P.I. 389/2020

THE SECURITY OF NETWORKS AND INFORMATION SYSTEMS LAW ,2020

Decision under sections 17(q), 17(r), 17(s), 17(v), 17(x), 19(1)(b), 19(1)(c), 20(1)(a), 20(1)(b), 20(1)(c), 46(1), 46(4) and 46(5)

89(**I**)/2020.	(a) In the exercise of its powers under sections 17(q), 17(r), 17(s), 17(v), 17(x), 19(1)(b), 19(1)(c), 20(1)(a), 20(1)(b), 20(1)(c), 46(1), 46(4) and 46(5) of the Security of Networks and Information Systems Law of 2020, and (b) taking into account Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016, the Digital Security Authority (hereinafter the ‘’Authority**”**), issues the following Decision establishing the framework of minimum measures for the security of networks and information systems and with a view of assisting Operators of Essential Services and Operators of Critical Information Infrastructures in Cyprus to comply with the requirements and obligations set out by the Law and Directive (EU) 2016/1148.
Short title.	1**.** This Decision may be cited as the Security of Networks and Information Systems (Security Measures of Operators of Essential Services and Operators of Critical Information Infrastructure) Decision, 2020.
	PART I **Introductory Provisions**
Interpretation. Recommendation 2003/361/EC.	**2**. (1) In this Decision, unless the context otherwise requires: «Authority» means the Digital Security Authority; «Small Organisation» means an organisation of enterprise which has the characteristics of a small enterprise defined by the Commission’s Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (Recommendation 2003/361/EC);

89(I)/2020.	"Law" means the Security of Networks and Information Systems Law ,2020 and includes any Law amending or substituted for the same; «essential service» means any service that is essential in order to ensure the operation of critical sectors of social and economic activity, including essential services and services provided by operators of critical information infrastructure; «operator» means an operator of essential services or an operator of critical information infrastructure, as defined by the Law. (2) Unless the context otherwise requires, the terms used in this Decision shall have the meaning assigned to them by the Law.
Scope of Application.	**3.** This Decision concerns the definition of the minimum requirements and obligations concerning the security of network and information systems that the operators must comply with.
Purpose.	**4**. The purpose of the regulatory obligations imposed on operators is to strengthen the security and resilience of their infrastructure and services, to deal with incidents of security breaches and to ensure the operational continuity of their networks, information systems and services in the event of catastrophic damage or in case of force- majeure.
	PART II **General conditions and obligations of operators of essential services and of operators of critical information infrastructure**
General condition.	**5.** All licensed operators must take the necessary measures to ensure the proper and efficient operation of their network in the event of damage and/or changes to normal operating levels, due to natural causes or malicious actions.
Obligations of operators.	**6.** Each operator must comply with the following obligations:

	(1) To carry out on an annual basis a risk assessment of networks, information systems and essential services in order to identify significant weaknesses and vulnerabilities in its network infrastructure, in accordance with the provisions of Part III of this Decision. The operator shall have an obligation to submit information to the Authority on the risk assessment that it carries out as set out in section 13, with a view of informing the Authority.
	(2) (a) To prepare business continuity plans in accordance with the provisions of Part IV of this Decision, which must be based on the outcome of the risk assessment, which it has carried out for its network and its services.
	(b) In particular, in the case of extraordinary circumstances, catastrophic damage and force majeure, it shall have an obligation to draw up and notify the Authority of a disaster recovery plan which sets out in detail the recovery measures to be taken. (3) To implement a Security Management System/Framework and to take appropriate and proportionate technical and organizational measures, in accordance with the provisions of Part V of this Decision, in order to manage risks, to prevent and minimize the impact of incidents, and in order to ensure the continuity of its services, regarding the security of the networks and information systems that it uses for its activities.
	(4) To monitor continuously and in real-time the state of the components/equipment of its networks, information systems and essential services in terms of their operational capability and the possible damages that may occur during the operation of the equipment. Operators must also maintain staff working on a shift basis and/or which is on standby in order to be able to immediately respond to potential damage which are likely to affect the services which are provided, outside of established working hours.

(5) To ensure the operational integrity of its network by ensuring that equipment is reliable, safe against external threats (e.g. malicious attacks) and capable of operation when downgraded, even in the event of partial damage, subject to force majeure. When designing and selecting their network architecture, operators should take into account any issues of redundancy and physical security of their equipment.

(6) To have available or to ensure the availability of suitable and sufficient spare parts of equipment and to maintain suitably qualified personnel so that in the event of faults affecting the functionality of the network, they can restore the operation of the network and the services provided on a twenty-four-hour basis.

(7) To comply with the standards or specifications established at Community level, which are characterized as mandatory and which have been published in a list of standards or specifications in the Official Journal of the European Communities, and/or national standards, where applicable.

PART III
Risk Assessment

Risk Assessment.

7. (1) Taking into account the development of technology, the cost of implementation and the variable impact and probability of the occurrence of risks related to the confidentiality, integrity, the lability and authenticity of the information, the operator shall establish, implement and maintain appropriate technical and organizational measures in order to ensure a level of security which is commensurate with the risk. The operator shall implement the information security measures with the aim of reducing risk to an acceptable level and ensuring that the risks are adequately addressed, unless the security measures are inadequate in relation to the specific status of the organization based on, inter alia, the risk management procedures that it applies. If the organization considers that its security measures are inadequate, or if it has to take into account additional obligations (e.g. under another legal framework), the organization must then decide how to appropriately address the risks that it has identified. The risk assessment framework is set out in Annex I.

(2) As part of the measures taken to protect their network, operators shall have an obligation to carry out a risk assessment at regular intervals and at least on an annual basis.

(3) In order to assess the appropriate level of security, the organization must establish, implement and maintain a process for managing information security risks, including, as appropriate:

(a) the identification of the organizational framework, including the criteria for assessing and mitigating information security risks, the roles and responsibilities, the risk owners, the criteria for analysing the risk for the impact and the probability of risk, the scales for rating the risk, the risk assessment criteria, and the policies for risk-taking and risk tolerance,

(b) the identification of information security risks, by taking into account the various threats, threat scenarios and vulnerabilities concerning the confidentiality, integrity, availability and authenticity of information,

(c) the analysis of the risks regarding the security of information, by taking into account the risk assessment criteria in relation to the impact and probability of the risk, as well as other relevant criteria for identifying the risk score,

(d) the assessment of information security risks, by taking into account the risk assessment criteria and the risk-taking policy, for the purpose of determining the appropriate risk management strategies,

(e) addressing information security risks, by taking into account, inter alia, the retention / acceptance of risks, the risk transfer, the risk avoidance, or the reduction of risk.

(4) When assessing the appropriate level of security, particular consideration must be given to risks that arise from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to the information that is transmitted, stored or processed in another manner.

	(5) When assessing the appropriate level of security, particular consideration must be given to risks which could potentially affect essential economic and social functions and services which are provided by the operator. (6) The outcome of the risk assessment shall be communicated to the Authority in accordance with the provisions of section 6(1). The Authority has the right to access the risk management procedure and the risk response plan that is drawn up by the operator. If the Authority considers that the risk management process and risk response plan do not adequately address the risks identified by the operator, the Authority has the power to impose or agree corrective measures/actions on the operator.
	PART IV **Business Continuity and Emergency Response**
Preparation of a Business Continuity Plan.	**8**. Operators must draw up a business continuity plan, which aims to ensure the uninterrupted/unhindered operation of their networks, information systems and the services that they provide. The plan shall be drawn up after carrying out the risk assessment and on the basis of the findings/outcome of the risk assessment. It shall contain a description of the measures taken by the operator to restore the operation of its network components and restore its services and information. The minimum content of the business continuity plan is described in Annex II.
Preparation of a Disaster Recovery Plan.	**9.** Operators shall have an obligation to draw up a Disaster Recovery Plan, in the context of which the necessary actions aimed at maintaining the availability of the services provided and maintaining the highest possible level of service in order to respond to the requirements of any public authority shall be recorded in case of catastrophic damage or force majeure. The Disaster Recovery Plan should be reviewed on the basis of established procedures by the personnel of the provider which is responsible for the preparation and the necessary revision of the Plan. The minimum content of the disaster recovery plan is described in Annex II.

