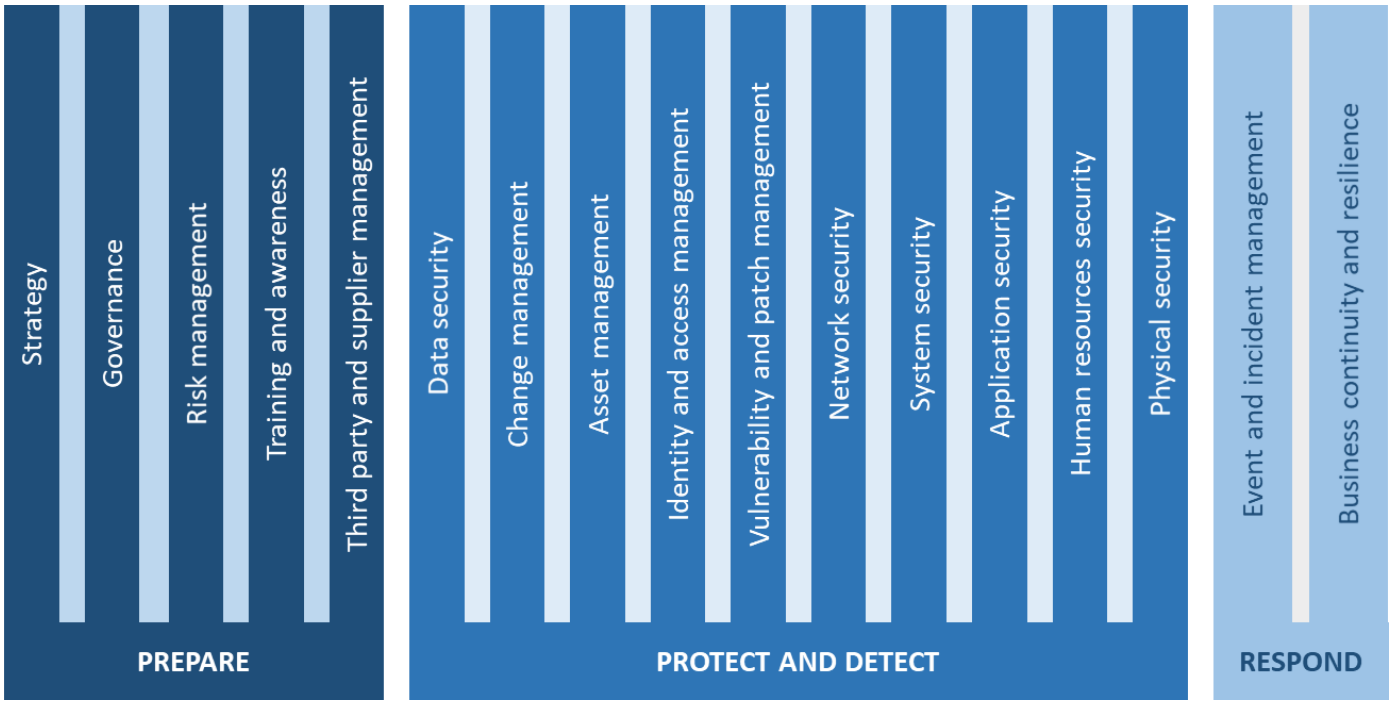

Figure 1 - Visual representation of the DSA NIS Security Measures Framework building blocks and control domains

The objectives of the three main building blocks are explained below:

Table 1 - Objectives of control domains and subdomains

Domain	PREPARE	PROTECT AND DETECT	RESPOND
Objective	The objective of the PREPARE building block is to ensure operators of essential services and critical infrastructures are taking into account information security risk in day-to-day operations and ensure top-level management commitment to address security threats, vulnerabilities and risks.	The objective of the PROTECT AND DETECT building block is to ensure operators of essential services and critical infrastructures establish, implement and maintain adequate information security measures appropriate to their risk exposure. This building block entails adopting preventive, detective and reactive measures from a technological, administrative and physical perspective.	The objective of the RESPOND building block is to ensure operators of essential services and critical infrastructures are able to respond to information security events and incidents that could affect the confidentiality, integrity, availability or authenticity of information. This building block entails adoption of operational resilience and business continuity and disaster recovery measures, as well as restoration to normal operations.

7. NIS SECURITY MEASURES

The NIS Security Measures are detailed below, categorised by domain and subdomain, including control objective and description.

7.1 PREPARE

The objective of the PREPARE building block is to ensure operators of essential services and critical infrastructures are taking into account information security risk in day-to-day operations and ensure top-level management commitment to address security threats, vulnerabilities and risks.

Domain	Subdomain	Ref.	Control	Control objective	Control description
PREPARE	Strategy	STR1	Information security strategy	To establish an information security strategy detailing the high-level objectives and approach in order to mitigate information security risks.	Define vision and commitment on information security in a strategy that details specific security objectives, approach to security and risk management, and means to validate the effectiveness of the strategy supported by key performance indicators. The information security strategy shall be reflected in the information security policy as described in control [GOV3]. Co-workers shall be aware of the information security strategy and policy as described in [TA1].
PREPARE	Governance	GOV1	Information security roles and responsibilities	To define information security roles and responsibilities within the organisation.	Define roles and responsibilities with respect to network and information security for all co-workers that are involved with the processing of information or have access to information processing systems. The defined roles and responsibilities shall be reflected in the information security policy [GOV3]. Co-workers shall be adequately informed and aware of their roles and responsibilities with regard to network and information security as defined in [TA1, TA2, TA3]. Information security roles and responsibilities should be designated within the management committee in order to ensure accountability for management decisions related to the security of network and information systems.
PREPARE	Governance	GOV2	Compliance with legal and regulatory requirements	To ensure compliance with all applicable legal and regulatory requirements with respect to network and information security.	Establish and maintain a central repository of, and be compliant with, all relevant legislative, statutory, regulatory, contractual requirements with respect to network and information security.

Domain	Subdomain	Ref.	Control	Control objective	Control description
PREPARE	Governance	GOV3	Information security policies, standards, guidelines and procedures.	To establish information security policies, standards, guidelines and procedures reflecting the information security strategy.	Define information security measures, and detail their implementation, into an information security policy reflecting the objectives as described in the information security strategy [STR1]. The information security policy should encompass organisation-wide roles and responsibilities as defined in [GOV4]. Specific information security policies and procedures shall be implemented for individual processes, systems or activities as needed. Information security operational guidelines and standard operating procedures shall be defined for specific activities that relate to information or information processing systems on an operational level.
PREPARE	Risk management	RM1	Methodology	To establish a risk management methodology, which reflects the organisation's risk assessment process, risk analysis criteria, risk acceptance criteria and risk appetite.	Establish a risk management methodology by defining the risk assessment process, the risk analysis criteria (i.e. impact criteria, likelihood criteria, risk scores), the risk acceptance criteria and the organisation's risk appetite. The risk management methodology will enable the organisation to assess the information security risks faced by the organisation and to implement adequate measures in order to treat or mitigate them. The organisation should put in place processes and tools as appropriate in order to support the risk management processes, at a minimum, a risk register, risk treatment plan, and an information security governance structure detailing roles and responsibilities. The defined risk management methodology should be validated, agreed and supported by top-level management and other relevant stakeholders within the organisation.
PREPARE	Risk management	RM2	Context	To establish a list of assets, systems, and processes within the organisation.	Establish a list of assets, systems and processes within the organisation and create an overview of the dependencies and interdependencies between these assets, systems and processes in order to clearly capture the context in which the risk assessment will be carried out. A clear view on the context of the organisation will enable the organisation to locate the risks identified within the organisation.

