National Cybersecurity Agency

Determination of the Director General of the National Cybersecurity Agency

referred to in Article 31(1) and (2) of Legislative Decree No. 138 of 4 September 2024, adopted in the manner referred to in Article 40(5)(l), which, under Article 42(1)(c), in the first phase of application, lays down the basic procedures and specifications for the fulfilment of the obligations referred to in Articles 23, 24, 25, 29 and 32 of the same decree.

THE DIRECTOR GENERAL

HAVING REGARD TO Decree-Law No 82 of 14 June 2021, as converted with amendments into Law No 109 of 4 August 2021, on *Urgent provisions on cybersecurity, the definition of the national cybersecurity architecture and the establishment of the National Cybersecurity Agency*;

HAVING REGARD TO Legislative Decree No. 138 of 4 September 2024, on *the transposition of Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the EU, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148*, hereinafter referred to as the NIS Decree, and, in particular, Article 31(1) and (2) thereof, which provides that, for Articles 23, 24, 25, 27, 28 and 29, the NIS Competent National Authority shall establish proportionate obligations taking due account of the degree of exposure of entities to risks, the size of entities and the likelihood of incidents occurring, as well as their severity, including their social and economic impact, as well as deadlines, arrangements, specifications and phased implementation of such obligations;

HAVING REGARD TO Article 40(5)(l) of the NIS Decree, which provides that such obligations shall be established by one or more Determinations of the National Cybersecurity Agency, after consulting the Working Group for the Implementation of the NIS Framework;

HAVING REGARD ALSO TO Article 42(1)(c) of the NIS Decree, which provides, in the first phase of application, that the NIS Competent Authority shall establish the basic arrangements and specifications for the fulfilment of the obligations above;

HAVING REGARD TO the Prime Ministerial Decree of 10 March 2023, appointing Prefect Bruno Frattasi as Director General of the National Cybersecurity Agency;

HAVING REGARD TO the *National Framework for Cybersecurity and Data Protection*, 2025 edition (Italian framework), developed by the Cyber Intelligence and Information Security (CIS) Research Centre of the Sapienza University of Rome and by the Cybersecurity National Lab of the National Interuniversity Consortium for Informatics (CINI), in cooperation with the National

Cybersecurity Agency (ACN), as a support tool for public and private organisations operating in the field of cybersecurity strategies and processes;

CONSIDERED that the technical annexes containing the aforesaid basic specifications, outlined at the second plenary meeting of the Working Group for the Implementation of the NIS Framework, held on 28 January 2025, were shared with the sectoral authorities and with the sectoral associations also using the sectoral working groups referred to in Article 11(4)(f) of the NIS Decree;

HAVING ACKNOWLEDGED the feedback received;-

HAVING CONSULTED the Working Group for the Implementation of the NIS Framework at its meeting of 10 April 2025;

DEEMED IT APPROPRIATE to initiate the information procedure under Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015;

CONSIDERED the degree of exposure of entities to risks, the size of the entities and the likelihood of accidents occurring, as well as their severity, including their social and economic impact;

ADOPTS THIS DETERMINATION

Article 1
(Definitions)

1. For the purposes of this Determination,
   a) “NIS Decree” shall mean Legislative Decree No 138 of 4 September 2024;
   b) “National Cybersecurity Agency” shall mean the National Cybersecurity Agency referred to in Article 5(1) of Decree-Law No 82 of 14 June 2021;
   c) “NIS Competent National Authority” shall mean the Competent National Authority referred to in Article 10(1) of the NIS Decree;
   d) “NIS Sectoral Authority” shall mean the government bodies referred to in Article 11(1) and (2) of the NIS Decree;
   e) “NIS entity” shall mean any public or private legal entity, as referred to in Article 2(1)(h) of the NIS Decree, that falls within the scope of application of the NIS Decree.
   f) “essential entities” shall mean NIS entities considered essential under the NIS Decree;
   g) “important entities” shall mean NIS subjects considered important under the NIS Decree;
   h) “notification of inclusion in the NIS entity list” shall mean the notification referred to in Article 7(3)(a) of the NIS Decree;

i) “administrative and management bodies” shall mean the administrative and management bodies referred to in Article 23 of the NIS Decree, including, where present, the board of directors of NIS entities;
j) “basic security measures”, shall mean basic specifications for the obligations referred to in Articles 23 and 24 of the NIS Decree, developed by the National Framework and organised into functions, categories, subcategories and requirements;
k) “basic significant incidents” shall mean the basic specifications describing significant incidents as referred to in Article 25 of the NIS Decree;
l) “relevant information and network systems” shall mean information technology and network systems whose compromise would significantly affect the confidentiality, integrity and availability of the activities and services that bring the NIS subject within the scope of the NIS Decree;
m) “providers of domain name registration services” shall mean the providers referred to in Article 2(1)(oo) of the NIS Decree;
n) “top-level domain name registry operators” shall mean the operators referred to in Article 2(1)(pp) of the NIS decree;
o) “PSNC-NIS entities” shall mean the entities referred to in Article 1(2-bis) of Decree-Law No 105 of 2019 considered as NIS entities;
p) “PSNC information and network systems” shall mean information technology and network systems included in the list referred to in Article 1(2)(b) of Decree-Law No 105 of 2019
q) “operators of essential services”, hereinafter referred to as OSE, shall mean NIS entities identified before the effective date of the NIS Decree as operators of essential services under Legislative Decree No 65 of 18 May 2018;
r) “OSE information and network systems” shall mean information technology and network systems of an operator of essential services that are used to provide the essential services for which the operator has been designated under Legislative Decree No 65 of 18 May 2018;
s) “telco operators” shall mean NIS entities that provide public electronic communications networks or publicly accessible electronic communications services under of Legislative Decree No 259 of 1 August 2003 to an equal or greater number of users, or, in alternative:
    1) to 1% of the national user base, calculated based on data published from the Quarterly Communications Observatory by the Communications Regulatory Authority;
    2) to one million;
t) “telco information and network systems” shall mean information technology and network systems that provide access to the fixed or mobile network, either from a workstation or from a mobile terminal, identified as critical by the telco operator, given it is capable of serving, for each of the services indicated:

1) a percentage of users equal to or greater than 1% of the national user base for that service, as determined by data published from the Quarterly Communications Observatory by the Communications Regulatory Authority;
2) to a user base of one million or more.

Article 2
(Adoption of basic specifications)

1. The basic specifications set out in Annexes 1, 2, 3 and 4, which form an integral part of this Determination, are hereby adopted for the initial implementation of the NIS Decree.
2. The basic security measures, for which the administrative and management bodies are responsible, as well as the IT risk management measures, are set out as follows:
   a) for important entities, in Annex 1;
   b) for essential entities, in Annex 2.
3. The basic significant incidents are established:
   a) for important entities, in Annex 3;
   b) for essential entities, in Annex 4.

Article 3
(Deadlines for the adoption of basic specifications)

1. The deadline for adopting the basic security measures set out in Annexes 1 and 2 is eighteen months from the date on which the NIS entity receives notification of its inclusion in the list of NIS entities.
2. The deadline for fulfilling the obligation to notify of the basic significant incidents set out in Annexes 3 and 4 is nine months from the date on which the NIS entity receives notification of its inclusion in the list of NIS entities.

Article 4
(Security, stability and resilience of domain name systems)

1. Without prejudice to the provisions of Article 29 of the NIS Decree, the top-level domain registry operators and providers of domain name registration services shall comply with the provisions of paragraphs 1 and 2 of the Article above,and, within eighteen months of receiving notification of inclusion in the list of NIS entities, adopt and publish the policies and procedures referred to in paragraph 3.

2. The arrangements for compliance with the provisions of Article 29(1) and (2), as well as the policies and procedures referred to in Article 29(3), shall be approved by the administrative and management bodies.
3. In accordance with Article 32(3), top-level domain name registry operators and providers of domain name registration service must implement policies that ensure a level of IT security consistent with the specifications referred to in Annex 1.
4. The administrative and management bodies shall approve the cybersecurity policies referred to in Article 32(3).

Article 5
(Reporting obligations for PSNC-NIS entities)

1. Without prejudice to the provisions of Article 33 of the NIS Decree, PSNC-NIS entities shall notify significant basic incidents referred to in Article 25 of the NIS Decree, under Annex 4, limited to information and network systems other than PSNC ones.
2. The deadline for fulfilling the obligation referred to in paragraph 1 shall run from the date of entry into force of this Determination.