Checks.	**10.** Operators must check the effectiveness of the Business Continuity Plan and the Disaster Recovery Plan systematically and at least on an annual basis. Operators must have available recorded procedures on the basis of which the specific checks are carried out. The frequency and scope of the checks shall be determined by the risks that have been identified and the security measures which are in place.
	PART V **System Implementation /Security Management Framework - Implementation of Technical and Organizational Measures**
Implementation of a Framework for Security Measures.	**11**. (1) Operators must implement as a minimum the Framework of Security Measures published by the Authority and which establishes the measures, the preparation (prepare), the protection and detection (protect and detect) and response (respond), with the aim of establishing, implementing and maintaining a multi-layered defence approach for maintaining the confidentiality, integrity, availability, authenticity and resilience of the network and information systems and the services provided. The framework of the minimum technical and organizational measures is described in Annex III. (2) Operators must implement appropriate preparedness measures ensuring that they take into account the risk to the security of information in their day-to-day operations and ensure the commitments of top-level management in addressing security threats, vulnerabilities and risks in accordance with Part 1.1 of Annex III.
	(3) Operators must implement appropriate protection and detection measures by ensuring that they establish, implement and maintain adequate information security measures which are appropriate to their exposure to risk. As a minimum, technological, administrative and physical

	prevention, detection and response measures must be taken in accordance with Part 1.2 of Annex III. (4) Operators must implement appropriate response measures ensuring that they are able to respond to incidents and occurrences that may affect the confidentiality, integrity, availability or authenticity of information. As a minimum, measures must be taken to ensure business resilience and business continuity and disaster recovery, as well as their return to their normal operations in accordance with Part 1.3 of Annex III.
Officer in charge of the security of networks and information systems.	**12.** (1) For the purpose of implementing the Framework, it is required to allocate roles and responsibilities for the security of networks and information systems within the organization. (2) The operator shall have an obligation to appoint a network and information systems security officer, whereby: **(a)** the network and information security officer shall be appointed on the basis of professional qualifications and in particular on the basis of specific knowledge in the field of network and information security and the ability to fulfil the duties referred to in subsection (3); **(b)** the network and information security officer must solely perform these duties. For small organizations, the network and information security officer may perform other duties only when they do not lead to a conflict of interest and taking into account the critical level of the organization, subject to the approval of the Authority, **(c)** the operator shall communicate the contact details of the network and information security officer to the Authority, **(d)** the operator shall ensure that candidates for the position of network and information security officer are adequately screened in order to ensure that the person concerned will carry out his/her duties properly.

Minimum responsibilities.

(3) The network and information security officer designated by the operator shall have at least the following duties:

(a) inform and advise the operator and the employees who have access to its network and information systems about their obligations under this framework;

(b) monitor compliance with the present framework, with other national or European information security provisions, as well as with the operator's policies in relation to the security of networks and information systems;

(c) provide advice on the management of information security and monitor its performance in accordance with Part III concerning risk management.

(d) cooperate and act as a single point of contact with the Authority on matters related to the activities of the Authority within the scope of its competencies, inter alia by providing support to external audit activities, by providing documents and information in advance to the Authority, as referred to in section 13.

(e) provide reports on the threats to information, on vulnerabilities and risks to the

(f) senior management through formal and regular reports.

Position of the network and information systems security officer.

(4) Every operator shall ensure that the network and information security officer participates properly and in a timely manner in all matters related to the security of networks and information systems-

(a) The operator shall support the network and information security officer in the performance of his duties, as referred to in subsection 3.

(b) The operator shall ensure that the network and information security officer does not receive instructions that conflict with the exercise of his duties. He shall not be fired or punished by the operator for the proper performance of his duties.

(c) The network and information security officer shall report directly to the highest administrative level of the operator in terms of his duties which are prescribed by this Decision.

(d) The network and information security officer shall be bound by rules of confidentiality and professional secrecy in the performance of his duties.

(e) The operator shall ensure that the security officer has access to the necessary financial and human resources, procedures and technical and organizational measures, in order to be in a position to perform his tasks and to properly support the operator in matters of network and information system security for compliance with the obligations prescribed by the Authority.

(f) The operator shall ensure that the security officer has the appropriate knowledge, training and experience which are consistent with his duties and that the security officer regularly updates his knowledge. The Authority may provide guidance on matters related to the appropriate training and experience of the security officer.

Recording and provision of Information.

13.(1) For the implementation of this decision, operators shall have an obligation to record all relevant information in relation to the management of information security risks and to provide the said information to the Authority on an annual basis and/or upon request, in order to achieve the information security objectives required by this Framework.

(2) Every operator must be in a position and shall have an obligation to provide the following information to the Authority, in order to prove its compliance with its obligations under this Framework:

(a) The risk management methodology, including the risk assessment criteria for the impacts and probability, the risk rating scales, the risk assessment criteria and the risk-taking policy / risk tolerance, in accordance with Part III of this Decision,

(b) The risk assessment, including the identification, analysis and assessment of all information security risks within the organization, in accordance with Part III of this Decision,

(c) The risk register, which provides an overview of the risk analysis and risk assessment of all information security risks identified within the organization;

(d) The risk response plan, which identifies the remediation measures for all risks that have been identified within the organisation regarding information security, i.e. the risk retention / risk acceptance, the risk transfer, the risk avoidance or the risk reduction, in accordance with Part III of this Decision,

(e) The governance structure, including the internal network and information security roles and the responsibilities in accordance with Article 12 regarding the information security officer;

(f) The security policy and information security strategy;

(g) The implementation plan for the measures for network and information security, which provides for a mechanism for monitoring implementation at operational level;

(h) The business continuity plan,

(i) The disaster recovery plan.

PART VI
Provision of information and implementation of this Decision

Provision of information to affected parties and consumers.

14.(1) Operators must inform all those affected, including consumers where applicable in relation to incidents that threaten and/or affect the operation of the network, of the information systems and/or the provision of services by them on the basis of clear procedures that they have recorded. Provided that affected parties may also include operators of essential services and/or operators of critical information infrastructure following the suggestion or consent of the Authority.

(2) The relevant announcement on catastrophic incidents or threats or events which are expected to adversely affect networks, information systems and essential services as well as the services provided should be communicated to the mass media. Indicative ways of informing consumers include the posting of a relevant announcement on the website of providers and sending messages by e-mail.

(3) In the context of the announcement, operators must inform all affected persons, including consumers where applicable, at least on the extent of the event, the possible effects, the measures taken by the operator to handle, the estimated time for the restoration of the service and must advise consumers, where applicable.

Informing the Authority. P.I. 218/2019.	15.(1) Operators must inform the Authority of the risks which threaten or affect the operation of the network, the integrity, confidentiality, authenticity and availability of information on their network and the provision of services, in accordance with the procedure and the form prescribed by the Decision regarding the obligation of operators of essential services and/or operators of critical information infrastructure and/or digital service providers, to notify any event which has a serious impact on the continuation of the services that they provide. (2) Operators should share the contact information of an authorized representative with whom the Authority will communicate on matters concerning the compliance of operators with the provisions of this Decision. Operators must notify the Authority of any amendment of the contact details of the authorized person.
	PART VIII **Control and consultations**
Control and evaluation of information.	**16.**(1) Without prejudice to the general powers and duties of control/investigation that the Authority has according to the legislation in force and in particular sections 17(q)(r)(s) and 20(1)(a) of the Law and the Decisions issued thereunder, the Authority may, at its discretion, monitor the correct execution of the obligations arising from this Decision and the relevant annexes, as well as the accuracy of the information provided to it in accordance with this Decision.
	(2) In the event that the control provided by subparagraph (1) which is carried out by the Authority requires a contract for the provision of services with technical consultants or other persons, the Authority shall take reasonable measures to ensure their independence as well as the observance of confidentiality and impartiality by them.

(3) In order to exercise its powers, the Authority may carry out an investigation in accordance with section 23 of the Law and impose corrective measures, having the power to:

(a) Instruct an operator to provide it with all the relevant documents in accordance with section 13.

(b) Issue guidelines and binding instructions to operators regarding the provision of documents and information to be given to the Authority and their format.

(c) Carry out information security audits in order to assess whether the operator complies with its obligations, as described in this Framework.

(d) Issue guidelines and binding instructions regarding operators who do not fulfil their obligations in accordance with this Framework.

In addition, the Authority shall have the power to issue official opinions and guidelines in order to assist operators in the implementation of specific measures set out in the Annexes of this Decision.

(e) obligations in accordance with this Framework.

In addition, the Authority shall have the power to issue official opinions and guidelines in order to assist operators in the implementation of specific measures set out in the Annexes of this Decision.