Domain	Subdomain	Ref.	Control	Control objective	Control description
PREPARE	Risk management	RM3	Risk identification	To identify threats, vulnerabilities and risks the organisation's assets, systems and processes are exposed to.	To identify and create a list of threats, vulnerabilities and risks the organisation is exposed to with regards to the assets, systems and processes as identified in [RM2]. The organisation is required to reflect the outcome of the risk identification in a risk register to enable the organisation can keep track of the threats, vulnerabilities and risks the organisation is exposed to.
PREPARE	Risk management	RM4	Risk analysis	To analyse information security risks in context of organisational assets with respect to varying likelihood and impact.	Analyse information security risks with respect to organisational assets as identified in [RM2] taking into account varying likelihood and impact scores as defined in [RM1]. The organisation shall determine a risk score in order to evaluate the appropriate mitigation strategy in [RM5]. In assessing the appropriate level of security, account shall be taken in particular of the risks resulting from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to information transmitted, stored or otherwise processed. In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented that could have a potential impact on vital economical and societal functions and services provided by the operator of essential services or critical information infrastructure provider. The outcome of the risk analysis should be documented in the organisational risk register.
PREPARE	Risk management	RM5	Risk evaluation	To evaluate information security risks based on the organisational risk appetite and determine appropriate treatment strategies.	Determine appropriate and adequate treatment strategies for risks analysed as described in [RM4]. The organisation shall take consider risk reduction, risk transfer, risk avoidance and risk acceptance (or retention) as appropriate risk treatment strategies. In evaluating the risk treatment strategies, the organisation shall take into account the risk appetite as defined in [RM1]. The outcome of the risk evaluation should be documented in the organisational risk register.

Domain	Subdomain	Ref.	Control	Control objective	Control description
PREPARE	Risk management	RM6	Risk treatment	To determine risk treatment actions in order to treat information security risks.	Determine appropriate and adequate risk treatment measures in order to fulfil the risk treatment strategy as determined in the risk evaluation process as described in [RM5]. In determining measures or controls, the organisation shall consider preventive, detect and reactive measures, from an administrative, technological and physical perspective in order to ensure a layered defence as appropriate. The organisation shall consider the security measures as described in the DSA NIS Security Measures Framework (this document) when determining risk treatment actions. The outcome of the risk treatment should be documented in the organisational risk treatment plan.
PREPARE	Training and awareness	TA1	Information security awareness program	To establish an information security awareness program for all co-workers within the organisation taking into account the elements described in the information security policies, standards, guidelines and procedures.	Define an information security awareness program in order to have adequate awareness amongst co-workers about roles and responsibilities with regard to network and information security as defined in [GOV4].
PREPARE	Training and awareness	TA2	Information security awareness, education and training	To provide information security awareness, education and training to all co-workers in the organisation as defined in the information security program.	Employees are adequately informed and aware about their roles and responsibilities with regard to network and information security - as defined in [GOV4] by means of appropriate awareness, education and training efforts conducted by support of top-level management. Information security awareness, training and education shall incorporate specific information related to operational activities performed by co-workers on behalf of the organisation in context of processing of information or access to information processing systems.
PREPARE	Third party and supplier management	TPS1	Third party and suppliers due diligence	To perform due diligence on third parties and suppliers.	Adequate due diligence should be performed when identifying and entering into a relationship with third parties and suppliers, taking into account third party risks, inter alia, vendor lock-in, incident management and liability with respect to network and information security. The organisation shall, in particular, take into account information security due diligence when engaging with third parties in context of software acquisition or delivery by third parties.

Domain	Subdomain	Ref.	Control	Control objective	Control description
PREPARE	Third party and supplier management	TPS2	Third party and supplier relationships	To ensure contractual safeguards are embedded in relationships with third parties and suppliers.	Maintain a central repository of suppliers, vendors and other third parties. The organisation should ensure all third party relationships are supported by adequate contractual safeguards in order to ensure that inter alia, roles and responsibilities as defined in [TPS3], and liability in case of incidents with regard to network and information security are appropriately documented.

7.2 PROTECT AND DETECT

The objective of the PROTECT AND DETECT building block is to ensure operators of essential services and critical infrastructures establish, implement and maintain adequate information security measures appropriate to their risk exposure. This building block entails adopting preventive, detective and reactive measures from a technological, administrative and physical perspective.

Domain	Subdomain	Ref.	Control	Control objective	Control description
PROTECT AND DETECT	Data security	DS1	Information lifecycle management	To ensure data is protected during the entire information lifecycle including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.	Establish, implement and maintain information security controls in order to protect information across the entire information lifecycle. The information lifecycle should be considered as all stages that relate to the processing of information, whereas processing refers to any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
PROTECT AND DETECT	Data security	DS2	Classification and labelling of information	To ensure data is classified and labelled to reflect its sensitivity in order to ensure data is handled accordingly.	Establish, implement and maintain a data classification and labelling policy that ensure information is classified and labelled according to the confidentiality and sensitivity. Consider implementing classification and labelling schemes based on international and industry best practices such as the Traffic Light Protocol. At a minimum, the organisation should distinguish public, private, and classified information.
PROTECT AND DETECT	Data security	DS3	Backup and data recovery	To ensure information can be restored from a back-up in context of security events and incidents.	Establish, implement and maintain a backup and data recovery process in order to ensure timely and effective restore of data after the occurrence of an event, incident, or at the request of a subject. Backup and data recovery processes should be adequately and frequently tested in order to ensure proper and reliable functioning of all supporting processes and systems. Supporting systems and infrastructure to enable backup and restore should be adequately geographically spread (offsite backup) in order to protect from physical security risks.

Domain	Subdomain	Ref.	Control	Control objective	Control description
PROTECT AND DETECT	Data security	DS4	Information transfers and exchange	To ensure adequate safeguards are adopted in context of information transfers and information exchange with internal and external parties in order to ensure secure data transfer.	Establish, implement and maintain information transfer and exchange processes in order to ensure information is protected while in transfer or while being exchanged with internal or external third parties. Information transfer and exchange should take into account regulatory and legislative requirements as defined in [GOV3], for example when processing information in context of international data transfers.
PROTECT AND DETECT	Data security	DS5	Data loss and data leakage prevention	To ensure data is protected against intentional or unintentional data loss and leakage.	Establish, implement and maintain reasonable measures to reduce the risk of data loss and data leakage by considering appropriate technical and organisational measures for prevention. Data loss and data leakage prevention measures should consider external and internal threat vectors that could potentially disclosure classified information. Adequate access control measures should be implemented to interface with Data loss and data leakage prevents as the policies on data sharing and disclosure should be role-based, as defined in [IAM1]. When establishing data loss and data leakage prevention measures, the organisation should consider classification, tracking, protection and monitoring of information.
PROTECT AND DETECT	Change management	CM1	Change management	To ensure changes to information processes and systems are implemented securely without affecting the confidentiality, integrity, availability or authenticity of information.	Establish, implement and maintain a change management process in order to control and manage changes to systems, applications and other supporting assets in context of processing of information. When establishing the change management process, the organisation shall consider change requests in order to capture changes requested by subjects. The change management process should enable the organisation to assess risks in context of change requests, and plan changes taking into account adequate security measures accordingly. The change management process should include provisioning and verification of changes.