Article 6
(Transitional regime for operators of essential services)

1. Notwithstanding the provisions of Article 2(2) and Article 3(1), operators of essential services, limited to OSE information and network systems, insofar as they do not conflict with the Law and the NIS Decree, shall ensure the preservation of the technical and organisational measures already adopted before the entry into force of the NIS Decree under Legislative Decree No 65 of 18 May 2018.
2. To ensure the continuity of the obligation to notify the incident referred to in Article 12(5) of Legislative Decree No 65 of 18 May 2018, from the entry into force of this Determination, under Article 25 of the NIS Decree, operators of essential services, limited to OSE information and network systems, shall notify the basic significant incidents referred to:
    a) in Annex 3, if these are important entities;
    b) in Annex 4, if these are essential entities.
3. The deadline for complying with this Article shall be the date of entry into force of this Determination.

Article 7

(Transitional regime for telco operators)

1. Notwithstanding the provisions of Article 2(2) and Article 3(1), telco operators, limited to telco information and network systems, insofar as they do not conflict with the Law and the NIS Decree, shall ensure the preservation of the security and integrity measures for networks and services already adopted before the entry into force of the NIS Decree under the Decree of the Minister of Economic Development of 12 December 2018.
2. To ensure the continuity of the obligation to notify the incident referred to in Article 40(3)(b) of Legislative Decree No 259 of 1 August 2003, under Article 25 of the NIS Decree, as of the entry into force of this Determination, telco operators, limited to telco information and network systems, shall notify the basic significant incidents referred to:
    a) in Annex 3, if these are important entities;
    b) in Annex 4, if these are essential entities.
3. For the purposes of paragraph 2, when defining the expected level of service as set out in Annexes 3 and 4, telco operators shall treat the following cases as basic significant incidents:
    a) a duration exceeding one hour and an affected user base greater than fifteen percent of the total national users of the service concerned;
    b) a duration exceeding two hours and an affected user base greater than ten percent of the total national users of the service concerned;
    c) a duration exceeding four hours and an affected user base greater than five percent of the total national users of the service concerned;
    d) a duration exceeding six hours and an affected user base greater than two percent of the total national users of the service concerned;
    e) a duration exceeding eight hours and an affected user base greater than one percent of the total national users of the service concerned;
4. The deadline for complying with this Article shall be the date of entry into force of this Determination.

Article 8
(Financial provisions)

1. This Determination does not give rise to any new or additional burdens on public finances, including within the meaning of Article 12(6) of the NIS Decree.

Article 9
(Advertising)

1. This Determination shall be published on the institutional websites of the National Cybersecurity Agency and the NIS sectoral authorities. Notice shall also be given by publication in the Italian Official Gazette .

Article 10
(Entry into force and transitional provisions)

1. For matters not covered by this Determination, the provisions of the NIS Decree shall apply.
2. This Determination shall enter into force on 30 April 2025.
3. Article 2(2) and (3) and Article 3 shall enter into force on the day following the completion of the procedure for the provision of information under Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015

Rome, *date of protocol*

THE DIRECTOR GENERAL
Bruno Frattasi

National Cybersecurity Agency

1. ANNEX 1

Basic security measures for important entities

1. GOVERNMENT (GOVERN)

1.1. **Organisational context (GV.OC)**: The context – mission, stakeholder expectations, dependencies, and legal, regulatory and contractual requirements – affecting the organisation's cybersecurity risk management decisions shall be understood[1].

1.1.1. **GV.OC-4**: The objectives, capabilities and critical services on which the stakeholders rely on or which they expect from the organisation are understood and communicated.

1. An up-to-date list of relevant information and network systems shall be kept.

1.2. **Risk management strategy (GV.RM)**: The organisation's priorities, constraints, risk tolerance and appetite for risk statements, and assumptions shall be established, communicated and used to support operational risk decisions.

1.2.1. **GV.RM-03**: Cybersecurity risk management activities and outcomes are an integral part of the organisation's risk management processes.

1. As part of the NIS entity's risk management processes, and in compliance with the policies set out in measure GV.PO-01, an IT security risk management plan, shall be defined, implemented, updated and documented to identify, analyse, assess, treat and monitor risks.

1.3. **Roles, responsibilities and related powers (GV.RR)**: Roles, responsibilities and related powers in cybersecurity to promote accountability, performance evaluation and continuous improvement shall be established and communicated.

1.3.1. **GV.RR-02**: Roles, responsibilities, and the corresponding powers related to cybersecurity risk management shall be established, communicated, understood, and enforced.

1. The IT security organisation shall be defined and approved by the administrative and management bodies, and made known to the competent bodies of the relevant NIS entity, and its roles and responsibilities shall be established.

[1] For the sake of consistency with the titles of the categories and subcategories of the National Framework, the terms “cybersecurity” and “organisation” have been retained. In the context of this Annex, these terms – except for the IT security organisation – are to be understood as equivalent to “IT security” and “NIS entity”, respectively.

2. An up-to-date list of the organisation's personnel referred to in point 1, including their specific roles and responsibilities, shall be maintained and made available to the relevant NIS entity.
3. The IT security organisation referred to in point 1 shall include the designated point of contact and at least one deputy, as provided for in the Determination issued pursuant to Section 7(6) of the NIS Decree.
4. The roles and responsibilities referred to in point 1 shall be reviewed and, if appropriate, updated periodically and, at least, every two years, as well as in the event of significant incidents, organisational changes or changes in exposure to threats and related risks.

1.3.2. **GV.RR-04**: Cybersecurity shall be included in human resources practices.

1. For at least the relevant information and network systems, access shall be granted only to personnel who have been identified following an assessment of their experience, capabilities, and reliability, and who provide appropriate assurances of full compliance with IT security regulations.
2. The system administrators of the information and network systems who have been identified following an assessment of their experience, capabilities and reliability,and who provide appropriate assurances of full compliance with IT security regulations.
3. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 1 and 2 shall be adopted and documented.

1.4. **Policy(GV.PO)**: The organisation's cybersecurity policy shall be established, communicated and enforced.

1.4.1. **GV.PO-01**: The cybersecurity risk management policy shall be established based on the organisational context, cybersecurity strategy, and priorities and shall be communicated and enforced.

1. IT security policies shall be adopted and documented for at least the following areas:
   a) risk management;
   b) roles and responsibilities;.
   c) reliability of human resources;.
   d) compliance and security audits;
   e) supply chain IT risk management;
   f) asset management;
   g) vulnerability management;
   h) business continuity, disaster recovery and crisis management;
   i) management of authentication, digital identities and access control;
   j) physical security;

k) staff training and awareness;
l) data security;
m) development, configuration, maintenance and decommissioning of information and network systems;
n) protection of networks and communications;
o) monitoring of security-related events,
p) incident response and recovery.

2. For the areas referred to in point 1, policies shall include, at least, the requirements set out in Table 1 of the Appendix to this Annex.
3. The administrative and management bodies shall approve the policies referred to in point 1.

1.4.2. **GV.PO-02**: The cybersecurity risk management policy shall be reviewed, updated, communicated and enforced to reflect changes in the organisation's requirements, threats, technology and mission.

1. The policies referred to in measure GV.PO-01 shall be reviewed and, if appropriate, updated periodically and at least annually, as well as in the event of changes in the IT security regulatory environment, significant incidents, organisational changes or changes in exposure to threats and related risks.
2. For the review referred to in point 1, verification shall include, at least, the compliance of the policies under measure GV.PO-01 with applicable IT security legislation.

1.5. **Supply Chain cybersecurity risk management (GV.SC):** supply chain cybersecurity risk management processes shall be identified, established, managed, monitored and improved by the organisation's stakeholders.

1.5.1. **GV.SC-01**: The supply chain cybersecurity risk management programme, strategy, objectives, policies and processes shall be established and accepted by the organisation's stakeholders.

1. With regard to the awarding of supplies that may affect the security of information and network systems – including through the use of central purchasing bodies as referred to in Article 1(1)(i) of Legislative Decree No 36 of 31 March 2023 – the following provisions shall apply:
   a) measure GV.RR-02 requires the involvement of the IT security organisation throughout the procurement process, beginning with the identification and design phase;
   b) in accordance with the risk assessment results associated with the procurement process, as referred to in measure GV.SC-07, security requirements are defined for

the procurement processes that are consistent with the security measures applied by the NIS entity to its information and network systems.

1.5.2. **GV.SC-02**: Cybersecurity roles and responsibilities for suppliers, customers and partners shall be established, communicated and coordinated internally and externally.

1. Within the framework of the IT security organisation referred to in measure GV.RR-02, any IT security roles and responsibilities assigned to the personnel of third parties shall be defined and made known to the competent bodies of the relevant NIS entity.
2. The personnel referred to in point 1 with specific roles and responsibilities are included in point 2 of measure GV.RR-02.

1.5.3. **GV.SC-04**: Suppliers are identified and prioritised based on criteria related to critical aspects.

1. An up-to-date inventory of suppliers whose procurement have a potential impact on the security of information and network systems shall be maintained, which includes at least:
   a) the contact details of the contact person in charge of the procurement process;
   b) the type of provision.