Public consultations.	**17.**(1) Without prejudice to the general duties and powers of the Authority and the procedures it prescribes in relation to public consultations and the Decisions issued under the Law, the Authority may hold consultations if it deems necessary with the interested parties on a case by case basis in relation to network and information systems security issues. (2) The subject matter of the consultations referred to in subparagraph (1) shall be determined by the Authority and may concern, inter alia: (a) the exchange of opinions on the need to preserve or adapt this Decision and its annexes, in view of the experience in their practical application and the relevant developments in the services provided, the relevant specifications and the market needs, (b) the determination of voluntary procedures, definitions and methods in the event that these components are not specified in the provisions of this Decision or its Annexes, (c) any procedural or other matter that may arise in the practical implementation of this Decision.
Making additions and amendments to the Annexes.	**18.**(1) The Authority may, by decision of the Commissioner, add annexes to the present Decision or amend the content of the annexes by means of amending decisions. (2) Before issuing a Decision pursuant to subsection (1) of this section, the Authority shall follow the procedure for carrying out a Public Consultation, on the basis of the relevant legislative provisions.
	PART IX **Compliance – penalties**
Breach of obligation.	**19**.(1) If an operator breaches an obligation arising from this Decision, the Commissioner shall communicate a Decision thereto which shall contain at least the following:

(a) A description of the identified infringement;

(b) A deadline for compliance and/or for defining a relevant action plan, as prescribed at the discretion of the Authority and which cannot be longer than six (6) months; and

(c) Deadlines for the voluntary submission of comments, for filing a request for hearing and/or for filing a request for extending the deadline by the concerned provider, in accordance with the respective Regulations/**Order**/Decision on the collection of information and the imposition of an administrative fine.

(2) In exceptional cases, following a reasoned request by the operator concerned and if it is objectively justified, the Authority may grant an extension of the deadline for compliance.

Administrative fine.

20. Pursuant to subsection (z) of section 17 of the Law and without prejudice to the other sanctions that the Law and the Decisions issued thereunder may prescribe, the Authority may impose an administrative fine pursuant to section 43 of the Law or any other Law amending or substituted for the same on any operator that breaches any of its obligations as set out in this Decision.

PART X
Final Provisions

Entry into force.

21. (1) This Decision shall enter into force from the date of its publication in the Official Gazette of the Republic.

Operators must comply with the following timetable of actions:

(a) Until the 31st of December 2020

- Send a report to the Authority setting out the present security status of the networks and information systems to the operator
  - The operator shall have an obligation to inform the Authority, in summary, of the security program that if follows on the said date, with

reference to the provisions of this Decision that the operator is already complying with. Taking also into account section 13 of this Decision, the operator shall also inform the Authority of the documents and information which are already available, where applicable.

- For the purpose of setting out the existing situation in a uniform manner, the Authority may provide a standard document with specific fields.

(b) Until the 31st of December 2021

○ Submission of documents and information in accordance with the requirements of section 13 of this Decision

- The operator should submit all the prescribed documents to the Authority for assessment by taking into account the requirements of section 13 of this Decision. The Authority may request additional information and, if deemed necessary, may request amendments and improvements. As set out in paragraphs 13(2)(d) and 13(2)(g), the documents should be accompanied by a detailed program for the implementation of the necessary security measures for mitigating the risks that have been identified to acceptable levels.
- The documents will be submitted electronically on a specific platform that may be set up by the Authority for this purpose.

(c) Until the 31st of December 2022

○ Completion of the implementation and application of the security measures that address the highest risks that have been identified in terms of their criticality

- The operator should ensure that as many measures needed and/or more measures (from the list of measures included in the Cyber Security Framework) are implemented and applied in order to reduce the highest risks that have been identified in terms of their criticality to acceptable levels.

	○ Program for the implementation of the entire Framework • The operator should submit an updated statement of risks, which should show the implementation of the measures for the highest risks and prescribed the implementation program for the entire Framework for reducing the remaining risks to acceptable levels. (d) Until the 31st of December 2023 and thereafter on an annual basis ○ Completion of the implementation of the rest of the Framework • The operator should ensure that the entire Framework is implemented, and submit an updated statement of risks, showing their implementation and the consequent mitigation of the risks that have been identified to acceptable levels. ○ Submission of documents and information in accordance with the requirements of section 13 of this Decision • The operator should submit all the prescribed documents by taking into account the requirements of section 13 of this Decision, to the Authority for evaluation, which should be updated for the new year and continue the cycle of implementation of the Framework. • The documents will be submitted electronically on a specific platform that will be set up for this purpose by the Authority. Provided that the Authority will carry out supervisory checks and compliance audits in order to confirm the implementation of the Framework and of the other obligations arising under the Legislation, on the basis of prioritization outcomes from the level of criticality of each operator, from the level of risks that have been identified, and in case of significant changes in the environment of the operators or in cyberspace in general. In exceptional cases, following a reasoned request by the operator concerned and if this is objectively justified, the Authority may accept an appropriate adjustment of the compliance deadlines in each individual case.

ANNEX I: RISK ASSESSMENT FRAMEWORK

(1) Operators should take into account and assess all factors (indicatively, network components, facilities, staff) which are related to and can affect the integrity of the network and the availability of services, in accordance with all security measures under the "Risk Management" category referred to in Annex III.

(2) As a best practice, operators are encouraged to set out criteria/parameters on the basis of which their network components are prioritized in terms of their criticality/importance with respect to their role in supporting their essential services. The prioritization of the importance of the parts of the network significantly affects the adoption of corrective measures.

(3) On the basis of the aforementioned criteria, operators shall determine the critical parts/components of the network, damage to which may have a significant impact on the confidentiality, integrity, availability and authenticity of networks, information systems and essential services.

(4) Operators should consider both endogenous risks, which depend on the level of the internal reliability and resilience of the network, and external threats, such as weather conditions, natural disasters, accidents and acts of sabotage. They should also consider risks that may potentially emanate from other interconnected networks.

(5) Operators should assess the likelihood of the risks occurring, they should assess their impact on the smooth operation of the network and the services provided, seriously taking into account the inherent weaknesses of the network. Operators must apply the necessary measures and controls in order to deal with the risks that they have identified in the context of the risk assessment exercise.

(6) Operators should identify ways to evaluate the effectiveness of the measures that they observe and apply procedures for evaluating the effectiveness of the measures applied.

(7) Operators should review the risk assessment at regular intervals by taking into account a) the effectiveness of the measures which are implemented, b) the recognition of new threats, c) the organizational or technological changes and d) other events that could set new data which they must take into account.

(8) The Authority may prescribe additional information that should be included in the risk assessment, in order to facilitate the carrying out of national risk assessments as well as for the purposes of the automated processing of information.

ANNEX II: BUSINESS CONTINUITY PLAN AND DISASTER RECOVERY PLAN

The business continuity and disaster recovery plan of every operator should include the following (in accordance with all security measures under the “Business Continuity and Resilience” category set out in Annex III):

(1) Identification of the personnel involved where the business continuity of networks, information systems and essential services is threatened, their role and their responsibilities.

(2) Identification of the incidents/conditions in which the business continuity plan and/or the disaster recovery plan is activated.

(3) Procedures for disseminating information to the competent personnel concerning the problem at hand.

(4) Operational procedures for analysing incident reports, the assessment of the problem, and the restoration of networks, information systems and essential services.

(5) Recovery times under different fault conditions.

(6) Communication details of the operator's staff with technicians, suppliers, contractors of the operator, with other operators as the case may be, as well as the procedures for their cooperation concerning the implementation of procedures which are defined in the business continuity plan.

(7) Information regarding the availability of replacement equipment.

(8) Evaluation of the measures that have been taken in order to resolve a specific problem and the procedures for revising the business continuity plan and the disaster recovery plan

ANNEX III: FRAMEWORK OF SECURITY MEASURES

1. SECURITY MEASURES

Security measures related to network and information security are described in detail below, per category, including the objective and description of the measures.

1.1 PREPARE

The goal of the PREPARE pillar is to ensure that operators take into account the risk to information security in their day-to- day operations and ensure the commitment of the top-level management for addressing the threats, vulnerabilities and risks to security.

Category	#	Measure	Objective of the Measure	Description of the Measure
Strategy	STR1	Information security strategy	Establishment of an information security strategy laying out in detail the objectives and the approach at a high level with the aim of mitigating information security risks.	Definition of the vision and commitment for information security in a strategy that sets out in detail the specific security objectives, as well as the approach to security and the management of risk, and the means for validating the effectiveness of the strategy with the support of key performance indicators. The information security strategy is reflected in the information security policy, as described in measure [GOV3]. Officers are aware of the information security strategy and policy as described in measure [TA1].
Governance	GOV 1	Information security roles and responsibilities	Define information security roles and responsibilities within the organization.	Definition of the network and information security roles and responsibilities for all personnel involved in the processing of information or personnel who has access to information processing systems. The defined roles and responsibilities are reflected in the information security policy [GOV3]. Officers must be adequately informed and aware of their roles and responsibilities regarding network and information security as defined in measures [TA1, TA2]. The roles and responsibilities related to information security should be defined by the management in order to ensure accountability in the decisions of the management related to the security of the
Governance	GOV 2	Compliance with legal and regulatory obligations	To ensure compliance with all applicable legal and regulatory obligations regarding network and information security.	Establishment and maintenance of a central depository, and compliance with all relevant statutory and regulatory requirements and contractual requirements concerning network and information security.