Domain	Subdomain	Ref.	Control	Control objective	Control description
PROTECT AND DETECT	Change management	CM2	Configuration management	To identify, maintain and verify information on assets and configurations in the organisation.	Establish, implement and maintain a configuration management processes in order to control and manage configurations of organisational assets supporting network and information systems. The organisation shall maintain a register of configurations applicable to these assets. Organisations shall determine and document the relationships between asset configurations in order to identify interdependencies and ensure appropriate change management towards the modification of configurations.
PROTECT AND DETECT	Asset management	AM1	Asset lifecycle management	To ensure assets are secure during the entire asset lifecycle including procurement, deployment, maintenance, and disposal.	Establish, implement and maintain information security controls in the asset lifecycle management plan in order to ensure information security is embedded throughout all phases of the asset lifecycle, i.e. procurement, deployment, maintenance, and disposal. Information lifecycle management as described in [DS1] should be part of the asset lifecycle management plan. The asset lifecycle management plan should describe all procedures for handling information in accordance with the data classification and labelling policy as described in [DS2].
PROTECT AND DETECT	Asset management	AM2	Inventory of assets and ownership	To ensure assets are captured in an inventory and ownership is defined in order to achieve traceability and accountability of assets.	Establish, implement and maintain an inventory of the assets in order to ensure the organisation has a clear, accurate and up-to-date overview of the assets (e.g.. hardware, software, information) it maintains. The inventory should specify the owner of the assets. The inventory should enable the organisation to keep track of all assets for which it should implement and maintain information security controls.
PROTECT AND DETECT	Asset management	AM3	Asset monitoring	To ensure assets are monitored security attacks, anomalies, and threats in order to trigger event and incident response processes accordingly.	Establish, implement and maintain asset monitoring capabilities in order enable the organisation to detect anomalies in the normal conditions (e.g. location, use...) and/or functioning of the assets. The organisation should indicate in the acceptable use policy, as described in [HRS6], what constitutes legitimate use and/or functioning of the assets. The organisation could also consider describing the legitimate use, functioning and location of assets in the inventory of the assets as described in [AM2] in order to create a comprehensive inventory of the assets. Once anomalies are detected, event and incident management

Domain	Subdomain	Ref.	Control	Control objective	Control description
					processes should be triggered in order to withstand irregularities in the organisation.
PROTECT AND DETECT	Asset management	AM4	Availability management	To ensure availability of network and information systems by achieving adequate availability of resources, redundancy and high-availability of systems and processes.	Establish, implement and maintain availability management processes in order to ensure the targeted level of operational services is provided by the organisation. The organisation should ensure that the availability of resources (e.g. premises, personnel, IT systems, etc.) is guaranteed at all times. As described in [NS6], the organisation should guarantee redundancy and high-availability for all IT systems. In order to ensure timely and effective recovery of data after the occurrence of an event or incident, or at the request of a subject. The organisation should create back-ups of information as described in [DS3].
PROTECT AND DETECT	Asset management	AM5	Cryptographic controls	To ensure the confidentiality, integrity and authenticity of information by adopting adequate cryptographic solutions.	Establish, implement and maintain a policy on the use of cryptographic controls in order to ensure confidentiality, integrity and authenticity of data at rest, data in use, and data in transit. The cryptographic control policy should take into account the application of cryptographic measures in all stages of the information lifecycle and consider applications, systems, network equipment and communication channels.
PROTECT AND DETECT	Asset management	AM6	Capacity management	To ensure appropriate capacity for, and service performance levels of, information systems and processes.	Establish, implement and maintain a capacity management process in order to ensure that the capacity and performance of the organisation's IT systems are not negatively affected by increased service demand levels. The capacity management process should include business capacity management in order to ensure business needs are translated in capacity requirements, service capacity management in order to manage the capacity of operational services, component capacity management in order to manage the performance of all IT systems and components and a capacity management reporting mechanism.

Domain	Subdomain	Ref.	Control	Control objective	Control description
PROTECT AND DETECT	Identity and access management	IAM1	Role based access control	To ensure subjects are authenticated and authorised on a least-privilege basis supported by organisational roles and responsibilities.	Establish, implement and maintain identity and access management measures that consider role based access controls in order provide technical and organisational means to enforce the least privilege principle and manage privileged users accordingly. Role based access control should ensure adequate permissions are granted to subjects based on the responsibilities linked to respective roles. Role based access control should be integration with human resources security processes as, defined in [HRS1], in order to ensure access roles are aligned with effective roles and responsibilities of subjects within the organisation.
PROTECT AND DETECT	Identity and access management	IAM2	External access controls	To ensure adequate safeguards are adopted in context of external access to organisational resources.	Establish, implement and maintain access controls for external and remote access to organisational resources. The organisation should mandate secure remote network access supported by Virtual Private Networks (VPN), and secure access to remote applications by using external application interfaces. The organisation shall ensure adequate identity and access management measures are implemented to reflect the information security policy, as defined in [GOV4], and specific role based access control, as defined in [IAM1].
PROTECT AND DETECT	Identity and access management	IAM3	Privileged users management	To ensure adequate safeguards are adopted for users that have privileged access to organisational resources, systems and networks.	Establish, implement and maintain measures to ensure privileged users are adequately managed and only activated on a need-to-have basis. The organisation shall ensure that subjects are not granted privileged user rights by default and adequate technical and organisational measures are implemented to ensure privileged user rights are protected from malicious, or otherwise negatively affecting, behaviour and intent. The organisation shall ensure systems and applications are not operating with privileged user rights by default in order to mitigate the risk of privilege escalation and privilege elevation.

Domain	Subdomain	Ref.	Control	Control objective	Control description
PROTECT AND DETECT	Identity and access management	IAM4	Strong authentication	To ensure authorised subjects authenticate securely and strong authentication measures are adopted.	Establish, implement and maintain strong access control and authentication measures in order to ensure subjects are adequately identified and authenticated when processing organisational resources. The organisation shall consider multi-factor authentication in order for a subject to prove its identity. Multi-factor authentication should encompass at least two of the following principles: identity provision by demonstrating ownership of an element (e.g. key or other physical authentication means) identity provision by demonstrating knowledge of an element (e.g. password, passphrase or other secret), identity provision by demonstrating biometrical or morphological ownership (e.g. iris scan, finger print or visual authentication by a trusted party such as a security guard).
PROTECT AND DETECT	Identity and access management	IAM5	Credential management	To ensure credentials to corporate resources are securely managed and subjects authenticate securely to organisational services.	Establish, implement and maintain credential management processes in order to ensure adequate management of identification and authentication means by which subjects can access organisational resources. The organisation should consider federated credentials (e.g. single sign-on) in order to enhance the identity and access management user experience and reduce authentication friction. The organisation shall consider credential management for subjects, systems and networks in order to ensure access control across the information lifecycle, as defined in [DS1].
PROTECT AND DETECT	Identity and access management	IAM6	Traceability and auditing	To ensure non-repudiation and traceability of subject actions performed in context of organisational resources in order to be able to trace back and investigate intentional or unintentional negatively impactions activities.	Establish, implement and maintain identity and access management measures to ensure chronological traceability and auditing capabilities in order to enable accountability of subjects performing actions on information systems and processing information. The organisation shall consider measures to ensure nonrepudiation by subjects. The organisation shall consider traceability and auditing capabilities in context of identity and access management applicable to systems, applications and networks.

