REGULATION FOR DIGITAL INFRASTRUCTURE AND CLOUD SERVICES FOR PUBLIC ADMINISTRATION, PURSUANT TO ARTICLE 33-SEPTIES, PARAGRAPH 4, OF DECREE-LAW NO 179 OF 18 OCTOBER 2012, CONVERTED, WITH AMENDMENTS, BY LAW NO 221 OF 17 DECEMBER 2012

THE NATIONAL CYBERSECURITY AGENCY
DIRECTOR-GENERAL

HAVING REGARD TO Law No 400 of 23 August 1988, entitled: 'Discipline of Government activity and Order of the Presidency of the Council of Ministers';

HAVING REGARD TO Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

HAVING REGARD TO Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free movement of non-personal data in the European Union;

HAVING REGARD TO Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on cybersecurity certification for information and communications technology and repealing Regulation (EU) No 526/2013 ('Cybersecurity Act');

HAVING REGARD TO Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS Directive 2);

HAVING REGARD TO Law No 317 of 21 June 1986, entitled: 'Provisions implementing European guidelines on European standardisation and the procedure for the provision of information in the field of technical regulations and rules on Information Society services';

HAVING REGARD TO Legislative Decree No 165 of 30 March 2001, entitled: 'General rules concerning employment in public administration', and in particular Article 1(2);

HAVING REGARD TO Legislative Decree No 196 of 30 June 2003, entitled: 'Personal Data Protection Code, laying down provisions for the adaptation of national law to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC';

HAVING REGARD TO Legislative Decree No 82 of 07 March 2005, entitled: 'Digital Administration Code';

HAVING REGARD TO Law No 196 of 31 December 2009 laying down 'Law on Accounting and

Public Finance';

HAVING REGARD TO Legislative Decree No 65 of 18 May 2018, entitled: 'Implementation of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union';

HAVING REGARD TO Decree-Law No 179 of 18 October 2012, converted, with amendments, by Law No 221 of 17 December 2012 laying down: 'Further urgent measures for the country's growth', and, in particular, Article 33*f* which provides for the consolidation and rationalisation of the country's sites and digital infrastructure by entrusting to the National Cybersecurity Agency, in agreement with the competent structure of the Presidency of the Council of Ministers and in compliance with the rules introduced by Decree-Law No 105 of 21 September 2019, converted, with amendments, by Law No 133 of 18 November 2019, the adoption of a regulation to establish minimum levels of security, processing capacity, energy savings and reliability of digital infrastructure for public administration as well as the quality, security, performance and scalability, interoperability, and portability features of cloud services for public administration and, finally, the terms and methods by which administrations must carry out the migrations provided for in paragraphs 1 and 1*a* of Article 33*f* and the modalities of the procedure for qualifying cloud services for public administration;

HAVING REGARD TO Decree-Law No 105 of 21 September 2019, converted, with amendments, by Law No 133 of 18 November 2019 laying down: 'Urgent provisions on the perimeter of national cyber security';

HAVING REGARD TO Decree-Law No 82 of 14 June 2021, converted, with amendments, by Law No 109 of 04 August 2021 laying down: 'Urgent provisions on cyber security, definition of the national cybersecurity architecture and establishment of the National Cybersecurity Agency' and, in particular, Article 7(1), points *m*) and *mb*), which assign to the National Cybersecurity Agency all the cyber security functions already assigned to the Agency for Digital Italy, the tasks referred to in Article 33*f*, paragraph 4 of Decree-Law No 179 of 2012, and the qualification of cloud services for public administration, as well as the second sentence of Article 17(6);

HAVING REGARD TO Decree-Law No 139 of 8 October 2021, converted, with amendments, by Law No 205 of 3 December 2021, laying down: 'Urgent provisions for access to cultural, sporting and recreational activities, as well as for the organisation of public administrations and on the protection of personal data', and, in particular, Article 9(1)(a) and (i) and paragraph 7 thereof;

HAVING REGARD TO Decree No 223 of the President of the Council of Ministers of 9 December 2021, laying down: 'Regulation for the organisation and functioning of the National Cybersecurity Agency';

HAVING REGARD TO the Decree of the President of the Council of Ministers of 17 May 2022, by which, pursuant to Article 7(1)(b) of Decree-Law No 82 of 14 June 2021, converted, with amendments, by Law No 109 of 4 August 2021, the 'National Cybersecurity Strategy 2022-2026' was adopted, including the 'Implementation Plan 2022-2026', which was notified in the Official Gazette of the Italian Republic No 127 of 1 June 2022;