Governance	GOV 3	Information security policies, standards, guidelines and procedures	Establishment of information security policies, standards, guidelines and procedures to be established which reflect the information security strategy	Definition of information security measures and detailed description of their implementation within the framework of an information security policy which reflects the objectives which are outlined in the information security strategy [STR1]. The information security policy should include the roles and responsibilities at the organisational level as set out in [GOV1.]. implementation of specific policies and procedures for the security of information in relation to specific processes, systems or activities, depending on the needs. Definition of operational guidelines for the security of information and standardized operating procedures for specific activities which relate to information or information processing systems at operational level.
Risk management	RM1	Methodology	Establishment of a risk management methodology which reflects risk assessment process, the risk analysis criteria, the risk acceptance criteria and the risk-taking policy of the organization.	Establishment of a methodology for risk management by defining the risk assessment process, the risk analysis criteria (i.e. impact criteria, probability criteria, risk score), the risk acceptance criteria and the organization's risk-taking policy. The risk management methodology will enable the organization to assess the information security risks that it faces, and implement appropriate measures to address or mitigate them. The organization should put in place processes and tools, as appropriate, to support its risk management processes, having as a minimum a risk register, a risk response plan and an information security governance structure setting out the roles and responsibilities in detail. The defined risk management methodology should be validated, agreed and supported by top-level management and by other relevant operators within the organization.
Risk management	RM2	Framework	Drawing up a list of assets, systems and processes within the organization.	Drawing up a list of assets, systems and processes within the organization and recording the dependencies and interdependencies between these assets, systems and processes in order to clearly capture the context / environment in which the risk assessment will be carried out. A clear view of the context of the organization will enable the identification of risks within the organization.
Risk management	RM3	Identification of risk	Identification of the threats, vulnerabilities and risks to which the organization's assets, systems and processes are exposed.	Identification and preparation of a list of threats, vulnerabilities and risks to which the organization is exposed with respect to the assets, systems and processes which are identified in measure [RM2]. The risks that will be identified within the scope of this process should be

Risk management	RM4	Risk analysis	Analysis of information security risks within the framework of assets against various probabilities and impacts.	Analysis of information security risks to assets, as defined in [RM2], by taking into account different probabilities and impact scores, as defined in [RM1]. The organization determines the risk score in order to assess its appropriate mitigation strategy [RM5]. When assessing the appropriate level of security, particular consideration shall be given to risks arising from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to information that is transmitted, stored or otherwise processed. Furthermore, regard should also be had to the risks which are presented which could potentially affect essential economic and social functions and services foreseen by Operators of Essential Services or Operators of Critical Information Infrastructure. The outcomes of the risk analysis should be recorded in the organization's risk register.
Risk management	RM5	Risk assessment	Assessment of information security risks on the basis of the organization's risk policy and determination of appropriate response strategies.	Definition of appropriate and sufficient strategies to address the risks analysed according to [RM4]. The organization shall take into account the reduction of the risk, the transfer of risk, the avoidance of the risk and the acceptance of risk (or the retention of risk) as appropriate risk management strategies. In assessing the risk strategies, the organization shall take into account its risk-taking policy as set out in [RM1]. The outcome of the risk assessment should be recorded in the organization's risk register.
Risk management	RM6	Handling risks	Determination of the actions for addressing information security risks.	Determination of appropriate and adequate risk mitigation measures in the context of the implementation of the risk mitigation strategy defined in the risk assessment process, as described in [RM5]. When determining the measures, the organization shall take into account preventive, detection and response measures from an administrative, technological and physical point of view, in order to ensure, where appropriate, a multi-layered defence. When determining the risk response actions, the operator shall consider the security measures described in the Security Measures Framework (this document). The outcome of the risk management should be recorded in the organisation's risk management plan.

Awareness and training	TA1	Awareness regarding information security	Establishment of a program for providing information with respect to information security for all officers within the organization, by taking into account the components described in the information security policies, standards, guidelines and procedures.	Establishment of an information security awareness program so that there is sufficient awareness amongst officers relating to the roles and responsibilities concerning network and information security as defined in [GOV1].
Awareness and training	TA2	Awareness and training on information security	Provision of training to all of the staff of the organization as defined in the information security program.	Adequately informing officers of their network and information security roles and responsibilities as defined in [GOV1] through appropriate education and training delivered with the support of top-level management. Information security training includes specific information about operational activities of officers on behalf of the organization in the context of information processing or access to information processing systems.
Managing third parties and suppliers	TPS1	Due diligence for third parties and suppliers	Exercise of due diligence regarding third parties and suppliers	Exercise of due diligence in identifying and entering into contractual relationships with third parties and suppliers, by taking into account third-party risks, including, but not limited to, supplier dependency, incident management and liability in relation to network and information security. The organization shall exercise due diligence in terms of information security when undertaking cooperation with third parties in particular in the context of obtaining or delivering software.
Managing third parties and suppliers	TPS2	Relationships with third parties and suppliers	Ensuring that contractual clauses on information security are incorporated into relationships with third parties and suppliers.	Maintenance of a central depository of suppliers, vendors and other third parties. The organization should ensure that all relationships with third parties are supported by appropriate contractual clauses to ensure, inter alia, that roles, responsibilities and liability in case of network and information security incidents are properly documented.

1.2 PROTECT AND DETECT

The aim of the PROTECT AND DETECT pillar is to ensure that operators establish, implement and maintain adequate information security measures which are appropriate to their exposure to risk. This pillar entails the adoption of prevention, detection and response measures from a technological, administrative and physical point of view.

Category	#	Measure	Objective of the Measure	Description of the Measure
Data Security	DS1	Management of the lifecycle of information	To ensure the protection of data throughout the lifecycle of the information, including the collection, recording, organization, structure, storage, adaptation or alteration, retrieval, search, use, communication by transmission, dissemination or any other form of disposal, association or combination, restriction, deletion or destruction.	Establishment, application and maintenance of information security measures for the protection of information throughout the lifecycle of the information. The lifecycle of the information is considered to be all the stages related to the processing of the information, while processing refers to any operation, or series of operations, which is carried out regarding personal data or sets of personal data, whether by automated means or not, such as the collection, recording, organization, structure, storage, adaptation or alteration, retrieval, search, use, disclosure by transmission, dissemination or any other form of disposal, correlation or combination, restriction, deletion or destruction.
Data Security	DS2	Sorting and labelling of information	To ensure that data is classified and labelled in such a way to reflect their sensitivity in order to ensure their proper processing.	Establishment, application and maintenance of a classification and labelling policy that ensures that information is classified and labelled according to its confidentiality and sensitivity. Consideration of possible implementation of classification and marking systems on the basis of international and industry best practices such as the “Traffic Light Protocol”. As a minimum, the organization should distinguish between public, private and classified information.
Data Security	DS3	Data backup and recovery	Enabling the recovery of information in the context of security events and incidents.	Establishment, application and maintenance of a data backup and recovery process to ensure the timely and effective recovery of data following an event or incident, or upon request. Data backup and recovery procedures should be adequately and frequently tested to ensure the proper and reliable operation of all supporting procedures and systems. Systems and supporting infrastructure, which enable data backup and recovery, should be geographically dispersed (storage at another location) in order to protect against natural security risks.