Domain	Subdomain	Ref.	Control	Control objective	Control description
PROTECT AND DETECT	Identity and access management	IAM7	Identity lifecycle management	To ensure identity roles and authorisation is reflecting the subject identity lifecycle.	Establish, implement and maintain adequate identity and access management measures across the identity lifecycle, inter alia, provisioning, authentication, authorization, and de-provisioning of identities. Identity lifecycle management controls should be integrated with human resources security processes, as defined in [HRS1], in order to ensure access roles are aligned with the employment lifecycle of subjects within the organisation.
PROTECT AND DETECT	Vulnerability and Patch Management	VM1	Vulnerability scanning and identification	To ensure system vulnerabilities are known to the organisation in order to mitigate accordingly.	Establish, implement and maintain a risk-based plan and approach to test applications, systems and networks for vulnerabilities and weaknesses that could be exploited by threats. The organisation should consider vulnerability scanning identification as part of new or changed processes or systems that involve processing of information. Vulnerabilities should be scanned and identified in context of threats to confidentiality, integrity and availability of information. The organisation should consider penetration testing as a means to scan and identify vulnerabilities. The outcome of vulnerability scanning and identification efforts should be documented and reported as described in [VM2].
PROTECT AND DETECT	Vulnerability and Patch Management	VM2	Documentation and reporting of vulnerabilities	To ensure system vulnerabilities are documented and reporting accordingly in order for management to make informed decisions in mitigation.	Establish, implement and maintain processes to document and report on identified vulnerabilities in order to be able to remedy and patch systems and processes to ensure the confidentiality, integrity and availability of information. Vulnerability documentation and reporting should be the result of a vulnerability scanning and identification effort as described in [VM1]. The organisation shall consider vulnerability documentation and reporting linked to high risks to be included in general management reporting efforts in order to ensure top-down awareness about potentially impactful vulnerabilities and identify appropriate safeguards in order to remedy and patch systems and processes as described in [VM3].
PROTECT AND DETECT	Vulnerability and Patch Management	VM3	Vulnerability remediation and patching	To ensure system vulnerabilities are remediated and patched upon decision of management.	Establish, implement and maintain processes to remediate and patch vulnerabilities identified in systems, applications, and network elements that require mitigation as a result of management evaluation. Vulnerability remediation and patching should be the outcome of the management decision based on vulnerability documentation and reporting as described in [VM2].

Domain	Subdomain	Ref.	Control	Control objective	Control description
PROTECT AND DETECT	Network security	NS1	Perimeter security	To ensure the interface of the local network with the external network is protected from security attacks, threats and other intentional or unintentional potentially negatively affecting activities.	Establish, implement and maintain adequate network security controls in order to protect the network perimeter from external threats and ensure the confidentiality, integrity and availability of information residing on the internal network. The organisation should take into account that perimeter security is only one specific layer in a layered defence architecture. The organisation shall take into account organisation-specific and sector-specific threats and risks to network perimeters in order to protect from network attacks. The organisation shall take into account network firewalls and intrusion detection and prevention systems as described in [NS7]. The organisation shall take reasonable steps to ensure traffic is filtered and matched with the organisational security policies.
PROTECT AND DETECT	Network security	NS2	Network segregation and segmentation	To ensure the separation of the logical network according to business functions and avoid infection spread.	Establish, implement and maintain adequate network segregation and segmentation in order to ensure a - either logical and/or physical - separation and segregation of information networks. The organisation shall take into account functional areas of business activity when designing, implementing and maintaining network segregation and segmentation measures. The organisation shall take into account the nature and scope of data processed in context of specific business activities in order to ensure adequate segregation and segmentation. The organisation should consider the adoption of Virtual Local Area Networking technology (VLAN) when designing its segregation and segmentation architecture. The organisation should at a minimum consider segregation or segmentation of research and development, administration, IT backbone infrastructure, and public (internet) facing applications and systems.

Domain	Subdomain	Ref.	Control	Control objective	Control description
PROTECT AND DETECT	Network security	NS3	Denial of service protection	To ensure organisational resources are protected from denial of service attacks and legitimate service operations are not affected.	Establish, implement and maintain adequate denial of service, and distributed denial of service, protection measures in order to ensure timely and qualitative delivery of service to authorized and authenticated users and maintain a respectable level of productivity. The organisation should consider incorporating capabilities to identify legitimate users and applications distinguishing malicious attempts to access resources when designing denial of service protection measures. The organisation should take into account redundancy and high availability measures as described in [NS6] in order to ensure failover in the case of a threat to availability of information and services.
PROTECT AND DETECT	Network security	NS4	Secure communication protocols	To ensure communication protocols are secured accordingly in order to achieve secure communication between network resources.	Establish, implement and maintain secure protocols to facilitate communication of information between network nodes, applications and systems in order to ensure confidentiality and integrity of information in transit and prevent network attacks and deter threats such as eavesdropping and other communication interception methods. The organisation shall consider state-of-the-art communication protocols when securing information transfer and exchange by means of network communications. The organisation shall consider security measures supported by cryptographic means as defined in [AM5] in order to secure communications, taking into technology such as Hyper Text Transfer Protocol Secure (HTTPS), Internet Protocol Security (IPsec), Transport Layer Security (TLS)/Secure Sockets Layer (SSL), depending on the pursued technology layer.

Domain	Subdomain	Ref.	Control	Control objective	Control description
PROTECT AND DETECT	Network security	NS5	Network access control	To ensure access to the logical network by external and internal systems is secured accordingly so that only authorised subjects can access organisational resources.	Establish, implement and maintain network access controls to ensure logical access to the organisational network and information resources are managed and unauthorised access is prevented. The organisation should consider specific technical and organisational measures such as network access authentication mechanisms to facilitate the operations of this measure. The organisation should consider network access control for wired, wireless, and other types of connecting to the network. The organisation should consider integrating network access control with centralised credentials and identity and access management processes as defined in [IAM5].
PROTECT AND DETECT	Network security	NS6	Redundancy and high availability	To ensure availability of information and information networks by achieving adequate availability of resources, redundancy and high-availability network equipment, systems and connections.	Establish, implement and maintain adequate measures to ensure a reasonable level of redundancy and high availability, especially for critical systems, services and applications that processes classified and/or operational information. The organisation shall consider redundancy and high availability on and technology levels, inter alia, storage, communications and processing. The organisation shall take into account redundancy and high availability technology such as failover systems, redundant array of independent disks (RAID), cold, warm and hot data storage facilities.
PROTECT AND DETECT	Network security	NS7	Intrusion detection and prevention	To ensure external intrusion attempts and security attacks are detected and prevented.	Establish, implement and maintain adequate measures to detect and prevent intrusions to the organisational network and resources. The organisation should consider intrusion detection systems (IDS) and intrusion prevention systems (IPS) to mitigate the risk of external intrusion attempts. The organisation shall take into account to establish a network monitoring management console to register intrusion attempts for further analysis. The organisation shall consider integrating triggers for incident response, as defined in [EIM2], while designing the intrusion detection and prevention processes. The organisation shall consider information and event management solutions (SIEM) to support intrusion detect and prevent processes.

Domain	Subdomain	Ref.	Control	Control objective	Control description
PROTECT AND DETECT	System security	SS1	Anti-malware	To ensure malware and malicious code does not affect organisational resources.	Establish, implement and maintain adequate measures to protect systems from malware and malicious code infections in order to ensure the confidentiality, integrity, availability and authenticity of information. The organisation shall consider in scope of anti-malware controls, inter alia, operating systems, network systems and services, network equipment operating systems, user endpoints and mobile devices, and portable media devices. The organisation shall ensure anti-malware measures rely on up-to-date information in order to detect and resolve malware threats.
PROTECT AND DETECT	System security	SS2	System and device hardening, and baseline security requirements	To minimise the attack surface of information systems by reducing functionality and features to the extent possible.	Establish, implement and maintain a process to ensure hardening of systems and devices based on security baseline requirements in order to prevent unauthorised access to, and use of, system resources and services. The organisation shall consider operating systems, applications and any other software installed on devices to be in scope of the hardening process. The organisation shall consider system hardening guidelines and documentation provided by software and hardware vendors, and guidelines and best practices published by system engineering communities, regulatory authorities, and other international best practices or frameworks. The organisation shall consider, at a minimum, vendor-supplied defaults and elimination of unnecessary default accounts, ensuring single primary functions per server to prevent functions with different security levels to co-exist on the same server, enabling only necessary services, protocols, and daemons, configuring system security parameters to prevent misuse, removing all unnecessary functionalities including scripts, drivers, features and subsystems in order to minimise the system attack surface. The organisation should consider implementing endpoint firewalls in order to prevent malicious code from impact the security of information stored on the endpoint.