1.5.4. **GV.SC-05**: Requirements for addressing cybersecurity risks in the supply chain shall be established, prioritised and integrated into contracts and other types of agreements with providers and other relevant third parties.

1. Unless justified and documented for regulatory or technical reasons, the security requirements of measure GV.SC-01, point 1(b) shall be included in requests for tenders, invitations to tender, contracts, agreements and conventions relating to supplies with a potential impact on the security of information and network systems.

1.5.5. **GV.SC-07**: The risks a provider poses, as a result of its products and services, and as a result of other third parties shall be understood, recorded, prioritised, assessed, dealt with, and monitored during the relationship.

1. The risk associated with supplies shall be assessed and documented as part of the risk assessment under measure ID.RA-05. To this end, at least the following shall be assessed:
   a) the provider's level of access to the NIS entity's information and network systems;
   b) the supplier's access to intellectual property and data, also assessed according to their criticality;
   c) the impact of a major procurement disruption;
   d) the time and cost of recovery in the event of unavailability of services;
   e) the provider’s roles and responsibilities in relation to the governance of information and network systems.

2. Compliance with the requirements set out in measure GV.SC-05 shall be periodically verified and documented.

2. IDENTIFICATION (IDENTIFY)

2.1. **Asset management (ID.AM):** The assets (e.g. data, hardware, software, systems, infrastructure, services, personnel) that enable the organisation to achieve its business objectives shall be identified and managed consistently with their importance in terms of the organisation's objectives and risk strategy.

2.1.1. **ID.AM-01**: Inventories of hardware managed by the organisation shall be maintained.

1. An up-to-date inventory of the physical equipment (hardware) composed of the information and network systems, including IT, IoT, OT and mobile devices, approved by internal NIS entities, shall be maintained.

2.1.2. **ID.AM-02**: Inventories of software, services and systems managed by the organisation shall be maintained.

1. An up-to-date inventory of the services, systems, and software applications that compose the information and network systems, including commercial, open-source, and custom applications, also accessible via APIs and approved by internal NIS entities, shall be maintained.

2.1.3. **ID.AM-04**: Inventories of services delivered by providers shall be maintained.

1. An up-to-date inventory of IT services delivered by providers, including cloud services, shall be maintained.

2.2. **Risk assessment (ID.RA)**: This includes the cybersecurity risk to which the organisation, its assets and personnel are exposed.

2.2.1. **ID.RA-01**. Vulnerabilities in assets shall be identified, confirmed and recorded.

1. The information set out in point 1 of the measure ID.RA-08 shall be used to identify possible vulnerabilities in the information and network systems.

2.2.2. **ID.RA-05**: Threats, vulnerabilities, probabilities and impacts shall be used to understand the inherent risk and to support the prioritisation of risk response measures.

1. In accordance with the IT security risk management plan referred to in measure GV.RM-03, a risk assessment concerning the security of information and network systems shall be conducted and documented. This also covers any dependencies on third-party suppliers and partners and includes at least:
   a) identification of risk;

b) risk analysis;
c) the weighting of risk.

2. The risk assessment referred to in point 1 shall be conducted at planned intervals and at least, every two years, as well as in the event of significant incidents, organisational changes or changes in exposure to threats and related risks.
3. The administrative and management bodies shall approve the risk assessment referred to in point 1.

2.2.3. **ID.RA-06**: Risk responses shall be chosen, prioritised, planned, monitored and communicated.

1. A treatment plan addressing risks shall be defined, documented, executed and monitored, and shall include, at least:
   a) the treatment options and measures to be implemented for the treatment of each identified risk, along with their priorities;
   b) the designation of competent bodies for the implementation of risk treatment measures and the time frame for such implementation;
   c) the description and reasons justifying the acceptance of any residual risks related to the treatment.
2. Where, for duly justified and documented regulatory or technical reasons, the requirements set out in Table 2 of the Appendix to this Annex are not implemented, compensatory mitigation measures shall be adopted, where applicable. These measures, along with any associated residual risks, shall be included in the plan referred to in point 1.
3. The plan referred to in point 1, including any decisions to accept residual risks, shall be approved by the administrative and management bodies.

2.2.4. **ID.RA-08**: Processes shall be established for receiving, analysing and responding to disclosures of vulnerabilities.

1. The communication channels of CSIRT Italy, as well as those of any relevant sectoral CERTs and Information Sharing and Analysis Centres (ISAC), shall be monitored, at least, to acquire, analyse, and respond to information on vulnerabilities.
2. Vulnerabilities, including those identified in accordance with measure ID.RA-01, shall be promptly addressed through security updates or mitigation measures, where available, or by accepting and documenting the risk following the treatment plan addressing IT risks under measure ID.RA-06.
3. A management plan addressing vulnerabilities shall be defined, implemented, updated and documented, including, at least:

a) the arrangements for the identification of vulnerabilities under measure ID.RA-01 and the corresponding planning of activities;
b) the arrangements to monitor, receive, analyse and respond to information on vulnerabilities;
c) the procedures, roles, and responsibilities for conducting the activities under (a) and (b).

4. The administrative and management bodies shall approve the plan referred to in point 3.

2.3. **Improvement (ID.IM)**: Improvements to the organisation's cybersecurity risk management processes, procedures and activities shall be identified in all functions of the framework.

2.3.1. **ID.IM-01**: Improvements shall be identified as a result of the assessments.

1. Following the review outcome referred to in point 1 of measure GV.PO-02, an adaptation plan shall be defined, implemented, documented, and approved by the administrative and management bodies. The plan shall identify the actions necessary to ensure the implementation of security policies.
2. The administrative and management bodies shall be kept informed of the results of the plans referred to in point 1 through regular reports.

2.3.2. **ID.IM-04**: Response plans addressing incidents and other cybersecurity plans that impact operations shall be established, communicated, maintained and improved.

1. For at least the relevant information and network systems, a business continuity plan shall be defined, implemented, updated and documented, including, at least:
   a) the purpose and scope;
   b) the roles and responsibilities;
   c) the main contacts and communication channels (internal and external);
   d) the conditions for activating and deactivating the plan;
   e) the necessary resources, including backups and redundancies.
2. For at least the relevant information and network systems, a disaster recovery plan shall be defined, implemented, updated and documented, including, at least:
   a) the purpose and scope;
   b) the roles and responsibilities;
   c) the main contacts and communication channels (internal and external);
   d) the conditions for activating and deactivating the plan;
   e) the necessary resources, including backups and redundancies;
   f) the order of resumption of operations;
   g) recovery procedures for specific operations, including recovery targets.

3. For at least the relevant information and network systems, a crisis management plan shall be defined, implemented, updated and documented, including, at least:
   a) the roles and responsibilities of personnel and, where appropriate, providers, specifying the allocation of roles in crises, including specific procedures to be followed;
   b) the procedures governing communication between the entities and the competent authorities.
4. The administrative and management bodies shall approve the plans in points 1, 2 and 3.
5. The plans referred to in point 1, 2 and 3 shall be reviewed and, if appropriate, updated periodically and, at least, every two years, as well as in the event of significant incidents or changes in exposure to threats and related risks.

3. PROTECTION (PROTECT)

3.1. **Identity management, authentication and access control (PR.AA)**: Access to physical and logical assets shall be restricted to authorised users, services, and hardware, and managed in accordance with the risk assessment of unauthorised access..

3.1.1. **PR.AA-01**: The organisation shall manage the identities and credentials of authorised users, services and hardware.

1. All utilities, including those with administrative privileges and those used for remote access, shall be surveyed and approved by internal NIS entities. Where justified and documented by technical reasons and based on the outcomes of the risk assessment conducted under measure ID.RA-05, utilities are assigned on an individual basis to users.
2. The credentials (e.g. user name and password) for users shall be robust and updated following the outcome of the risk assessment conducted under measure ID.RA-05.
3. For at least the relevant information and network systems, user identities and their associated access rights shall be periodically reviewed and updated/revoked in the event of changes (e.g. personnel transfer or termination of personnel).
4. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 1, 2 and 3 shall be adopted and documented.

3.1.2. **PR.AA-03**: Users, services and hardware shall be authenticated.

1. User authentication procedures for accessing information and network systems shall be commensurate with the associated risk. To this end, at least the following risks shall be assessed:
   a) associated to user privileges;

b) associated to the criticality of information and network systems;
c) the type of operations that users can perform on IT and network systems.

2. Multi-factor authentication methods shall be used for at least the relevant information and network systems, following the outcome of the risk assessment conducted under measure ID.RA-05.
3. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 1 and 2 shall be adopted and documented.