Data Security	DS4	Transfer and exchange of information	To implement adequate measures in the context of the transmission and exchange of information internally or with third parties, in order to ensure the safe transfer of data.	Establishment, application and maintenance of procedures for the transfer and exchange of information in order to ensure the protection of information when it is transferred or exchanged internally or with third parties. The transfer and exchange of information should take into account regulatory and legislative requirements, as set out in [GOV2], for instance when processing information in the context of international data transfers.
Data Security	DS5	Prevent data loss and data leakage	To ensure data protection from intentional or unintentional data loss and leakage.	Establishment, application and maintenance of reasonable measures for reducing the risk of data loss and data leakage by taking appropriate technical and organizational measures for prevention. The measures for preventing data loss or leakage should take into account external and internal sources of threat that could potentially disclose classified or sensitive information. Adequate access control measures should be implemented in order to interface with the measures for the prevention of data loss and data leakage. Policies for exchanging and sharing data should be based on the role of the user as defined in [IAM1]. When determining the measures for the prevention of data loss and leakage, the organization should consider the classification, protection and monitoring of information.
Change management	CM1	Change management	To ensure that changes to processes and information systems are implemented in a secure manner, without compromising the confidentiality, integrity, availability or authenticity of information.	Establishment, application and maintenance of procedures for the management of changes in order to control and manage changes to systems, applications and other supporting assets in the context of the processing of information. When defining the change management process, the organization must provide for change requests in order to accommodate changes requested by participants. The change management process should enable the organization to assess the risks in the context of change requests and to plan changes by taking into account appropriate security measures. The change management process should include the preparation and verification of changes.
Change management	CM2	configuration management	To be found, to be preserved and yes information about the organization's assets and configurations is verified.	Establishment, application and maintenance of processes for managing the configuration of the assets which support the networks and information systems. The organization shall keep a record of the configurations which are applicable to those assets. Organizations shall define and document the relationships between the configurations of the assets for the purpose of identifying interdependencies and to ensure the proper management of the change with respect to the modification of configurations.

Asset management	AM1	Management of the lifecycle of assets	To ensure that assets are secure throughout their lifecycle, including their supply, development, maintenance and disposal.	Establishment, application and maintenance of measures for the security of information within the framework of the plan for the management of the lifecycle of the assets, in order to ensure that the security of information forms an integral part of that lifecycle, i.e. the supply, installation, maintenance and disposal. The management of the lifecycle of information as described in measure [DS1], should form part of the plan for the management of the lifecycle of the assets. The plan for the management of the lifecycle of the assets must describe all procedures for handling information in accordance with the policy for the classification and labelling of data as described in measure [DS2].
Asset management	AM2	Recording of assets and ownership	To ensure that assets are recorded in an inventory and that ownership is established for the purposes of achieving traceability and accountability for the assets.	Establishment, application and maintenance of a list of the assets in order to ensure that the organization has a clear, accurate and up-to-date inventory of the assets (e.g. hardware, software, information) that it maintains. The list should identify the owner of these assets. The list should also enable the organization to track all assets for which it should implement and maintain information security measures.
Asset management	AM3	Monitoring of assets	To ensure that assets are monitored for attacks, anomalies and security threats in order to activate the procedures for handling incidents and events.	Establishment, application and maintenance of capabilities for the monitoring of assets so that the organization is in a position to detect anomalies in relation to normal conditions (e.g. location, usage) and/or the operation of those assets. The organization should state in the acceptable use policy, as described in [HRS6], what is acceptable use and/or operation of the assets. The organization could also consider including the description of acceptable use, function and location of the assets in the list of assets, as described in [AM2], in order to have a complete inventory of these assets. When anomalies are detected, procedures should be activated for the management of incidents and events in order for the organization to be resilient to the presence of anomalies.

Asset management	AM4	Availability management	To ensure the availability of networks and information systems by achieving the adequate availability of resources, redundancy and highly available systems / processes.	Establishment, application and maintenance of procedures for the management of availability in order to ensure that the desired level of operational services is provided by the organization. The organization should ensure the availability of resources (e.g. premises, staff, IT systems, etc.) at all times. As described in measure [NS6], the organization should guarantee the backup and high availability of all IT systems in order to ensure the timely and effective recovery of data following an event or incident, or upon request. The organization should create backup copies of the information described in [DS3].
Asset management	AM5	Encryption	To ensure the confidentiality, integrity and authenticity of information by adopting appropriate encryption solutions.	Establishment, application and maintenance of a policy regarding the use of encryption measures in order to ensure the confidentiality, integrity and authenticity of data during storage, use and transfer. The encryption policy should consider the implementation of encryption measures at all stages of the lifecycle of the information and examine applications, systems, network equipment and communication channels.
Asset management	AM6	Capacity management	To ensure the appropriate capacity and performance of service of the information systems and processes.	Establishment, application and maintenance of a capacity management process in order to ensure that the capacity and performance of the organization's IT systems are not adversely affected by increased levels of service demand. The capacity management process should include the management of operational capacity in order to ensure that operational needs are converted into capacity requirements, to ensure the management of the capacity of services in order to properly manage the capacity of IT subsystems and a mechanism for submitting reports on the management of capacity.
Identity and access management	IAM1	Control of access based on roles	To authenticate the authenticity and the authorization of users based on the minimum privilege and organizational roles and competencies.	Establishment, application and maintenance of measures for managing the identity and access, which consider access measures based on roles for the purpose of providing technical and organizational means for enforcing the principle of minimum privilege and managing privileged users accordingly. The control of role-based access should ensure that sufficient permissions are granted to users on the basis of their responsibilities associated with their respective roles. The control of role-based access should be performed in accordance with the procedures for the security of human resources as defined in [HRS1], in order to ensure that access roles are aligned with the roles and responsibilities of officers within the organization.

Identity and access management	IAM2	Control of external access	To ensure adequate measures in the context of external access to organizational resources.	Establishment, application and maintenance of measures for the control of access for external and remote access to organizational resources. The organization should ensure the ability to remotely access the network by using virtual private networks (VPNs) and access remote applications through the use of external application interfaces. The organization should implement adequate measures for identity and access management in order to reflect its information security policy as defined in [GOV3] and the specific role-based access control as defined in measure [IAM1].
Identity and access management	IAM3	Management of privileged users	To ensure adequate measures for users who have privileged access to organizational resources, systems and networks.	Establishment, application and maintenance of measures in order to ensure the proper management of privileged users, and to activate them only when necessary. The organization should ensure that users are not granted privileged rights by default and that appropriate technical and organizational measures are implemented to ensure that the privileged rights of users are protected from malicious acts or from other negative behaviours or intentions. The organization shall ensure that systems and applications do not operate with privileged user rights by default, in order to mitigate the risk of escalation of privileges.
Identity and access management	IAM4	Strong measures for identity verification	To ensure that the identity of authorized persons is verified n people securely and using strong identity verification measures.	Establishment, application and maintenance of strong measures for controlling access and authentication in order to ensure that authorized individuals are properly identified and authenticated when processing organizational resources. The organization must consider multi-factor authentication in order to prove an individual's identity. This process must include at least two of the following principles: providing identity by possessing a specific factor (e.g. a key or other means of authentication), by knowing a factor (e.g. a code or access phrase, or other secret), with biometric or morphological features (e.g. iris scan, fingerprint or visual identity verification by a trusted party such as a security guard).
Identity and access management	IAM5	Credential management	To ensure the secure management of credentials for access to corporate resources, and that users are securely authenticated for use of organization services.	Establishment, application and maintenance of procedures for the management of credentials in order to ensure the proper management of authentication and verification means by which users can access organizational resources. The organization should consider using bundled credentials (e.g. single sign-on) to improve user experience for authentication and access. The organization must consider the management of credentials for users, systems and networks in order to ensure the control of access throughout the lifecycle of the information as set out in measure [DS1].

Identity and access management	IAM6	Traceability and control	To ensure the non-denial of traceability of the actions of users which are carried out within the scope of organizational resources so that intentional or unintentional activities that have a negative impact can be detected and investigated.	Establishment, application and maintenance of measures for identity and access management in order to ensure chronological traceability and ability to control, in order to enable the accountability of users who execute commands in information processing systems. The operator must consider measures that ensure non-repudiation by users. The organization must consider the ability to perform traceability and control within the context of managing the identity and access which is applicable to the systems, applications and networks.
Identity and access management	IAM7	Management of the lifecycle of the identity	To ensure that the roles and the approval of the identity reflect the lifecycle of the identity of the user.	Establishment, application and maintenance of adequate measures for the identity and access management throughout the lifecycle of the identity, including but not limited to the provision, identity verification, approval and removal of identities. Controls regarding the management of the lifecycle of the identity should be integrated into the procedures for the security of human resources as set out in measure [HRS1], in order to ensure that access roles are aligned with the lifecycle of employment of staff within the organization.
Management of vulnerabilities and security updates	VM1	Detection and identification of vulnerabilities	To ensure that the vulnerabilities of systems are known to the organization so that they can be handled appropriately.	Drawing up, application and maintenance of a plan and of a risk-based approach for testing applications, systems and networks for vulnerabilities and weaknesses that could be exploited by threats. The organization should consider detection in order to identify vulnerabilities that arise from new or modified processes or systems in the context of processing information. Vulnerabilities must be detected and located in the context of threats against the confidentiality, integrity and availability of information. The organization should consider penetration testing as a means for detecting and identifying vulnerabilities. The outcomes of vulnerability detection and identification efforts should be recorded as described in measure [VM2].