Domain	Subdomain	Ref.	Control	Control objective	Control description
PROTECT AND DETECT	System security	SS3	Mobile device security	To ensure mobile devices that have access to organisational resources are secured accordingly.	Establish, implement and maintain mobile device security measures in order to ensure the confidentiality, integrity, availability and authenticity of mobile systems used by subjects to connect to, interact with, or otherwise process organisational assets and resources. The organisation shall consider mobile device management, secure storage and encryption controls, as defined in [DS4], strong authentication, as defined in [IAM4], secure communications and network controls as defined in [NS4] The organisation shall ensure mobile devices, and information residing on mobile devices, are adequately protected against theft and loss. The organisation shall consider remote wiping and geolocation tracking capabilities.
PROTECT AND DETECT	System security	SS4	Application configuration management	To ensure applications used to access or otherwise process organisational resources are managed and secured accordingly.	Establish, implement and maintain application configuration management measures in order to prevent unauthorised and malicious installation, configuration or modification of applications and software on organisational assets and devices. The organisation shall consider establishing a central application configuration and management interface to ensure all organisational devices are centrally managed and configurations and software updates can be pushed to end devices. This central management interface should enable the organisation to whitelist and blacklist certain types of applications.

Domain	Subdomain	Ref.	Control	Control objective	Control description
PROTECT AND DETECT	Application security	AS1	Secure software development lifecycle	To ensure adequate security safeguards are adopted in context of software development activities performed by the organisation.	Establish, implement and maintain secure software development practices in traditional software development lifecycle processes in order to ensure security by design and by default in context of application and software development activities. The organisation shall consider to implement, at a minimum, a software risk assessment exercise at the early stage of the project, perform security testing and code review in the development stages of the project, and perform a security assessment and secure configuration exercise at the delivery stages of the project. The organisation shall ensure adequate measures are implemented to separate software development environments from operational business environments. The organisation shall ensure data used for testing purposes is anonymised and disregarded from confidential and sensitive information in context of development activities.
PROTECT AND DETECT	Human resources security	HRS1	Employment lifecycle	To ensure adequate safeguards are implemented to ensure subjects working on behalf of the organisation having access to organisational resources support the information security policy and objectives of the organisation.	Establish, implement and maintain a plan in order to ensure information security is embedded throughout the entire employment lifecycle (i.e. before, during and after employment of employees) and take all reasonable efforts in order to ensure employees understand their information security responsibilities. The plan shall include appropriate information security measures in each phase of employment, e.g. screening of subjects before hiring, training and awareness of employees, incorporation of adequate contractual safeguards in employment contracts, establishment of an acceptable use policy, return of employee devices containing critical information and removal of access to systems and applications in accordance with the identity management lifecycle as defined in [IAM7].
PROTECT AND DETECT	Human resources security	HRS2	Employee monitoring	To ensure subjects working on behalf of the organisation are compliant to the information security policy and adhere to security responsibilities throughout the employment lifecycle.	Establish, implement and maintain a plan in order to monitor compliance of employees with their information security obligations and responsibilities embedded throughout the employment lifecycle.

Domain	Subdomain	Ref.	Control	Control objective	Control description
PROTECT AND DETECT	Human resources security	HRS3	Disciplinary measures and enforcement	To ensure subjects working on behalf of the organisation are held accountable for intentional or unintentional activities that affect the information security objectives of the organisation.	Establish, implement and maintain a set of disciplinary measures in order to ensure that subjects comply with their information security obligations and responsibilities and action is taken in case there is a breach of information security obligations and responsibilities. The organisation shall consider setting up a formal enforcement and sanction process for subjects failing to comply with information security obligations and responsibilities. Non-compliance with information security obligations and responsibilities shall be detected via employee monitoring processes [HRS2].
PROTECT AND DETECT	Human resources security	HRS4	External human resources	To ensure external subjects working on behalf of the organisation are adhering to the information security policy and objectives of the organisation.	Establish, implement and maintain information security responsibilities in the relationship with external workforces e.g. contractors, in order to ensure the appropriate protection of information exchanged with external subjects.
PROTECT AND DETECT	Human resources security	HRS5	Insider threat protection	To ensure protection from threats to the security of networks and information internal to the organisation.	Establish, implement and maintain adequate measures in order to prevent, detect and monitor insider attacks from oblivious, negligent, malicious or professional insiders. The organisation shall train employees and raise awareness of information security practices within the organisation in accordance with [TA2], perform adequate screening of candidates in accordance with [HRS1] and monitor employees [HRS2] in order to reduce likelihood the occurrence of insider attacks.
PROTECT AND DETECT	Human resources security	HRS6	Employment agreements and acceptable use	To ensure information security responsibilities and acceptable use of assets are embedded in employment agreements and the onboarding processes to achieve accountability and awareness.	Establish, implement and maintain an acceptable use policy, which specifies what the organisation considers acceptable uses of information systems that are made available to subjects in order to ensure that subjects are aware of what is expected from them with regards to the use of e.g. computers, mobile devices. The organisation should consider testing awareness of the acceptable use policy. The organisation should also put in place adequate employment agreements, which clearly state the information security obligations and responsibilities of the employee.

Domain	Subdomain	Ref.	Control	Control objective	Control description
PROTECT AND DETECT	Physical security	PS1	Environmental controls	To ensure adequate safeguards are adopted in order to protect the organisation against the effects from natural disasters such as floods, earthquakes and fires.	Establish, implement and maintain appropriate safeguards in order to protect the organisation against the effects from natural disasters such as floods, earthquakes and fires. The organisation shall consider the geographical location when setting up its network infrastructure and ensure that critical components and systems should be geographically spread.
PROTECT AND DETECT	Physical security	PS2	Perimeter access controls	In order to ensure the physical perimeter of the organisation is secured and prevent unauthorised access.	Establish, implement and maintain physical security perimeters in order to protect information processing facilities. The organisation shall establish appropriate perimeter access controls by putting in place physical borders such as fences, doors, and walls. The organisation shall also require employees and visitors to identify themselves with the security guard in order to enter (a certain section of) the organisation. The organisation should consider installing surveillance cameras in order to detect intruders at the boundaries of the organisation.
PROTECT AND DETECT	Physical security	PS3	Internal access controls	To ensure access control to internal working areas and facilities are secured in order to ensure physical access is limited to a need-to-have basis.	Establish, implement and maintain internal access controls which are aligned with the roles as described in [IAM1] in order to ensure that only subjects with a legitimate interest have access to (certain parts of) the organisation, e.g. by putting in place specific badge scanners in order to access a certain part of the organisation.
PROTECT AND DETECT	Physical security	PS4	Cabling, equipment and facilities security	To ensure cabling and equipment supporting the processing of information is physically secured from interference, interception or damaged.	Establish, implement and maintain appropriate safeguards in order to protect cabling and other equipment from interference, interception or damage, which would cause downtime to the services of the organisation. The organisation shall ensure that cables supplying power to critical infrastructure are properly protected and shall train employees in compliance with [TA2] in order to make them aware of the importance of equipment supporting information processing activities. Physical access to the logical networks should also be protected by appropriate measures in order to prevent unauthorized physical access to the logical equipment and network of the organisation. The organisation shall consider adequate network access controls as defined in [NS5]. The organisation shall ensure the physical integrity and regular maintenance of the premises in which the equipment of the network is installed, as well as the proper functioning of the security measures.

Domain	Subdomain	Ref.	Control	Control objective	Control description
PROTECT AND DETECT	Physical security	PS5	Internal environmental controls	To ensure the internal areas and facilities of the organisation are protected from physical damage.	Establish, implement and maintain physical security and safety measures in order to prevent physical damage to internal areas and facilities of the organisation. When implementing internal environmental controls, the organisation should consider the risks related to fire and temperature, electricity, the use of water, and other elements that could negatively impact the physical security of assets. The organisation shall consider fire suppression, humidity controls, and other measures according to the specifics of internal physical areas such as data centres or other areas where processing equipment is located.