3.1.3. **PR.AA-05**: Access permissions, rights and authorisations shall be defined in policy. These shall be managed, enforced and reviewed; furthermore, they shall incorporate the principles of least privilege and separation of duties.

1. Permissions shall be granted to users in accordance with the principle of minimum privilege and separation of duties, also considering the need-to-know basis.
2. A complete distinction shall be ensured between users with and without system administrator privileges, with different credentials assigned accordingly.
3. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 1 and 2 shall be adopted and documented.

3.1.4. **PR.AA-06**: Physical access to assets shall be managed, monitored, and implemented in a manner commensurate with the associated risk.

1. Protection measures shall be in place for physical access to at least the relevant information and network systems.
2. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 1 shall be adopted and documented.

3.2. **Awareness and training (PR.AT)**: Personnel shall be made aware of and trained in cybersecurity to effectively carry out their roles and responsibilities related to cybersecurity.

3.2.1. **PR.AT-01**: Staff shall be made aware and trained to possess the knowledge and skills necessary to perform general tasks, taking cybersecurity risks into account.

1. An IT security training plan for personnel, including administrative and management bodies, shall be defined, implemented, updated and documented, which shall include at least:
   a) the scheduling of planned training activities with details of the training content delivered;
   b) any procedures used to verify the acquisition of content.
2. The administrative and management bodies shall approve the training plan referred to in point 1.

3. An up-to-date register shall be maintained, listing the employees who have completed the training referred to in point 1, the training content and the list of assessments conducted, where applicable.

3.3. **Data security (PR.DS)**: Data shall be managed consistently with the organisation's risk strategy to ensure the confidentiality, integrity, and availability of information.

3.3.1. **PR.DS-01**: Data confidentiality, integrity and availability of data at rest shall be protected.

1. This shall apply to, at least, the relevant information and network systems and shall be based on the outcome of the risk assessment under measure ID.RA-05. Subject to justified and documented regulatory or technical reasons, data stored on portable devices – including laptops, smartphones, and tablets – and on removable media shall be encrypted using state-of-the-art protocols and algorithms and deemed secure.
2. Unless otherwise justified regulatory or technical reasons, the automatic execution of removable media shall be disabled, and removable media shall be scanned for malicious code prior to use within information and network systems.
3. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 1 and 2 shall be adopted and documented.

3.3.2. **PR.DS-02**: Data confidentiality, integrity and availability of data in transit shall be protected.

1. For at least the relevant information and network systems – including voice, video and text communication systems – and in accordance with the results of the risk assessment under measure ID.RA-05, including voice, video and text communication systems, except for justified and documented regulatory or technical reasons, state-of-the-art encryption protocols and algorithms considered secure shall be used for the transmission of data to and from outside the NIS entity.
2. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 1 shall be adopted and documented.

3.3.3. **PR.DS-11**: Data backups shall be created, protected, maintained and verified.

1. In accordance with the operational continuity and disaster recovery stipulations specified in the documentation referenced under measure ID.IM-04, data and configurations shall be routinely backed up, and offline backup copies shall be retained for at least the relevant information and network systems.
2. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 1 shall be adopted and documented.

3.4. **Platform security (PR.PS)**: Hardware, software (e.g. firmware, operating systems, applications) and services across both physical and virtual platforms shall be managed consistently in accordance with the organisation's risk strategy to protect their confidentiality, integrity and availability.

3.4.1. **PR.PS-02**: Software shall be maintained, replaced and removed based on the risk implications.

1. Except where justified and documented for regulatory or technical reasons, only software – including operating systems –for which the availability of security updates shall be guaranteed.
2. Except for justified and documented regulatory or technical reasons, the latest security updates released by the manufacturer shall be installed without undue delay, in accordance with the vulnerability management plan under measure ID.RA-08.
3. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 1 and 2 shall be adopted and documented.

3.4.2. **PR.PS-04**: Logs shall be generated and made available for continuous monitoring.

1. All remote access activities, particularly those performed by users with administrative privileges, shall be logged.
2. For at least the relevant information and network systems, the logs necessary for monitoring security events – including those related to access under point 1 – shall be securely stored and, where possible, centralised.
3. In accordance with the outcomes of the risk assessment under measure ID.RA-05, the retention period for the logs referred to above shall be defined and documented.
4. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 1 and 2 shall be adopted and documented.

3.4.3. **PR.PS-06**: Safe software development practices shall be integrated, and their performance shall be monitored throughout the entire software life cycle.

1. Safe code development practices in software development shall be adopted and documented.

3.5. **Resilience of technological infrastructure (PR.IR):** Security architectures shall be managed by the organisation's risk strategy to protect the confidentiality, integrity, and availability of assets and enhance organisational resilience.

3.5.1. **PR.IR-01**: Networks and environments shall be protected against unauthorised access and use.

1. Remote access activities for at least the relevant information and network systems shall be defined, documented, and secured through appropriate access control measures.
2. An up-to-date list of information and network systems accessible remotely shall be maintained, including details of the access methods.
3. Perimeter systems such as firewalls shall be deployed, updated, maintained and configured.
4. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 1, 2 and 3 shall be adopted and documented.

4. DETECTION (DETECT)

4.1. **Continuous monitoring (DE.CM)**: Assets shall be monitored for anomalies, indicators of impairment and other potentially adverse events.

4.1.1. **DE.CM-01**: Networks and network services shall be monitored for potentially adverse events.

1. For at least the relevant information and network systems, appropriate technical tools shall be deployed, configured, updated, and maintained to ensure the prompt detection of significant incidents.
2. The expected service levels (SLs) associated with the NIS entity's services and activities shall be defined and documented to support the early identification of significant incidents.
3. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 1 and 2 shall be adopted and documented.

4.1.2. **DE.CM-09**: Processing hardware, software, runtime environments and their associated data shall be monitored for potentially adverse events.

1. Except for justified and documented regulatory or technical reasons, endpoint protection systems for detecting malicious code shall be deployed, updated, maintained and properly configured.
2. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 1 shall be adopted and documented.

5. REPLY (RESPOND)

5.1. **Incident management (RS.MA)**: Responses to detected cybersecurity incidents shall be managed.

5.1.1. **RS.MA-01**: The incident response plan shall be activated in coordination with the relevant third parties once an incident is declared.

1. A plan for the management of IT security incidents and notification to CSIRT Italia, in accordance with Article 25 of the NIS Decree, shall be defined, implemented, updated, and documented. The plan shall include, at least:
   a) the procedures and steps for handling and reporting incidents, with clearly defined roles and responsibilities;
   b) the procedures for preparing and submitting the reports referred to in Article 25(5)(c), (d), and (e) of the NIS Decree;
   c) contact details for reporting incidents;
   d) internal communication procedures, including the escalation to administrative and management bodies, and protocols for external communication;
   e) the reports to be used for documenting the incident.
2. The administrative and management bodies shall approve the plan referred to in point 1.
3. The plans referred to in point 1 shall be reviewed and, if appropriate, updated periodically and, at least, every two years, as well as in the event of significant incidents, incorporating relevant lessons learned, or changes in exposure to threats and related risks.

5.2. **Reporting and communication of incident response (RS.CO)**: Response activities shall be coordinated with internal and external stakeholders, as required by applicable laws, regulations, or organisational policies.

5.2.1. **RS.CO-02**: Internal and external stakeholders shall be informed of any incidents.

1. Based on the incident management plan referred to in measure RS.MA-01, procedures shall be adopted and documented to ensure timely communication – without undue delay, where appropriate and feasible – after consultation with CSIRT Italy or when mandated by the National Cybersecurity Agency pursuant to Article 37(3)(g) and (h) of the NIS Decree:
   a) to the recipients of their services, regarding significant incidents that may adversely affect the provision of those services;
   b) to the recipients of services potentially affected by a significant IT threat, including the nature of the threat and the corrective or mitigating measures or actions they may take in response.
2. Procedures shall also be adopted and documented to inform the public of the incidents that took place, if so, directed by the National Cybersecurity Agency under Article 37(3)(i) of the NIS Decree.

6. RESTORATION (RECOVER)

6.1. **Execution of the Accident Recovery Plan (RC.RP)**: Recovery activities shall be performed to ensure the operational availability of systems and services affected by cybersecurity incidents.

6.1.1. **RC.RP-01**: The recovery phase of the incident response plan shall be initiated once the incident response process has commenced.

1. As part of the incident management plan under measure RS.MA-01, recovery procedures shall be defined and documented with the aim of restoring, at least, the normal operation of information and network systems affected by IT security incidents, including those referred to in Article 25 of the NIS Decree.

Appendix

Table 1: Requirements referred to in point 2 of measure GV.PO-01.