Management of vulnerabilities and security updates	VM2	Recording and reporting vulnerabilities	To ensure that vulnerabilities are recorded and reported so that the management can make informed decisions on how to handle them.	Establishment, application and maintenance of procedures for recording and reporting vulnerabilities that have been identified in order to enable the remediation and updating of systems and procedures to ensure confidentiality, integrity and availability of information. The recording and reporting of vulnerabilities should be the outcome of vulnerability detection and localization efforts as described in measure [VM1]. The organization should consider including information on high-risk vulnerabilities in general reports to the management in order to ensure top-down awareness of vulnerabilities that have potential impacts and to identify appropriate measures to remediate and implement corrective systems and processes, as described in measure [VM3].
Management of vulnerabilities and security updates	VM3	Fixing of vulnerabilities and security updates	To ensure the remediation of the vulnerabilities of systems and the application of security updates following a decision by the management.	Establishment, application and maintenance of procedures in order to remediate vulnerabilities and introduce security updates for vulnerabilities that have been identified in systems, applications and network components, and which require mitigation as a result of the assessment of the management. The remediation of vulnerabilities and security updates must come from the decision of the management on the basis of the recording and reporting of vulnerabilities as described in measure [VM2].
Network security	NS1	Perimeter security	To ensure that the local network interface with the external network is protected from attacks, threats and other intentional or unintentional actions with potentially negative effects.	Establishment, application and maintenance of appropriate network security measures for the purpose of protecting the perimeter of the network from external threats and ensuring the confidentiality, integrity and availability of information located in the internal network. The organization should consider that perimeter security is only one specific layer in a multi-layered defence architecture. To protect against network attacks, the organization should consider specific threats to the organisation and specific network threats and risks to the sector. The organization should take into account firewalls and intrusion detection and prevention systems as described in measure [NS7]. The organization should take reasonable steps to ensure that data traffic is filtered on the basis of the organization's security policies.

Network security	NS2	Separation and segmentation of the network	To ensure the separation of the logical network, according to the business functions, and to prevent the spread of malicious components.	Establishment, application and maintenance of appropriate network separation and segmentation to ensure - logical and/or physical - separation of information networks. In designing, implementing and maintaining network separation and segmentation measures, the organization should take into account the various areas of the organization's operational activity. The organization should take into account the nature and extent of data processed in the context of specific business activities in order to ensure adequate segregation. The organization should consider adopting virtual local area networking (VLAN) when designing network segmentation and architecture. As a minimum, the organization should consider the separation of research and development, administration, central information infrastructure, and publicly available (online) applications and systems.
Network security	NS3	Protection against denial of service	To ensure that organizational resources are protected from denial of service attacks, and that legitimate service activities are not affected.	Establishment, application and maintenance of adequate protection against denial of service and distributed denial of service in order to ensure the timely and qualitative provision of service to authorized and authenticated users and to maintain a consistent level of productivity. In designing the relevant protection measures, the organization should consider incorporating capabilities to detect legitimate users and applications against malicious attempts of accessing resources. The organization should take into account redundancy and high availability measures, as described in measure [NS6], in order to ensure uninterrupted operation in case of a threat to the availability of information and services.
Network security	NS4	Secure communication protocols	To ensure appropriate communication protocols in order to achieve secure communication between network resources.	Establishment, application and maintenance of secure protocols for facilitating the flow of information between network points, applications and systems, in order to ensure the confidentiality and integrity of information during their transit and to prevent network attacks and threats, such as the interception of communications. The organization should examine the most modern communication protocols when ensuring the transfer and exchange of information through communication networks. The organization must consider security measures supported by cryptographic means, as defined in measure [AM5] for the security of communications, by using technologies such as Hypertext Transfer Protocol Secure (HTTPS), Internet Protocol security (IPsec), Transport Layer Security (TLS) / Secure Sockets Layer (SSL), depending on the intended level of technology.

Network security	NS5	Control of access to the network	To ensure that access to the logical network from external and internal systems is properly secured so that only authorized persons can access organizational resources.	Establishment, application and maintenance of measures for controlling access to the network in order to ensure reasonable access to the network of the organisation and to information resources, and to prevent unauthorized access. The organization should consider specific technical and organizational measures, such as authentication mechanisms for network access, in order to facilitate the operation of this measure. The organization should consider the control of access to the network for wired, wireless and other types of network connectivity. The organization should consider the possibility of integrating the control of access to the network with centralized credentials and with procedures for identity and access management as defined in measure [IAM5].
Network security	NS6	Redundancy and high availability	To ensure the availability of information and information networks by achieving sufficient availability of resources, backup equipment, high-availability systems and connections	Establishment, application and maintenance of adequate measures to ensure a reasonable level of redundancy and high availability, in particular for mission-critical systems, services and applications that process classified and/or operational information. The organization must consider redundancy and high availability at all levels of technology, including storage, communication and processing. The organization should consider backup and high-availability technologies such as alternate connection or backup systems, Redundant Arrays of Independent Disks (RAID), and cold, warm, and hot data storage facilities
Network security	NS7	Intrusion detection and prevention	To ensure the detection and prevention of external intrusion attempts and security attacks.	Establishment, application and maintenance of adequate measures to detect and prevent intrusions into the organization's network and resources. The organization should consider intrusion detection systems (IDS) and intrusion prevention systems (IPS) in order to mitigate the risk of an external intrusion attempt. The organization should consider creating a management console to monitor the network with the aim of logging all intrusion attempts for further analysis. As part of the design of intrusion detection and prevention processes, the organization should consider automatically activating levers to respond to incidents, as defined in [EIM2],. The organization should consider security incident and incident management (SIEM) solutions to support intrusion prevention and detection processes.

Security of systems	SS1	Combating malware	To ensure that organizational resources are not affected by malware and code contamination.	Establishment, application and maintenance of adequate measures to protect systems from malware and code contamination in order to ensure the confidentiality, integrity, availability and authenticity of the information. The provider should examine a range of anti-malware measures, including operating systems, network systems and services, network equipment operating systems, user end-points and mobile devices, and mobile content devices. The organization must ensure that measures to combat malware are based on up-to-date data in order to detect and resolve malware threats.
Security of systems	SS2	Shielding systems and devices and basic safety requirements	To minimize, as far as possible, the extent of the attack to information systems, through the reduction of their functionality and their characteristics.	Establishment, application and maintenance of a process to shield systems and devices based on defined basic security requirements in order to prevent the unauthorized access and use of system resources and services. The organization should examine operating systems, applications and any other software which is installed on devices that fall within the scope of the shielding process. The organization should review system shielding guidelines and documents provided by software and hardware vendors, as well as the guidelines and best practices that are published by systems technology groups, regulatory authorities, and other international best practices or frameworks. The organization must take into account, at least, default configurations and the removal of unnecessary predefined accounts, ensuring uniform primary functions per server in order to avoid functions with different security levels on the same server, providing only the necessary services, protocols and daemons, by using system security parameters to prevent abuse, and by removing any unnecessary functionalities, such as scripts, drivers, features, and subsystems, in order to minimize the extent of the attack on the system. The organization should consider implementing system-level firewalls in order to prevent malicious code from affecting the security of the information which is stored at the endpoint.
Security of systems	SS3	Security of mobile devices	To ensure appropriate security of mobile devices which access organizational resources.	Establishment, application and maintenance of security measures for mobile devices in order to ensure the confidentiality, integrity, availability, and authenticity of mobile systems used by officers to connect to, interact with, or process organizational infrastructure and resources. The organization must consider the management of mobile devices, secure storage and encryption measures as defined in measure [DS5], strong authentication as defined in measure [IAM4], and secure communication and networking measures as defined in measure [NS4] . The operator must ensure the adequate protection of mobile devices and information which is stored on mobile devices against theft and loss. The organization should consider the possibility of remote cleaning and geo-location.