7.3 RESPOND

The objective of the RESPOND building block is to ensure operators of essential services and critical infrastructures are able to respond to information security events and incidents that could affect the confidentiality, integrity, availability or authenticity of information. This building block entails adoption of operational resilience and business continuity measures.

Domain	Subdomain	Ref.	Control	Control objective	Control description
RESPOND	Event and incident management	EIM1	Event and incident readiness and detection	To ensure the organisation is able to detect security events and incidents that could pose a threat to the information security objectives of the organisation and trigger incident response processes accordingly.	Establish, implement and maintain an event and incident management and response plan in order to ensure the organisation is ready to react upon a significant information security event or incident. The organisation shall consider to align its event and incident response processes with general monitoring capabilities and specific security monitoring functions such as intrusion detection and prevention services as described in [NS7].
RESPOND	Event and incident management	EIM2	Event and incident analysis and evaluation	To ensure the organisation is able to analyse and evaluate information security events and incidents in order to trigger adequate containment and recovery processes.	Establish, implement and maintain processes that allow for analysis and evaluation of events and incidents in order to be able to make informed decisions on actions to take and measures to adapt in order to recover or contaminate security events and incidents. The organisation shall consider the impact on data subjects, business operations, external parties and the ecosystem of Critical Information Infrastructures and Operators of Essential Services in general. The organisation shall ensure event and incident analysis and evaluation are performed in alignment with top-level management whereas events and incidents are linked to high risk scenarios.
RESPOND	Event and incident management	EIM3	Event and incident containment and recovery	To ensure adequate containment and recovery of security events and incidents that negatively affect the information security objectives of the organisation.	Establish, implement and maintain event and incident containment and recovery processes to ensure security events and incidents are contained and as little systems, applications, networks and data are affected, and critical operations are safeguarded to the extent possible. The organisation shall consider event and incident recovery objectives, taking into account the recovery point objective (RPO) and recovery time objective (RTO) in order to identify the targeted duration of time and a service level within which a business process must be restored after an incident.

Domain	Subdomain	Ref.	Control	Control objective	Control description
RESPOND	Event and incident management	EIM4	Post-event and post-incident activities	To ensure the organisation learns from security events and incidents in order to prevent similar events and incidents from happening in the future.	Establish, implement and maintain post-event and post-incident processes in order to capture lessons learnt from information security events and incidents and determine whether additional security measures are to be established to prevent similar events and incidents from occurring again. The organisation shall consider establishing a post-mortem procedure that includes an event and incident evaluation meeting with affected system owners, data custodians, and other relevant stakeholders that were involved in the event or incident to exchange lessons learnt and determine preventive measures.
RESPOND	Event and incident management	EIM5	Regulatory incident notification and collaboration requirements	To ensure the organisation notifies relevant stakeholders in the case of security events or incidents as described in legal and regulatory requirements.	Establish, implement and maintain processes to ensure compliance with regulatory and legislative requirements with regard to incident notification. The organisation shall ensure adequate notification and reporting processes are defined to communicate information security events and incidents to applicable regulatory authorities such as the Digital Security Authority. In the context of personal data, the organisation shall ensure compliance with relevant laws and regulations related to the protection of personal data and communicate where necessary to the appropriate data protection authority.
RESPOND	Event and incident management	EIM6	Event and incident stakeholder communication	To ensure the organisation notifies and communicates on network and information security events and incidents affecting subjects to internal and external stakeholders.	Establish, implement and maintain processes to ensure communication with respect to information security events and incidents towards external and internal stakeholders in order to ensure event and incident awareness and allow external and internal stakeholders to determine adequate reactive measures if necessary. The organisation shall consider collaborating with external and internal stakeholders with respect to event and incident containment in order to minimise the impact of an event of incident, and post-event and post-incident activities in order to determine preventive measures, such as the Digital Security Authority and emergency services.

Domain	Subdomain	Ref.	Control	Control objective	Control description
RESPOND	Business continuity and resilience	BCR1	Business impact analysis	To ensure the organisation has analysed and evaluated critical business processes to be taken into account in the business continuity plan in order to enable the organisation to restore business processes to an acceptable level as soon as possible in the occurrence of an event or incident.	Establish, implement and maintain a business impact analysis process in order to identify all critical assets within the organisation. The business impact analysis will allow the organisation to prioritize functions and systems based on necessity for the provision of operational services. The business impact analysis shall be carried out based on a classification scheme taking into account defined criticality levels and shall consider whether critical functions or systems stand on their own or are connected to another function or system in the organisation.
RESPOND	Business continuity and resilience	BCR2	Business continuity plan	To ensure the organisation has a plan to maintain continuity of critical business processes and restore during and after an event or incident.	Establish, implement and maintain a business continuity plan in order to ensure the organisation can respond to emergency situations in an immediate and appropriate manner and is able to maintain business functions by minimizing the consequences and damages resulting from an incident. The business continuity plan shall include the disaster recovery plan as described in [BCR4] and shall take into account performed business impact analyses.
RESPOND	Business continuity and resilience	BCR3	Business continuity exercises and simulations	To ensure the organisation and subjects working on behalf of the organisation are aware and informed of their responsibilities during an event or incident that triggers the business continuity plan.	Establish, implement and maintain controls to test, revise and improve the business continuity plan by performing exercises where events and incidents occurring in the organisation are simulated, in order to test the organisation's response to similar events and incidents and to improve the business continuity processes. Business continuity exercises and simulations should enable the organisation to uncover opportunities for improvement and obtain better results over time. The organisation should consider linking the business continuity plan to change management processes as described in [CM1] in order to reflect the consequences of changes within the organisation in the business continuity plan. The organisation should carry out business continuity exercises and simulations at regular intervals in order to keep employees vigilant for events and incidents that could damage the organisation. When establishing a business continuity plan, the organisation shall consider disaster recovery as defined in [BCR4].

Domain	Subdomain	Ref.	Control	Control objective	Control description
RESPOND	Business continuity and resilience	BCR4	Disaster recovery plan	To ensure the organisation has a plan to restore critical information technology (IT) systems to an acceptable service level during or after an incident.	Establish, implement and maintain a disaster recovery plan in order to ensure the restoration and recovery of all IT critical processes and supporting assets such as power supply and electricity, after the occurrence of an incident. The disaster recovery plan should incorporate clear instructions for IT personnel in order to ensure a timely and effective response to all incidents affecting the IT environment of the organisation. The disaster recovery plan should specify the recovery time objective in order to avoid unacceptable consequences to the organisation.

8. ANNEX A: INFORMATIVE REFERENCES FOR CONTROL DOMAINS

This annex provides informative references to guidance, published by public organisations such as ENISA and National Competent Authorities, which can help operators of essential services and critical information infrastructure providers to implement the information security controls contained in the NIS Cyber Security Framework.