Policy areas	Requirements
a) Risk management.	GV.OC-04: point 1. GV.RM-03: point 1. ID.RA-05: points 1, 2 and 3. ID.RA-06: points 1, 2 and 3.
b) Roles and responsibilities.	GV.RR-02: points 1, 2, 3 and 4.
c) Reliability of human resources.	GV.RR-04: points 1 and 2.
d) Compliance and security audits.	GV.PO-01: points 1, 2 and 3. GV.PO-02: points 1 and 2. ID.IM-01: points 1 and 2.
e) Management of IT security risks in the supply chain	GV.SC-01: point 1. GV.SC-02: point 1. GV.SC-04: point 1. GV.SC-05: point 1. GV.SC-07: points 1 and 2.
f) Asset management.	ID.AM-01: point 1. ID.AM-02: point 1. ID.AM-04: point 1.
g) Vulnerability management.	ID.RA-01: point 1. ID.RA-08: points 1, 2, 3 and 4.
h) Business continuity, disaster recovery and crisis management.	ID.IM-04: points 1, 2, 3, 4 and 5.
i) Management of authentication, digital identities and access control.	PR.AA-01: points 1, 2 and 3. PR.AA-03: points 1 and 2. PR.AA-05: points 1 and 2. PR.IR-01: points 1 and 2.

Policy areas	Requirements
j) Physical Security	PR.AA-06: point 1.
k) Staff training and awareness.	PR.AT-01: points 1, 2 and 3.
l) Data security.	PR.DS-01: points 1 and 2. PR.DS-02: point 1. PR.DS-11: point 1.
m) Development, configuration, maintenance and decommissioning of information and network systems.	PR.PS-02: points 1, 2. PR.PS-04: points 1, 2 and 3. PR.PS-06: point 1.
n) Protection of networks and communications.	PR.IR-01: point 3.
o) Monitoring of security events.	DE.CM-01: points 1 and 2. DE.CM-09: point 1.
p) Incident response and recovery.	RS.MA-01: points 1, 2 and 3. RS.CO-02: points 1 and 2. RC.RP-01: point 1.

Table 2: Requirements specified in point 2 of measure ID.RA-06.

Requirements
GV.SC-05: point 1.
PR.AA-01: point 1.
PR.DS-01: points 1 and 2.
PR.DS-02: point 1.
PR.PS-02: points 1 and 2.
DE.CM-09: point 1.

2. ANNEX 2

Basic security measures for essential entities

7. GOVERNMENT (GOVERN)

7.1. **Organisational context (GV.OC)**: The context – mission, stakeholder expectations, dependencies, and legal, regulatory and contractual requirements – affecting the organisation's cybersecurity risk management decisions shall be understood[2].

7.1.1. **GV.OC-4**: The objectives, capabilities and critical services on which the stakeholders rely on or which they expect from the organisation are understood and communicated.

1. An up-to-date list of relevant information and network systems shall be kept.

7.2. **Risk management strategy (GV.RM)**: The organisation's priorities, constraints, risk tolerance and appetite for risk statements, and assumptions shall be established, communicated and used to support operational risk decisions.

7.2.1. **GV.RM-03**: Cybersecurity risk management activities and outcomes are an integral part of the organisation's risk management processes.

1. As part of the NIS entity's risk management processes, and in compliance with the policies set out in measure GV.PO-01, an IT security risk management plan, shall be defined, implemented, updated and documented to identify, analyse, assess, treat and monitor risks.

7.3. **Roles, responsibilities and related powers (GV.RR)**: Roles, responsibilities and related powers in cybersecurity to promote accountability, performance evaluation and continuous improvement shall be established and communicated.

7.3.1. **GV.RR-02**: Roles, responsibilities, and the corresponding powers related to cybersecurity risk management shall be established, communicated, understood, and enforced.

1. The IT security organisation shall be defined and approved by the administrative and management bodies, and made known to the competent bodies of the relevant NIS entity, and its roles and responsibilities shall be established.

[2] For the sake of consistency with the titles of the categories and subcategories of the National Framework, the terms “cybersecurity” and “organisation” have been retained. In the context of this Annex, these terms – except for the IT security organisation – are to be understood as equivalent to “IT security” and “NIS entity”, respectively.

2. An up-to-date list of the organisation's personnel referred to in point 1, including their specific roles and responsibilities, shall be maintained and made available to the relevant NIS entity.
3. The IT security organisation referred to in point 1 shall include the designated point of contact and at least one deputy, as provided for in the Determination issued pursuant to Section 7(6) of the NIS Decree.
4. The roles and responsibilities referred to in point 1 shall be reviewed and, if appropriate, updated periodically and, at least, every two years, as well as in the event of significant incidents, organisational changes or changes in exposure to threats and related risks.

7.3.2. **GV.RR-04**: Cybersecurity shall be included in human resources practices.

1. For at least the relevant information and network systems, access shall be granted only to personnel who have been identified following an assessment of their experience, capabilities, and reliability, and who provide appropriate assurances of full compliance with IT security regulations.
2. The system administrators of the information and network systems who have been identified following an assessment of their experience, capabilities and reliability,and who provide appropriate assurances of full compliance with IT security regulations.
3. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 1 and 2 shall be adopted and documented.
4. This is due to the risk assessment outcome as set out in measure ID.RA-05, any obligations in the area of IT security that remain valid after the termination or change of the employment relationship of the employees of the NIS entity (e.g. by including confidentiality clauses) are defined at the contractual level.
5. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 4 shall be adopted and documented.

7.4. **Policy (GV.PO)**: The organisation's cybersecurity policy shall be established, communicated and enforced.

7.4.1. **GV.PO-01**: The cybersecurity risk management policy shall be established based on the organisational context, cybersecurity strategy, and priorities and shall be communicated and enforced.

1. IT security policies shall be adopted and documented for at least the following areas:
   a) risk management;
   b) roles and responsibilities;
   c) reliability of human resources;
   d) compliance and security audits;

e) supply chain IT risk management;
f) asset management;
g) vulnerability management;
h) business continuity, disaster recovery and crisis management;
i) management of authentication, digital identities and access control;
j) physical security;
k) staff training and awareness;
l) data security;
m) development, configuration, maintenance and decommissioning of information and network systems;
n) protection of networks and communications;
o) monitoring of security-related events,
p) incident response and recovery.

2. For the areas referred to in point 1, policies shall include, at least, the requirements set out in Table 1 of the Appendix to this Annex.
3. The administrative and management bodies shall approve the policies referred to in point 1.

7.4.2. **GV.PO-02**: The cybersecurity risk management policy shall be reviewed, updated, communicated and enforced to reflect changes in the organisation's requirements, threats, technology and mission.

1. The policies referred to in measure GV.PO-01 shall be reviewed and, if appropriate, updated periodically and at least annually, as well as in the event of changes in the IT security regulatory environment, significant incidents, organisational changes or changes in exposure to threats and related risks.
2. For the review referred to in point 1, verification shall include, at least, the compliance of the policies under measure GV.PO-01 with applicable IT security legislation.
3. An up-to-date register containing the outcome of the review in point 1 shall be maintained.

7.5. **Supply Chain cybersecurity risk management (GV.SC):** supply chain cybersecurity risk management processes shall be identified, established, managed, monitored and improved by the organisation's stakeholders.

7.5.1. **GV.SC-01**: The supply chain cybersecurity risk management programme, strategy, objectives, policies and processes shall be established and accepted by the organisation's stakeholders.

1. With regard to the awarding of supplies that may affect the security of information and network systems – including through the use of central purchasing bodies as referred to in Article 1(1)(i) of Legislative Decree No 36 of 31 March 2023 – the following provisions shall apply:
   a) measure GV.RR-02 requires the involvement of the IT security organisation throughout the procurement process, beginning with the identification and design phase;
   b) in accordance with the risk assessment results associated with the procurement process, as referred to in measure GV.SC-07, security requirements are defined for the procurement processes that are consistent with the security measures applied by the NIS entity to its information and network systems.
2. For the safety requirements under 1(b), at least the following areas shall be considered, where applicable:
   a) reliability of suppliers, taking into account at least their specific vulnerabilities (if any), the overall quality of their products and cybersecurity practices – particularly concerning the subject matter of the procurement – their ability to ensure provisioning, support, and maintenance over time, and, where applicable, the results of coordinated security risk assessments of critical supply chains conducted by the NIS Cooperation Group;
   b) roles and responsibilities in the procurement process;
   c) reliability of human resources;
   d) compliance and security audits;
   e) vulnerability management;
   f) business continuity and disaster recovery;
   g) management of authentication, digital identities and access control;
   h) physical security;
   i) staff training and awareness;
   j) data security;
   k) protection of networks and communications;
   l) monitoring of security events, including access and activity;
   m) incident management and reporting;
   n) safe code development and security by design and by default;
   o) routine and evolutionary maintenance, including security updates;
   p) termination of the provision, including the return and deletion of data;
   q) subcontracting, sub-provision or related potential security requirements along the supply chain.