Security of systems	SS4	Application configuration management	To ensure appropriate management of applications used to access or process organizational resources.	Establishment, application and maintenance of measures for the management of the configuration of applications in order to prevent the unauthorized and malicious installation, configuration or modification of applications and software on organizational assets and devices. The organization should consider creating a central interface for the management and configuration of applications in order to ensure that all of the devices of the organization are managed centrally, while configuration and software updates can be pushed to end devices. This central management interface should enable the organization to establish a list of certain types of applications that are permitted or not permitted.
Application security	AS1	Secure lifecycle for the development	To ensure adequate security measures in the context of software development activities developed by the oi	Establishment, application and maintenance of practices for the secure development of software in traditional processes for the lifecycle for the development of software in order to ensure that security is built into the design of activities for the application and development of software. The organization should consider applying, at a minimum, a risk assessment at the initial stage of the project, by performing security testing and code review in the development stages of the project and performing a security assessment and secure configuration during the delivery of the project. The organization must ensure that appropriate measures are in place to separate software development environments from the operational production environment. The organization should ensure that data used for testing is anonymized and not linked to confidential and sensitive information in the context of development activities.
Human resource security	HRS1	Employment lifecycle	To implement adequate measures in order to ensure that officers working on behalf of the organization who have access to organizational resources support the organization's information security policy and objectives.	Establishment, application and maintenance of a plan to ensure that information security is integrated throughout the lifecycle of employment (i.e. before, during and after the employment of employees) and to make all reasonable efforts to ensure that employees understand their responsibilities in relation to information security. The plan includes appropriate information security measures at each phase of employment, e.g. background checks before employment, employee training and awareness, incorporating adequate provisions into employment contracts, establishing an acceptable use policy, employees returning devices that contain critical information and removing access to systems and applications in accordance with the management of the lifecycle of identities as defined in measure [IAM7].

Human resource security	HRS2	Employee monitoring	To ensure that officers working on behalf of the organization comply with the information security policy and meet their security responsibilities throughout the duration of employment.	Establishment, application and maintenance of a plan to monitor the compliance of employees with information security obligations and responsibilities throughout the duration of employment.
Human resource security	HRS3	Disciplinary measures and enforcement	To ensure that officers working on behalf of the organization are accountable for intentional or unintentional activities which affect the organization's information security objectives.	Establishment, application and maintenance of a series of disciplinary measures to ensure the compliance of officers with their information security obligations and responsibilities and to take action in case of a breach of these obligations and responsibilities. The organization should consider establishing a formal sanctioning process for officers who do not comply with their information security obligations and responsibilities. Non-compliance with information security obligations and responsibilities to be identified through employee monitoring procedures [HRS2].
Human resource security	HRS4	External partners	To ensure that external associates working on behalf of the organization adhere to the organization's information security policy and security objectives.	Establishment, application and maintenance of information security measures in relation to external personnel, e.g. with contractors in order to ensure the adequate protection of information that is exchanged with external partners.
Human resource security	HRS5	Protection against insider threats	To ensure protection against network and information security threats from within the organization.	Establishment, application and maintenance of appropriate measures to prevent, detect and monitor attacks from inside persons, through ignorance, negligence, or malicious or professional intent. The organization must train and raise awareness amongst employees concerning information security practices within the organization in accordance with measure [TA2], carry out adequate screening of candidates in accordance with measure [HRS1], and monitor employees [HRS2] in order to reduce the likelihood of insider attacks.

Human resource security	HRS6	Employment agreements and acceptable use	To ensure that responsibilities related to information security and the acceptable use of assets are incorporated into employment agreements and employee initiation procedures in order to achieve accountability and awareness	Establishment, application and maintenance of an acceptable use policy, which sets out what the organization considers to be an acceptable use of information systems that are made available to officers, in order to ensure that officers are aware what is expected of them in terms of use, e.g., computers and mobile devices. The organization should consider testing the awareness of the acceptable use policy. The organization should also enter into adequate employment agreements which clearly state the employee's information security obligations and responsibilities.
Physical security	PS1	Environmental measures	To ensure that adequate measures are taken to protect the organization from the effects of natural disasters, such as floods, earthquakes and fires.	Establishment, application and maintenance of appropriate measures to protect the organization from the effects of natural disasters, such as floods, earthquakes and fires. The organization must take the geographic location into account when building the network infrastructure and ensure that critical infrastructure components and systems are geographically dispersed.
Physical security	PS2	Control of perimeter access	To ensure the physical perimeter of the organization by securing and preventing unauthorized access.	Establishment, application and maintenance of a physical security perimeter to protect information processing facilities. The organization must establish appropriate perimeter access control measures by implementing physical boundaries such as fences, doors and walls. The organization must also require employees and visitors to provide identification to security guards in order to enter (in some part of) the organization. The organization should consider installing CCTV cameras to detect intruders within the organization's boundaries.
Physical security	PS3	Control of internal access	To ensure the control of access to internal workplaces and facilities, in order to ensure that physical access is limited on a need basis	Establishment, application and maintenance of internal access measures, aligned with the roles described in [IAM1], to ensure that only those with a legitimate interest have access to (specific parts of) the organization, e.g. by creating special ID scanners to access a part of the organization.

Physical security	PS4	Safety of cabling, equipment and facilities	To ensure the physical protection of the cabling and equipment which supports the processing of information, against interference, intrusion or damage.	Establishment, application and maintenance of appropriate measures to protect cabling and other equipment from interference, intrusion or damage that could cause an interruption to the services of the organization. The organization must ensure that cables that supply electricity to critical infrastructure are properly protected and must train employees in accordance with measure [TA2] so that they are aware of the importance of equipment that supports information processing activities. Physical access to logical networks should also be protected with appropriate measures in order to prevent unauthorized physical access to the organization's logical equipment and network. The operator must consider taking appropriate measures regarding network access as defined in [NS5]. The organization must ensure the physical integrity and regular maintenance of the facilities where the network equipment is installed, as well as the proper operation of security measures.
Physical security	PS5	Internal environmental measures	To ensure that the internal areas and facilities of the organization are protected from physical damage.	Establishment, application and maintenance of physical security and protection measures so as to avoid any physical damage to the internal areas and facilities of the organization. In implementing internal environmental measures, the organization should consider the risks related to fire and temperature, humidity, electricity, water use and other components that could adversely affect the physical security of the assets. The organization should consider fire suppression, moisture control and other measures which are appropriate to the characteristics of indoor physical areas, such as data centres or other areas where equipment for the processing of information are located.

1.3 RESPOND

The aim of the RESPOND pillar is to ensure that operators are able to respond to events and incidents that may affect the confidentiality, integrity, availability or authenticity of the information. This pillar entails the adoption of business resilience and business continuity and disaster recovery measures, as well as the restoration of normal activities.

Category	#	Measure	Objective of the	Description of the Measure
Management of events and incident	EIM1	Preparedness and detection of incidents and events	To ensure that the organization is able to identify incidents and events that may pose a threat to the organization's information security objectives and to activate the corresponding incident response procedures.	Establishment, application and maintenance of an event and incident management and response plan to ensure that the organization is ready to respond in case of a serious information security event or incident. The organization should consider aligning its event and incident response processes with general monitoring capabilities and specific security monitoring functions, such as intrusion detection and prevention services described in measure [NS7].
Management of events and incident	EIM2	Analysis and evaluation of events and incidents	To ensure that the organization is in a position to analyse and assess information security events and incidents in order activate appropriate containment and recovery procedures.	Establishment, application and maintenance of procedures that enable the analysis and evaluation of events and incidents so that the organization is in a position to make reasoned decisions concerning the actions and measures to be taken in order to respond to or recover from events and incidents wthatconcern security. The organization should consider the impact on data subjects, business activities, external parties and the ecosystem of providers. The organization should ensure that the analysis and evaluation of events and incidents is carried out in consultation with senior management in order to link events and incidents to high-risk scenarios.
Management of events and incident	EIM3	Mitigation and recovery from events and incidents	To ensure adequate containment and recovery from security events and incidents which adversely affect the organization's information security objectives.	Establishment, application and maintenance of procedures in order to contain and recover from events and incidents so as to minimize their impact on systems, applications, networks and data and to ensure, to the extent possible, the critical operations of organization. The organization should consider its event and incident recovery objectives, by taking into account the recovery objective (RPO) and the recovery time (RTO), in order to determine the targeted duration and the level of services within which a business process must be restored following an incident.