Domain	Informative references			
	Title	**Author**	**Date of publication**	**URL**
PREPARE	Governance framework for European standardisation	ENISA	July 01, 2016	https://www.enisa.europa.eu/publications/policy-industry-research
	NCSS Good Practice Guide	ENISA	November 14, 2016	https://www.enisa.europa.eu/publications/ncss-good-practice-guide
	National Cyber Security Strategies: An Implementation Guide	ENISA	December 19, 2012	https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
	Secure ICT Procurement in Electronic Communications	ENISA	December 11, 2014	https://www.enisa.europa.eu/publications/secure-ict-procurement-in-electronic-communications
	Supply Chain Integrity: An overview of the ICT supply chain risks and challenges, and vision for the way forward	ENISA	September 11, 2015	https://www.enisa.europa.eu/publications/sci-2015
	Good Practice Guide on Training Methodologies	ENISA	November 12, 2014	https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies
	Cyber Security Culture in organisations	ENISA	February 06, 2018	https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations
	Incident notification for DSPs in the context of the NIS Directive	ENISA	February 27, 2017	https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive
	The cost of incidents affecting CIIs	ENISA	August 05, 2016	https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis
	Communication network dependencies for ICS/SCADA Systems	ENISA	February 01, 2017	https://www.enisa.europa.eu/publications/ics-scada-dependencies
	Stocktaking, Analysis and Recommendations on the protection of CIIs	ENISA	January 21, 2016	https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis
PROTECT AND DETECT	Defining and Understanding Security in the Software Development Life Cycle	SANS	/	https://software-security.sans.org/resources/paper/cissp/defining-understanding-security-software-development-life-cycle
	Secure Software Engineering Initiatives	ENISA	May 01, 2011	https://www.enisa.europa.eu/publications/secure-software-engineering-initiatives
	Asset protection	CPNI	/	https://www.cpni.gov.uk/protecting-my-asset
	Physical Security	CPNI	/	https://www.cpni.gov.uk/physical-security
	Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations	ENISA	January 18, 2016	https://www.enisa.europa.eu/publications/vulnerability-disclosure

Domain	Informative references			
	Title	**Author**	**Date of publication**	**URL**
	Effective Patch Management	ENISA	August 28, 2018	https://www.enisa.europa.eu/publications/info-notes/effective-patch-management
RESPOND	Business and IT Continuity: Overview and Implementation Principles	ENISA	February 01, 2008	https://www.enisa.europa.eu/publications/business-and-it-continuity-overview-and-implementation-principles
	Business Continuity for SMEs	ENISA	March 24, 2010	https://www.enisa.europa.eu/publications/business-continuity-for-smes
	Enabling and managing end-to-end resilience	ENISA	January 24, 2011	https://www.enisa.europa.eu/publications/end-to-end-resilience
	Strategies for incident response and cyber crisis cooperation	ENISA	August 25, 2016	https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation
	Actionable information for security incident response	ENISA	January 19, 2015	https://www.enisa.europa.eu/publications/actionable-information-for-security
	Good Practice Guide for Incident Management	ENISA	December 20, 2010	https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management
	NCSS Good Practice Guide	ENISA	November 14, 2016	https://www.enisa.europa.eu/publications/ncss-good-practice-guide

9. ANNEX B: IMPLEMENTATION GUIDANCE: ISO/IEC 27001 AND NIST SP800-53

This annex includes references to implementation guidance per control as described in section 6 of this document. The implementation guidance in the table below refers to two international standards: ISO/IEC 27001 and NIST SP800-53 Rev. 4.

Ref.	Control	ISO/IEC 27001	NIST SP800-53 Rev. 4
AM1	Asset lifecycle management	A.8	CM-8, PL-4, PS-4, PS-5, RA-2, MP-2, MP-3, MP-4, MP-5, MP-6, MP7, PE-16, PE-18, PE-20, SC-8, SC-28
AM2	Inventory of assets and ownership	A.8.1.1, A.8.1.2	CM-8
AM3	Asset monitoring	A.12.4	PE-20
AM4	Availability management	A.11.2.4, A.17.2	SC-5, SC-36
AM5	Cryptographic controls	§10, A.18.1.5	SC-12, SC-13
AM6	Capacity management	A.12.1.3	AU-4, CP-2, SC-5
AS1	Secure software development lifecycle	A.14.2	SA-8, SA-10, SA-11
BCR1	Business impact analysis	A.16.1.1, A.17.1.1, A.17.1.2	RA-2, RA-3, PM-9
BCR2	Business continuity plan	A.16.1.1, A.17.1.1, A.17.1.2	CP-2, CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13, IR-8
BCR3	Business continuity exercises and simulations	A.17.1.3	CP-4, IR-2, IR-3, PM-14
BCR4	Disaster recovery plan	A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3	CP-2, IR-8, CP-4, IR-3, PM-14
CM1	Change management	A.12.1.2	CM-3, CM-5, SA-10
CM2	Configuration management	A.5.1.1, A.5.1.2, A.6.1.1, A.8.1.1, A.8.1.2, A.9.2.3, A.9.4.5, A.12.1.1, A.12.1.2, A.12.1.4, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4, A.18.1.1, A.18.1.2; A.18.2.2	CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-8, CM-9, CM-10, CM-11
DS1	Information lifecycle management	§8.1, A.8.1, A.8.2, A.8.3	SA-1, SA-3, SA-4, SA-5, SA-8, SA-9, SA-11, SA-12, MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8
DS2	Classification and labelling of information	A.8.2	SC-28, SE-1, AC-16
DS3	Backup and data recovery	A.12.1, A.12.3	CP-1, CP-2, CP-3, CP-4, CP-5, CP-6, CP-7, CP-9, CP-10, CP-11
DS4	Information transfers and exchange	A.13.2	AC-4, AC-17, AC-18, AC-19, AC-20, CA-3, PE-17, SC-7, SC-8, SC-15, CA-3, PS-6, SA-9, SC-8, PS-6
DS5	Data loss and data leakage prevention	A.8.3.1	MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8
EIM1	Event and incident readiness and detection	A.12.4.1, A.16.1.1, A.16.1.3., A.16.1.4	IR-1, IR-3, IR-4, IR-8, AC-2, AU-12, CA-7, CM-3, SC-7, AU-3, AU-6, AU-11, AU-12, AU-14
EIM2	Event and incident analysis and evaluation	A.16.1.4	AU-6, IR-4
EIM3	Event and incident containment and recovery	A.16.1.5	IR-4, IR-9

Ref.	Control	ISO/IEC 27001	NIST SP800-53 Rev. 4
EIM4	Post-event and post-incident activities	A.16.1.6, A.16.1.7	IR-4, AU-4, AU-9, AU-10(3), AU-11
EIM5	Regulatory incident notification and collaboration requirements	A.18.1.1, A.18.1.4	IR-1
EIM6	Event and incident stakeholder communication	A.16.1.2, A.16.1.3	AU-6, IR-6, IR-7
GOV1	Information security roles and responsibilities	§5.3, A.6.1	PL-1, PL-4
GOV2	Compliance with legal and regulatory requirements	§4.2, A.6.1.3, A.18.1	AR-2, AU-6, AU-11
GOV3	Information security policies, standards, guidelines and procedures	§5.2, A.5.1	
HRS1	Employment lifecycle	A.7	PS-1, PS-2, PS-5
HRS2	Employee monitoring	A.12.4	PS-8
HRS3	Disciplinary measures and enforcement	A.12.4	PS-8
HRS4	External human resources	A.15.2	PS-7
HRS5	Insider threat protection	A.7, A.12.4	PS-1, PS-2, PS-5, PS-8
HRS6	Employment agreements and acceptable use	A.8.1.3	PS-6
IAM1	Role based access control	A.9.1.1	AT-3, AC-2, AC-3, AT-3
IAM2	External access controls	A.9.1.2, A.13.2.	SA-9, AC-20, CA-2, CA-3, CP-2
IAM3	Privileged users management	A.9.1.1, A.9.2.3.	AT-3, AC-2, AC-3, AT-3
IAM4	Strong authentication	A.9.1.2	AC-3, AC-5, AC-6
IAM5	Credential management		IA-5, IA-6, IA-9, IA-10, IA-11
IAM6	Traceability and auditing	A.12.7	AU-1, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-9, AU-10, AU-11, AU-12, AU-13, AU-14, AU-15, AU-16
IAM7	Identity lifecycle management	A.9.1, A.9.3	AC-6, AC-13, AC-24
NS1	Perimeter security	A.13.1.1, A.13.1.2	SC-5, SC-7, SC-30, SI-8, AC-4, CA-3
NS2	Network segregation and segmentation	A.13.1.3	SC-3, SC-44, SC-37, PM-7
NS3	Denial of service protection	A.13.1.1, A.13.1.2	SC-5, SC-30, SI-8, AC-4, CA-3
NS4	Secure communication protocols	A.13	SC-8, SC-9, SC-10, SC-11, SC-12, SC-13
NS5	Network access control	A.13.1.1, A.13.1.2	SC-14, AC-1, AC-18, AC-24
NS6	Redundancy and high availability	A.11.2.4, A.17.2	SC-5, SC-36
NS7	Intrusion detection and prevention	A.13.1.2	IR-4, IR-10, SC-28, SI-4, SI-5
PS1	Environmental controls	A.11.1.4, A.11.2.1, A.11.2.2	PE-1, PE-13, PE-14, PE-15, PE-18
PS2	Perimeter access controls	A.11.1.1, A.11.1.2, A.11.1.3	PE-3, PE-6
PS3	Internal access controls	A.11.1.1, A.11.1.2, A.11.1.3	PE-2, PE-3, PE-6