7.5.2. **GV.SC-02**: Cybersecurity roles and responsibilities for suppliers, customers and partners shall be established, communicated and coordinated internally and externally.

1. Within the framework of the IT security organisation referred to in measure GV.RR-02, any IT security roles and responsibilities assigned to the personnel of third parties shall be defined and made known to the competent bodies of the relevant NIS entity.
2. The personnel referred to in point 1 with specific roles and responsibilities are included in point 2 of measure GV.RR-02.

7.5.3. **GV.SC-04**: Suppliers are identified and prioritised based on criteria related to critical aspects.

1. An up-to-date inventory of suppliers whose procurement have a potential impact on the security of information and network systems shall be maintained, which includes at least:
   a) the contact details of the contact person in charge of the procurement process;
   b) the type of provision.

7.5.4. **GV.SC-05**: Requirements for addressing cybersecurity risks in the supply chain shall be established, prioritised and integrated into contracts and other types of agreements with providers and other relevant third parties.

1. Unless justified and documented for regulatory or technical reasons, the security requirements of measure GV.SC-01, point 1(b) shall be included in requests for tenders, invitations to tender, contracts, agreements and conventions relating to supplies with a potential impact on the security of information and network systems.

7.5.5. **GV.SC-07**: The risks a provider poses, as a result of its products and services, and as a result of other third parties shall be understood, recorded, prioritised, assessed, dealt with, and monitored during the relationship.

1. The risk associated with supplies shall be assessed and documented as part of the risk assessment under measure ID.RA-05. To this end, at least the following shall be assessed:
   a) the provider's level of access to the NIS entity's information and network systems;
   b) the supplier's access to intellectual property and data, also assessed according to their criticality;
   c) the impact of a major procurement disruption;
   d) the time and cost of recovery in the event of unavailability of services;
   e) the provider’s roles and responsibilities in relation to the governance of information and network systems.
2. Compliance with the requirements set out in measure GV.SC-05 shall be periodically verified and documented.

8. IDENTIFICATION (IDENTIFY)

8.1. **Asset management (ID.AM):** The assets (e.g. data, hardware, software, systems, infrastructure, services, personnel) that enable the organisation to achieve its business objectives shall be identified and managed consistently with their importance in terms of the organisation's objectives and risk strategy.

8.1.1. **ID.AM-01**: Inventories of hardware managed by the organisation shall be maintained.

1. An up-to-date inventory of the physical equipment (hardware) composed of the information and network systems, including IT, IoT, OT and mobile devices, approved by internal NIS entities, shall be maintained.

8.1.2. **ID.AM-02**: Inventories of software, services and systems managed by the organisation shall be maintained.

1. An up-to-date inventory of the services, systems, and software applications that compose the information and network systems, including commercial, open-source, and custom applications, also accessible via APIs and approved by internal NIS entities, shall be maintained.

8.1.3. **ID.AM-03**: Network communications and internal and external network data flows authorised by the organisation shall be maintained.

1. An up-to-date inventory of network flows between the NIS entity's information and network systems and the outside world, approved by internal stakeholders of the NIS entity, shall be maintained.

8.1.4. **ID.AM-04**: Inventories of services delivered by providers shall be maintained.

1. An up-to-date inventory of IT services delivered by providers, including cloud services, shall be maintained.

8.2. **Risk assessment (ID.RA)**: This includes the cybersecurity risk to which the organisation, its assets and personnel are exposed.

8.2.1. **ID.RA-01**. Vulnerabilities in assets shall be identified, confirmed and recorded.

1. The information set out in point 1 of the measure ID.RA-08 shall be used to identify possible vulnerabilities in the information and network systems.
2. For at least the relevant information and network systems, and subject to justified and documented regulatory or technical reasons, the vulnerability management plan under measure ID.RA-08 shall ensure that vulnerability identification activities – including, at least, vulnerability assessments and/or penetration testing – are conducted periodically and, in any case, prior to commissioning.

3. The activities referred to in point 2 shall be documented by means of reports containing, at least:
   a) a general description of the activities conducted and their outcomes;
   b) the description of the vulnerabilities detected and their level of impact on security.

8.2.2. **ID.RA-05**: Threats, vulnerabilities, probabilities and impacts shall be used to understand the inherent risk and to support the prioritisation of risk response measures.

1. In accordance with the IT security risk management plan referred to in measure GV.RM-03, a risk assessment concerning the security of information and network systems shall be conducted and documented. This also covers any dependencies on third-party suppliers and partners and includes at least:
   a) identification of risk;
   b) risk analysis;
   c) the weighting of risk.
2. The risk assessment referred to in point 1 shall be conducted at planned intervals and at least, every two years, as well as in the event of significant incidents, organisational changes or changes in exposure to threats and related risks.
3. The administrative and management bodies shall approve the risk assessment referred to in point 1.
4. The risk assessment referred to in point 1 considers at least the internal and external threats, unresolved vulnerabilities, and impacts resulting from any incidents.

8.2.3. **ID.RA-06**: Risk responses shall be chosen, prioritised, planned, monitored and communicated.

1. A treatment plan addressing risks shall be defined, documented, executed and monitored, and shall include, at least:
   a) the treatment options and measures to be implemented for the treatment of each identified risk, along with their priorities;
   b) the designation of competent bodies for the implementation of risk treatment measures and the time frame for such implementation;
   c) the description and reasons justifying the acceptance of any residual risks related to the treatment.
2. Where, for duly justified and documented regulatory or technical reasons, the requirements set out in Table 2 of the Appendix to this Annex are not implemented, compensatory mitigation measures shall be adopted, where applicable. These measures, along with any associated residual risks, shall be included in the plan referred to in point 1.

3. The plan referred to in point 1, including any decisions to accept residual risks, shall be approved by the administrative and management bodies.

8.2.4. **ID.RA-08**: Processes shall be established for receiving, analysing and responding to disclosures of vulnerabilities.

1. The communication channels of CSIRT Italy, as well as those of any relevant sectoral CERTs and Information Sharing and Analysis Centres (ISAC), shall be monitored, at least, to acquire, analyse, and respond to information on vulnerabilities.
2. Vulnerabilities, including those identified in accordance with measure ID.RA-01, shall be promptly addressed through security updates or mitigation measures, where available, or by accepting and documenting the risk following the treatment plan addressing IT risks under measure ID.RA-06.
3. A management plan addressing vulnerabilities shall be defined, implemented, updated and documented, including, at least:
   a) the arrangements for the identification of vulnerabilities under measure ID.RA-01 and the corresponding planning of activities;
   b) the arrangements to monitor, receive, analyse and respond to information on vulnerabilities;
   c) the procedures, roles, and responsibilities for conducting the activities under (a) and (b).
4. The administrative and management bodies shall approve the plan referred to in point 3.
5. For point 1, the channels of software suppliers that are deemed critical shall also be monitored.

8.3. **Improvement (ID.IM)**: Improvements to the organisation's cybersecurity risk management processes, procedures and activities shall be identified in all functions of the framework.

8.3.1. **ID.IM-01**: Improvements shall be identified as a result of the assessments.

1. Following the review outcome referred to in point 1 of measure GV.PO-02, an adaptation plan shall be defined, implemented, documented, and approved by the administrative and management bodies. The plan shall identify the actions necessary to ensure the implementation of security policies.
2. The administrative and management bodies shall be kept informed of the results of the plans referred to in point 1 through regular reports.
3. A plan for evaluating the effectiveness of information security risk management

measures shall be defined, implemented, updated, and documented. This plan shall specify the measures to be assessed and the methods for their evaluation.

4. The administrative and management bodies shall be kept informed of the results of the assessment plan referred to in point 3 through regular reports.

8.3.2. **ID.IM-04**: Response plans addressing incidents and other cybersecurity plans that impact operations shall be established, communicated, maintained and improved.

1. For at least the relevant information and network systems, a business continuity plan shall be defined, implemented, updated and documented, including, at least:
   a) the purpose and scope;
   b) the roles and responsibilities;
   c) the main contacts and communication channels (internal and external);
   d) the conditions for activating and deactivating the plan;
   e) the necessary resources, including backups and redundancies.
2. For at least the relevant information and network systems, a disaster recovery plan shall be defined, implemented, updated and documented, including, at least:
   a) the purpose and scope;
   b) the roles and responsibilities;
   c) the main contacts and communication channels (internal and external);
   d) the conditions for activating and deactivating the plan;
   e) the necessary resources, including backups and redundancies;
   f) the order of resumption of operations;
   g) recovery procedures for specific operations, including recovery targets.
3. For at least the relevant information and network systems, a crisis management plan shall be defined, implemented, updated and documented, including, at least:
   a) the roles and responsibilities of personnel and, where appropriate, providers, specifying the allocation of roles in crises, including specific procedures to be followed;
   b) the procedures governing communication between the entities and the competent authorities.
4. The administrative and management bodies shall approve the plans in points 1, 2 and 3.
5. The plans referred to in point 1, 2 and 3 shall be reviewed and, if appropriate, updated periodically and, at least, every two years, as well as in the event of significant incidents or changes in exposure to threats and related risks.