Management of events and incidents	EIM4	Activities following the event and incident	To ensure that the organization learns from security events and incidents in order to prevent similar events and incidents in the future.	Establishment, application and maintenance of procedures following an event and incident in order to record lessons learned from information security events and incidents and to determine whether additional security measures should be established in order to prevent similar events and incidents. The organization should consider establishing a process following an incident, which includes the holding of meetings in order to assess the event or incident with affected system owners, data controllers and other stakeholders involved in the measure in order to deal with the incident, with the aim of sharing lessons learned and determining preventive measures.
Management of events and incidents	EIM5	Regulatory obligations for the notification of incidents and cooperation	To ensure that the organization informs relevant stakeholders in the event of security incidents or incidents, as described in legal and regulatory obligations.	Establishment, application and maintenance of procedures to ensure compliance with regulatory and statutory requirements regarding the reporting of incidents. The organization must ensure that adequate notification and reporting procedures are in place for events and incidents regarding information security to the relevant regulatory authorities, such as the DSA. In the context of personal data, the organization must ensure compliance with the relevant legislative and regulatory provisions concerning the protection of personal data and must communicate, where necessary, with the competent data protection authority.
Management of events and incidents	EIM6	Communication with interested operators concerning events and incidents	To ensure that the organization communicates information concerning network and information security events and incidents to internal and external operators concerned.	Establishment, application and maintenance of procedures to ensure relevant communication regarding information security events and incidents to external and internal recipients in order to ensure awareness regarding the event or incident and provide external and internal operators concerned with the ability to determine appropriate response measures, if necessary. The organization should consider working with external and internal operator stakeholders to mitigate events and incidents to minimize related impacts and follow up activities to establish preventative measures, such as with the DSA and emergency services.
Business continuity and resilience	BCR1	Analysis of business impacts	To ensure that the organization has analysed and assessed the critical business processes to be considered in the business continuity plan so that the organization can restore business processes to an acceptable level as soon as possible in the event of an event or incident.	Establishment, application and maintenance of a process for the analysis of business impacts in order to identify all critical assets within the organization. The analysis of business impacts will enable the organization to prioritise functions and systems on the basis of the need to deliver business services. The analysis of business impacts must be carried out on the basis of a classification system that takes into account defined levels of criticality and examines whether critical functions or systems operate independently or are linked to another function or system of the organization.

Business continuity and resilience	BCR2	Business continuity plan	To ensure that the organization has a plan in place in order to maintain the continuity of critical business processes and to recover during and after an event or incident.	Establishment, application and maintenance of a business continuity plan to ensure that the organization can respond to emergency situations in a prompt and appropriate manner, and is able to maintain business operations while minimizing the consequences and damages which arise from an incident. The business continuity plan must include the disaster recovery plan described in measure [BCR4] and must take into account the analysis of business impacts.
Business continuity and resilience	BCR3	Business continuity exercises and simulations	To ensure that the organization and its personnel are aware of their responsibilities during an event or incident that triggers the business continuity plan.	Establishment, application and maintenance of measures for testing, reviewing and improving the business continuity plan through exercises that simulate events and incidents inside the organization, with the aim of testing the organization's response to similar events and incidents and improving business continuity processes. Business continuity exercises and simulations should enable the organization to identify opportunities for improving and achieving better outcomes over time. The organization should consider linking the business continuity plan to the change management processes as described in [CM1] so that the business continuity plan takes into account the consequences of any changes within the organization. The organization should carry out business continuity drills and simulations at regular intervals so that employees are alert to events and incidents that could harm the organization. When developing the business continuity plan, the organization should also consider disaster recovery as defined in measure [BCR4].
Business continuity and resilience	BCR4	Disaster recovery plan	To ensure that the organization has a plan for restoring critical information systems to an acceptable level during or after an incident.	Establishment, application and maintenance of a disaster recovery plan to ensure the restoration and recovery of all critical processes of IT systems and supporting assets, such as power supply following an incident. The disaster recovery plan should include clear instructions for IT staff in order to ensure a timely and effective response to all incidents affecting the organization's IT environment. The disaster recovery plan should specify the recovery objective (RPO) and the recovery time objective (RTO) in order to avoid unacceptable consequences for the organization.

2. APPENDIX A: SOURCES FOR FURTHER INFORMATION ON SECURITY MEASURES

This annex provides informative references to the guidelines published by public bodies such as ENISA and competent national authorities, which can help operators implement the information security measures contained in the Framework.

Pillar	Informative Reports			
	Title	Author	Date of publication	URL
PREPARE	Governance framework for European standardization	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 organizations	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 Lifecycle	SANS	/	https://software security.sans.org/resources/paper/cissp/defining understanding-security-software-development-lifecycle
	Secure Software Engineering Initiatives	ENISA	May 01, 2011	https://www.enisa.europa.eu/publications/secure software-engineering-initiatives

Pillar	Informative Reports			
	Title	Author	Date of publication	URL
	Asset protection CP	NI	/	https://www.cpni.gov.uk/protecting-my-asset
	Physical Security C	PNI	/	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
	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 Incidents 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

2. APPENDIX B: IMPLEMENTATION GUIDELINES: ISO/IEC 27001 AND NIST SP800-53

This annex includes references to the application instructions for each security measure. The application guidelines in the table below refer to two international standards: ISO/IEC 27001 and NIST SP800-53 Rev. 4, and are provided to help operators understand the content of the safety measures.

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	A.1.1, A.8.1.2	CM-8
AM3	Asset monitoring	A.12.4	PE-20
AM4 A	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	cure software development lifecycle	A.14.2	SA-8, SA-10, SA-11
BCR 1	Business impact analysis	A.16.1.1, A.17.1.1, A.17.1.2	RA-2, RA-3, PM-9
BCR 2	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
BCR 3	Business continuity exercises and simulations	A.17.1.3	CP-4, IR-2, IR-3, PM-14
BCR 4	Disaster recovery plan	A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 A.12.1.2	CP-2, IR-8, CP-4, IR-3, PM-14
CM1	Change management		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 In	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	Pick up 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
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
GOV 1	Information security roles and responsibilities	§5.3, A.6.1	PL-1, PL-4

GOV 2	Compliance with legal and regulatory requirements	§4.2, A.6.1.3, A.18.1	AR-2, AU-6, AU-11
GOV 3	Information security policies, standards, guidelines and procedures	§5.2, A.5.1	
HRS 1	Employment lifecycle	A.7	PS-1, PS-2, PS-5
HRS 2	Employee monitoring	A.12.4	PS-8
HRS 3	Disciplinary measures and enforcement	A.12.4	PS-8
HRS 4	External human resources	A.15.2	PS-7
HRS 5	Insider threat protection	A.7, A.12.4	PS-1, PS-2, PS-5, PS-8
HRS 6	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
IAM7I	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 N	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
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,	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	ISO 27005	PM-8, PM-9, PM-11, SA-14
RM2	Context	§4, ISO 27005	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	ISO 27005	RA-3, SI-5, PM-12, PM-16
RM4	Risk Analysis	§6.1, §6.2, ISO 27005	RA-1, RA-2, RA-3, RA-4, RA-5, RA-6
RM5	Risk Evaluation	§6.1, §6.2, ISO 27005	RA-1, RA-2, RA-3, RA-4, RA-5, RA-6
RM6	Risk Treatment	§6.1, §6.2, ISO 27005	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
Ref.	Control	ISO/IEC 27001	NIST SP800-53 Rev. 4
SS4	Application configuration management	A.12.1, A.12..4.1	CM-3, CM-5, SA-10, SI-2
STR 1	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

3. ANNEX C: GLOSSARY

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

English Term	Description
Asset	An asset constitutes any resource that can be valuable for an organization.
Attack Surface	The collection of different points such as components, software or vulnerabilities (in a computing device or network) where an unauthorized 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 operator.
Availability	Ensuring that information or services are accessible when an authorized operator requires access.
Confidentiality	Ensuring that information is not accessible to unauthorized 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 unauthorized 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.
Integrity	Integrity ensures the consistency, accuracy, and trustworthiness of data.
Incident	An event that has a potential or actual negative impact on the confidentiality, integrity or availability of a system.
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, viruses, worms and spyware.
Network Perimeter	Boundary between the private/local part of a network and the public/provider part of a network or the internet.
Patching	A set of changes made to software in order to fix bugs, weaknesses or vulnerabilities and enhance the performance of that software.
Risk	A risk is the likelihood of a threat exploiting a vulnerability outcome 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.
Risk identification	Procedure of finding, listing and describing risks.
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 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.

4. ANNEX D: NIS WORKING GROUP REFERENCE DOCUMENT

The table below demonstrates that the security controls as described in the NIS Working Group reference document are covered by this Security Measures Framework.

NIS Cooperation Group Reference Document	DSA Security Measures Framework
1. Governance and ecosystem	
1.1. Information System Security Governance & Risk Management	
Information system security risk analysis	RM4
Information 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
Administrative 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	
Industrial control systems	AM5, IAM2, SS1
2.5. Physical and Environmental Security	STR1, GOV2
3. Defence	PS1, PS2, PS3, PS4, PS5
3.1. Detection	
Detection	EIM1
Logging Logs	AM3
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