Ref.	Control	ISO/IEC 27001	NIST SP800-53 Rev. 4
PS4	Cabling, equipment and facilities security	A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3, A.11.2.4, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8	PE-9, PE-10, PE-11, PE-12
PS5	Internal environmental controls	A.11.1.3, A.11.1.5	PE-3, PE-5
RM1	Methodology		PM-8, PM-9, PM-11, SA-14
RM2	Context	§4	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5, PM-15, PM-16
RM3	Risk Identification		RA-3, SI-5, PM-12, PM-16
RM4	Risk Analysis	§6.1, §6.2	RA-1, RA-2, RA-3, RA-4, RA-5, RA-6
RM5	Risk Evaluation	§6.1, §6.2	RA-1, RA-2, RA-3, RA-4, RA-5, RA-6
RM6	RiskTreatment	§6.1, §6.2	RA-1, RA-2, RA-3, RA-4, RA-5, RA-6
SS1	Anti-malware	A.12.2.1	SI-3
SS2	System and device hardening, and baseline security requirements	A.12.1, A.12.5, A.12.6	CM-1, CM-2, CM-3, CM-4, CM-6
SS3	Mobile device security	A.6.2.1, A.11.2.6, A.13.2.1	SC-8, SC-42, SC-43, SI-3, AC-17, AC-18, AC-19
SS4	Application configuration management	A.12.1, A.12..4.1	CM-3, CM-5, SA-10, SI-2
STR1	Information security strategy		PL-1, PL-2, PL-8, PL-9
TA1	Information security awareness program	§7.3, A.7.2.2	AT-1, AT-2, AT-3, AT-4, AT-5
TA2	Information security awareness, education and training	§7.3, A.7.2.2	AT-1, AT-2, AT-3, AT-4, AT-5
TPS1	Third party and suppliers due diligence	A.15	PS-7, SA-9, SA-12, , AU-16, AC-17, IA-8
TPS2	Third party and supplier relationships	A.15	PS-7, SA-9, SA-12, , AU-16, AC-17, IA-8
VM1	Vulnerability scanning and identification	A.12.6	RA-5, SA-22, SI-2
VM2	Documentation and reporting of vulnerabilities	A.12.6	
VM3	Vulnerability remediation and patching		RA-5, SA-22, SI-2

10. ANNEX G: GLOSSARY

This annex provides definitions for the key terms used in this security measures framework. The definitions can be used as a basis for the definitions to be included in the general provisions of the legislation.

Term	Description
Asset	An asset constitutes any resource that can be valuable for an organisation.
Attack surface	The collection of different points such as components, software or vulnerabilities (in a computing device or network) where an unauthorised or unauthenticated user can enter or extract data from an environment.
Authentication	The process of confirming a claimed characteristic of a user, device or other entity.
Availability	Ensuring that information or services are accessible when an authorized entity requires access.
Confidentiality	Ensuring that information is not accessible to unauthorised users, processes or other entities.
Credential	Evidence used for validating or authenticating an identity.
Cryptography	Set of techniques for transforming data in order to hide its contents and prevent unauthorised modification or use.
Data leakage	The (un)intentional exposure of secured information to an untrusted destination or recipient.
Data loss	Event that leads to data being compromised, destroyed or stolen.
Denial of Service	The intentional obstruction of access to services or resources.
Due diligence	The investigation of a process, person or business.
Event	Manifestation or shift of a certain set of circumstances.
Firewall	A system that creates a barrier between different networks, which restricts and monitors traffic coming in from an untrusted network to a trusted network in order to protect the trusted network against various threats.
Hardening	Reducing the vulnerability surface of a system to improve security.
Incident	An event that has a potential or actual negative impact on the confidentiality, integrity or availability of a system.
Integrity	Integrity ensures the consistency, accuracy, and trustworthiness of data.
Malware	Software that can perform an unauthorized process that has a negative impact on the integrity, availability or confidentiality of a resource. Examples include, but are not limited to, ransomware, virus, worm and spyware.
Patching	A set of changes made to software in order to fix bugs, weaknesses or vulnerabilities and enhance the performance of that software.
Network perimeter	Boundary between the private/local part of a network and the public/provider part of a network or the internet.
Risk	A risk is the likelihood of a threat exploiting a vulnerability resulting in an impact.
Threat	An event which could negatively impact an asset.
Traffic Light Protocol	Classification scheme defined by the FIRST.Org as a standard for information classification.
Vulnerability	Weakness or error in an information system that could be exploited by a threat in order to compromise the security of the information system.
Risk identification	Procedure of finding, listing and describing risks.
Risk analysis	Process of understanding the risk and determining the corresponding risk level.
Risk evaluation	Process of comparing the outcome of the risk analysis to defined risk criteria in order to assess which risks are tolerable.
Risk treatment	Process of modifying the risk by lowering the likelihood or impact of the risk.

11. ANNEX H: NIS COOPERATION GROUP REFERENCE DOCUMENT

The table below demonstrates that all security controls as described in the NIS Cooperation Group reference document[1] are also covered in this security measures framework.

NIS Cooperation Group Reference Document	NIS Measures Framework
1. Governance and ecosystem	
1.1. Information System Security Governance & Risk Management	
Information system security risk analysis	RM4
Information system security policy	GOV1; GOV3
Information system security accreditation	RM2, RM3, RM4
Information system security indicators	STR1
Information system security audit	GOV3
Human resource security	HRS1, HRS2, HRS3, HRS4, HRS5, HRS6
1.2. Ecosystem Management	
Ecosystem mapping	TPS2
Ecosystem relations	TPS1
2. Protection	
2.1. IT Security Architecture	
Systems configuration	SS2
System segregation	NS2, SS2
Traffic filtering	NS1
Cryptography	AM5
2.2. IT Security Administration	
Administration accounts	GOV1, IAM1, IAM3
Administration information systems	GOV1, IAM1
2.3. Identity and Access Management	
Authentication and identification	IAM1, IAM4, IAM5
Access rights	IAM2, IAM3
2.4. IT Security Maintenance	
IT security maintenance procedure	AM5, IAM2, SS1
Industrial control systems	STR1, GOV2
2.5. Physical and Environmental Security	PS1, PS2, PS3, PS4, PS5
3. Defense	
3.1. Detection	
Detection	EIM1
Logging	AM3
Logs correlation and analysis	AM3
3.2. Computer Security Incident Management	
Information system security incident response	EIM1, EIM2, EIM3
Incident report	EIM5
Communication with competent authorities	EIM6
4. Resilience	
4.1. Continuity of operations	
Business continuity management	BCR1, BCR2, BCR3
Disaster recovery management	BCR4
4.2. Crisis management	
Crisis management organization	GOV3, BCR2
Crisis management process	GOV3, BCR2

[1] NIS Cooperation Group, Reference document on security measures for Operators of Essential Services, February 2018, https://circabc.europa.eu/sd/a/c5748d89-82a9-4a40-bd51-44292329ed99/reference_document_security_measures_OES.pdf.