9. PROTECTION (PROTECT)

9.1. **Identity management, authentication and access control (PR.AA)**: Access to physical and logical assets shall be restricted to authorised users, services, and hardware, and managed in accordance with the risk assessment of unauthorised access..

9.1.1. **PR.AA-01**: The organisation shall manage the identities and credentials of authorised users, services and hardware.

1. All utilities, including those with administrative privileges and those used for remote access, shall be surveyed and approved by internal NIS entities. Where justified and documented by technical reasons and based on the outcomes of the risk assessment conducted under measure ID.RA-05, utilities are assigned on an individual basis to users.
2. The credentials (e.g. user name and password) for users shall be robust and updated following the outcome of the risk assessment conducted under measure ID.RA-05.
3. For at least the relevant information and network systems, user identities and their associated access rights shall be periodically reviewed and updated/revoked in the event of changes (e.g. personnel transfer or termination of personnel).
4. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 1, 2 and 3 shall be adopted and documented.

9.1.2. **PR.AA-03**: Users, services and hardware shall be authenticated.

1. User authentication procedures for accessing information and network systems shall be commensurate with the associated risk. To this end, at least the following risks shall be assessed:
   a) associated to user privileges;
   b) associated to the criticality of information and network systems;
   c) the type of operations that users can perform on information and network systems.
2. Multi-factor authentication methods shall be used for at least the relevant information and network systems, following the outcome of the risk assessment conducted under measure ID.RA-05.
3. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 1 and 2 shall be adopted and documented.

9.1.3. **PR.AA-05**: Access permissions, rights and authorisations shall be defined in policy. These shall be managed, enforced and reviewed; furthermore, they shall incorporate the principles of least privilege and separation of duties.

1. Permissions shall be granted to users in accordance with the principle of minimum privilege and separation of duties, also considering the need-to-know basis.
2. A complete distinction shall be ensured between users with and without system administrator privileges, with different credentials assigned accordingly.

3. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 1 and 2 shall be adopted and documented.

9.1.4. **PR.AA-06**: Physical access to assets shall be managed, monitored, and implemented in a manner commensurate with the associated risk.

1. Protection measures shall be in place for physical access to at least the relevant information and network systems.
2. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 1 shall be adopted and documented.

9.2. **Awareness and training (PR.AT)**: Personnel shall be made aware of and trained in cybersecurity to effectively carry out their roles and responsibilities related to cybersecurity.

9.2.1. **PR.AT-01**: Staff shall be made aware and trained to possess the knowledge and skills necessary to perform general tasks, taking cybersecurity risks into account.

1. An IT security training plan for personnel, including administrative and management bodies, shall be defined, implemented, updated and documented, which shall include at least:
   a) the scheduling of planned training activities with details of the training content delivered;
   b) any procedures used to verify the acquisition of content.
2. The administrative and management bodies shall approve the training plan referred to in point 1.
3. An up-to-date register shall be maintained, listing the employees who have completed the training referred to in point 1, the training content and the list of assessments conducted, where applicable.

9.2.2. **PR.AT-02**. Individuals in specialised roles shall be made aware and trained to possess the knowledge and skills to perform the relevant tasks, taking cybersecurity risks into account.

1. The plan under measure PR.AT-01 provides for dedicated training for personnel in specialised roles – those requiring a range of security-related skills and competencies, including system administrators – and includes at least the following:
   a) instructions on the secure configuration and operation of information and network systems;
   b) information on known IT threats;
   c) instructions on how to behave in the event of safety-relevant events.

2. An up-to-date register shall be maintained, listing the employees who have completed the training referred to in point 1, the training content and the list of assessments conducted, where applicable.

9.3. **Data security (PR.DS)**: Data shall be managed consistently with the organisation's risk strategy to ensure the confidentiality, integrity, and availability of information.

9.3.1. **PR.DS-01**: Data confidentiality, integrity and availability of data at rest shall be protected.

1. This shall apply to, at least, the relevant information and network systems and shall be based on the outcome of the risk assessment under measure ID.RA-05. Subject to justified and documented regulatory or technical reasons, data stored on portable devices – including laptops, smartphones, and tablets – and on removable media shall be encrypted using state-of-the-art protocols and algorithms and deemed secure.
2. Unless otherwise justified regulatory or technical reasons, the automatic execution of removable media shall be disabled, and removable media shall be scanned for malicious code prior to use within information and network systems.
3. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 1 and 2 shall be adopted and documented.

9.3.2. **PR.DS-02**: Data confidentiality, integrity and availability of data in transit shall be protected.

1. For at least the relevant information and network systems – including voice, video and text communication systems – and in accordance with the results of the risk assessment under measure ID.RA-05, except for justified and documented regulatory or technical reasons, state-of-the-art encryption protocols and algorithms considered secure shall be used for the transmission of data to and from outside the NIS entity.
2. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 1 shall be adopted and documented.

9.3.3. **PR.DS-11**: Data backups shall be created, protected, maintained and verified.

1. In accordance with the operational continuity and disaster recovery stipulations specified in the documentation referenced under measure ID.IM-04, data and configurations shall be routinely backed up, and offline backup copies shall be retained for at least the relevant information and network systems.
2. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 1 shall be adopted and documented.
3. For at least the relevant information and network systems, the confidentiality and integrity of backup data shall be ensured through adequate physical protection of media or encryption.

4. The usability of backups shall be periodically verified by conducting recovery tests.
5. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 3 and 4 shall be adopted and documented.

9.4. **Platform security (PR.PS)**: Hardware, software (e.g. firmware, operating systems, applications) and services across both physical and virtual platforms shall be managed consistently in accordance with the organisation's risk strategy to protect their confidentiality, integrity and availability.

9.4.1. **PR.PS-01**: Configuration management shall be established and applied.

1. Their secure (hardened) reference configurations shall be defined, documented, and maintained in an up-to-date list for at least the relevant information and network systems.
2. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 1 shall be adopted and documented.

9.4.2. **PR.PS-02**: Software shall be maintained, replaced and removed based on the risk implications.

1. Except where justified and documented for regulatory or technical reasons, only software – including operating systems –for which the availability of security updates shall be guaranteed.
2. Except for justified and documented regulatory or technical reasons, the latest security updates released by the manufacturer shall be installed without undue delay, in accordance with the vulnerability management plan under measure ID.RA-08.
3. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 1 and 2 shall be adopted and documented.
4. Except for justified and documented regulatory or technical reasons, and based on the risk assessment outcome under measure ID.RA-05, software updates deemed critical shall be verified in a test environment before deployment in the operational environment.
5. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 4 shall be adopted and documented.

9.4.3. **PR.PS-03**: Hardware shall be maintained, replaced and removed based on the risk implications.

1. For at least the relevant information and network systems, procedures for the secure physical transfer and decommissioning of data storage devices shall be adopted and documented.
2. Additionally, one or more maintenance records for the hardware shall be maintained for the relevant information and network systems.

9.4.4. **PR.PS-04**: Logs shall be generated and made available for continuous monitoring.

1. All remote access activities, particularly those performed by users with administrative privileges, shall be logged.
2. For at least the relevant information and network systems, the logs necessary for monitoring security events – including those related to access under point 1 – shall be securely stored and, where possible, centralised.
3. In accordance with the outcomes of the risk assessment under measure ID.RA-05, the retention period for the logs referred to above shall be defined and documented.
4. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 1 and 2 shall be adopted and documented.

9.4.5. **PR.PS-06**: Safe software development practices shall be integrated, and their performance shall be monitored throughout the entire software life cycle.

1. Safe code development practices in software development shall be adopted and documented.

9.5. **Resilience of technological infrastructure (PR.IR):** Security architectures shall be managed by the organisation's risk strategy to protect the confidentiality, integrity, and availability of assets and enhance organisational resilience.

9.5.1. **PR.IR-01**: Networks and environments shall be protected against unauthorised access and use.

1. Remote access activities for at least the relevant information and network systems shall be defined, documented, and secured through appropriate access control measures.
2. An up-to-date list of information and network systems accessible remotely shall be maintained, including details of the access methods.
3. Perimeter systems such as firewalls shall be deployed, updated, maintained and configured.
4. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 1, 2 and 3 shall be adopted and documented.

9.5.2. **PR.IR-03**: Mechanisms shall be implemented to meet resilience requirements in everyday and adverse situations.

1. Protected emergency communication systems shall be used based on the risk assessment results specified in measure ID.RA-05.

2. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 1 shall be adopted and documented.

10. DETECTION (DETECT)

10.1. **Continuous monitoring (DE.CM)**: Assets shall be monitored for anomalies, indicators of impairment and other potentially adverse events.

10.1.1. **DE.CM-01**: Networks and network services shall be monitored for potentially adverse events.

1. For at least the relevant information and network systems, appropriate technical tools shall be deployed, configured, updated, and maintained to ensure the prompt detection of significant incidents.
2. The expected service levels (SLs) associated with the NIS entity's services and activities shall be defined and documented to support the early identification of significant incidents.
3. In compliance with the policies under measure GV.PO-01, procedures relating to points 1 and 2 shall be adopted and documented.
4. For at least the relevant information and network systems, analysis and filtering tools shall be used to monitor incoming traffic flows, including email.
5. For the information and network systems relevant to point 1, remote accesses, perimeter system activities (e.g., routers and firewalls), relevant administrative events, as well as successful and failed access attempts to network resources, terminal workstations, and applications shall be monitored to detect IT security events.
6. For these relevant information and network systems, qualitative and quantitative parameters shall be defined, monitored, and documented to detect unauthorised access or misuse of granted privileges.
7. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 4, 5 and 6 shall be adopted and documented.

10.1.2. **DE.CM-09**: Processing hardware, software, runtime environments and their associated data shall be monitored for potentially adverse events.

1. Except for justified and documented regulatory or technical reasons, endpoint protection systems for detecting malicious code shall be deployed, updated, maintained and properly configured.
2. In compliance with the policies set out in measure GV.PO-01, procedures relating to points 1 shall be adopted and documented.

11. REPLY (RESPOND)

11.1. **Incident management (RS.MA)**: Responses to detected cybersecurity incidents shall be managed.

11.1.1. **RS.MA-01**: The incident response plan shall be activated in coordination with the relevant third parties once an incident is declared.

1. A plan for the management of IT security incidents and notification to CSIRT Italia, in accordance with Article 25 of the NIS Decree, shall be defined, implemented, updated, and documented. The plan shall include, at least:
   a) the procedures and steps for handling and reporting incidents, with clearly defined roles and responsibilities;
   b) the procedures for preparing and submitting the reports referred to in Article 25(5)(c), (d), and (e) of the NIS Decree;
   c) contact details for reporting incidents;
   d) internal communication procedures, including the escalation to administrative and management bodies, and protocols for external communication;
   e) the reports to be used for documenting the incident.
2. The administrative and management bodies shall approve the plan referred to in point 1.
3. The plans referred to in point 1 shall be reviewed and, if appropriate, updated periodically and, at least, every two years, as well as in the event of significant incidents, incorporating relevant lessons learned, or changes in exposure to threats and related risks.

11.2. **Reporting and communication of incident response (RS.CO):** Response activities shall be coordinated with internal and external stakeholders, as required by applicable laws, regulations, or organisational policies.

11.2.1. **RS.CO-02**: Internal and external stakeholders shall be informed of any incidents.

1. Based on the incident management plan referred to in measure RS.MA-01, procedures shall be adopted and documented to ensure timely communication – without undue delay, where appropriate and feasible – after consultation with CSIRT Italy or when mandated by the National Cybersecurity Agency pursuant to Article 37(3)(g) and (h) of the NIS Decree:
   a) to the recipients of their services, regarding significant incidents that may adversely affect the provision of those services;
   b) to the recipients of services potentially affected by a significant IT threat, including the nature of the threat and the corrective or mitigating measures or actions they may take in response.

2. Procedures shall also be adopted and documented to inform the public of the incidents that took place, if so directed by the National Cybersecurity Agency under Article 37(3) (i) of the NIS Decree.

12. RESTORATION (RECOVER)

12.1. **Execution of the Accident Recovery Plan (RC.RP)**: Recovery activities shall be performed to ensure the operational availability of systems and services affected by cybersecurity incidents.

12.1.1. **RC.RP-01**: The recovery phase of the incident response plan shall be initiated once the incident response process has commenced.

1. As part of the incident management plan under measure RS.MA-01, recovery procedures shall be defined and documented with the aim of restoring, at least, the normal operation of information and network systems affected by IT security incidents, including those referred to in Article 25 of the NIS Decree.

12.2. **Communication on recovery from incidents (RC.CO)**: Restoration activities shall be coordinated with internal and external parties.

12.2.1. **RC.CO-03**: Restoration activities and progress in restoring operational capabilities shall be communicated to designated internal and external stakeholders.

1. Procedures shall be established and documented to notify internal stakeholders, including the relevant NIS entity, of recovery activities following an incident.

3. ANNEX 3

Basic significant incidents for important entities

Code	Description
IS-1	The NIS entity possesses evidence of a loss of confidentiality – towards external parties– of digital data that it owns or partially controls.
IS-2	The NIS entity possesses evidence of a loss of integrity – affecting external parties –, regarding data it owns or over which it exercises, even partially, control.
IS-3	The NIS entity possesses evidence of a breach of the expected service levels for its services and/or activities, as defined under the service level (SL) expectations established in accordance with measure DE.CM-01.

National Cybersecurity Agency

4. ANNEX 4

Basic significant incidents for essential entities

Code	Description
IS-1	The NIS entity possesses evidence of a loss of confidentiality – towards external parties– of digital data that it owns or partially controls.
IS-2	The NIS entity possesses evidence of a loss of integrity – affecting external parties –, regarding data it owns or over which it exercises, even partially, control.
IS-3	The NIS entity possesses evidence of a breach of the expected service levels for its services and/or activities, as defined under the service level (SL) expectations defined in accordance with measure DE.CM-01.
IS-4	The NIS subject also possesses evidence – based on the qualitative and quantitative parameters defined in measure DE.CM-01 – of unauthorised access to, or misuse of, digital data it owns or partially controls.

National Cybersecurity Agency

Appendix

Table 1: Requirements referred to in point 2 of measure GV.PO-01.

Policy areas	Requirements
q) Risk management.	GV.OC-04: point 1. GV.RM-03: point 1. ID.RA-05: points 1, 2, 3 and 4. ID.RA-06: points 1, 2 and 3.
r) Roles and responsibilities.	GV.RR-02: points 1, 2, 3 and 4.
s) Reliability of human resources.	GV.RR-04: points 1, 2 and 4.
t) Compliance and security audits.	GV.PO-01: points 1, 2 and 3. GV.PO-02: points 1, 2, 3. ID.IM-01: points 1, 2, 3 and 4.
u) Management of IT security risks in the supply chain	GV.SC-01: points 1 and 2. GV.SC-02: point 1. GV.SC-04: point 1. GV.SC-05: point 1. GV.SC-07: points 1 and 2.
v) Asset management.	ID.AM-01: point 1. ID.AM-02: point 1. ID.AM-03: point 1. ID.AM-04: point 1.
w) Vulnerability management.	ID.RA-01: points 1, 2 and 3. ID.RA-08: points 1, 2, 3, 4 and 5.
x) Business continuity, disaster recovery and crisis management.	ID.IM-04: points 1, 2, 3, 4 and 5.
y) Management of authentication, digital identities and access control.	PR.AA-01: points 1, 2 and 3. PR.AA-03: points 1 and 2. PR.AA-05: points 1 and 2. PR.IR-01: points 1 and 2.
z) Physical security.	PR.AA-06: point 1.
aa) Staff training and awareness.	PR.AT-01: points 1, 2 and 3. PR.AT-02: points 1 and 2.
bb) Data security.	PR.DS-01: points 1 and 2. PR.DS-02: point 1. PR.DS-11: points 1, 3 and 4.
cc) Development, configuration, maintenance and decommissioning of information and network systems.	PR.PS-01: point 1. PR.PS-02: points 1, 2 and 4. PR.PS-03: points 1 and 2. PR.PS-04: points 1, 2 and 3.

Policy areas	Requirements
	PR.PS-06: point 1.
dd) Protection of networks and communications.	PR.IR-01: point 3. PR.IR-03: point 1.
ee) Monitoring of security events.	DE.CM-01: points 1, 2, 4, 5 and 6. DE.CM-09: point 1.
ff) Incident response and recovery.	RS.MA-01: points 1, 2 and 3. RS.CO-02: points 1 and 2. RC.RP-01: point 1. RC.CO-03: point 1.

Table 2: Requirements specified in point 2 of measure ID.RA-06.

Requirements
GV.SC-05: point 1.
ID.RA-01: point 2.
PR.AA-01: point 1.
PR.DS-01: points 1 and 2.
PR.DS-02: point 1.
PR.PS-02: points 1, 2 and 4.
DE.CM-09: point 1.