HAVING REGARD TO the Decree of the President of the Council of Ministers of 1 September

2022, laying down: ‘Modalities and time limits to ensure the transfer of functions, capital goods and documentation from the Agency for Digital Italy and the Department for Digital Transformation to the National Cybersecurity Agency’ published in the *Official Gazette* of the Italian Republic No 246 of 20 October 2022;

HAVING REGARD TO Decree No 166 of the President of the Council of Ministers of 1 September 2022, entitled: ‘Regulation laying down procedures for the drawing up of contracts for works, services and supplies for the activities of the National Cybersecurity Agency for the protection of national security in cyberspace’;

HAVING REGARD TO the Decree of the President of the Council of Ministers of 10 March 2023, by which the Prefect Bruno Frattasi was appointed as Director-General of the National Cybersecurity Agency;

HAVING REGARD TO decision No 628 of 15 December 2021 of the Agency for Digital Italy to adopt the ‘Regulation laying down the minimum levels of security, processing capacity, energy savings and reliability of digital infrastructure for PA and the quality, security, performance and scalability, and portability features of cloud services for public administration, the migration modalities, as well as the modalities for qualifying cloud services for public administration’, which was notified in the Official Gazette of the Italian Republic No 19 of 25 January 2022 (the so-called ‘PA Cloud Regulation’);

HAVING REGARD TO decision No 306 of 18 January 2022 of the National Cybersecurity Agency adopting the template for the establishment of the list and classification of data and services;

HAVING REGARD TO decision No 307 of 18 January 2022 of the National Cybersecurity Agency adopting the Update of the additional minimum levels of security, processing capacity, and reliability of digital infrastructure for public administration and of the additional quality, security, performance and scalability features of cloud services for public administration, as well as qualification requirements for cloud services for public administration;

HAVING REGARD TO the Decree of the Director-General of the National Cybersecurity Agency of 2 January 2023, Protocol No 29, laying down: ‘New qualification process for cloud services for public administration’, which was notified in the Official Gazette of the Italian Republic No 7 of 10 January 2023;

HAVING REGARD TO the Decree of the Director-General of the National Cybersecurity Agency of 8 February 2023, Protocol No 5489, laying down: ‘Postponement of time limits for the adaptation of public administration infrastructure’, which was notified in the Official Gazette of the Italian Republic No 58 of 9 March 2023;

HAVING REGARD TO the Decree of the Director-General of the National Cybersecurity Agency of 28 July 2023, Protocol No 20610, laying down: ‘Changes to the minimum levels of cloud infrastructure and services for public administrations’, which was notified in the Official Gazette of the Italian Republic No 190 of 16 August 2023;

HAVING REGARD TO the Circular of the Agency for Digital Italy No 1 of 14 June 2019, containing: ‘Census of the ICT assets of Public Administrations and classification of infrastructure

suitable for use by National Strategic Poles';

HAVING REGARD TO the 'National Framework for Cybersecurity and Data Protection', 2019 edition (National Framework), created by the Cyber Intelligence and Information Security (CIS) Research Centre of the Sapienza University of Rome and the Cybersecurity National Lab of the National Interuniversity Consortium for IT (CINI), with the support of the Personal Data Protection Authority and the Department of Security Information (DIS) of the Presidency of the Council of Ministers, as a support tool for public and private organisations on strategies and processes aimed at protecting personal data, with specific reference to their security against possible cyber attacks, and cybersecurity, as well as the continuous monitoring thereof;

TAKING INTO ACCOUNT Italian Cloud Strategy which dictates the strategic directions for the migration path to the cloud of data and digital services of the public administration, and illustrates the criteria for the classification of data and services and the composition of high-reliability infrastructure;

CONSIDERING the opinion delivered to the Agency for Digital Italy by the Guarantor for the protection of personal data on 16 December 2021 on the draft regulation on cloud services for public administration, pursuant to Article 33*f* of Decree-Law No 179 of 18 October 2012;

HAVING COMPLETED the information procedure under Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015, by communication of 1 February 2024;

HAVING OBTAINED the opinion of the Guarantor for the protection of personal data, given at the meeting of 9 May 2024;

IN AGREEMENT WITH the Department for Digital Transformation of the Presidency of the Council of Ministers;

hereby adopts the following Regulation

Chapter I
General provisions

Article 1
(Definitions)

1. The following definitions are set out for the purposes of this Regulation:
   a) 'ACN', the National Cybersecurity Agency, referred to in Decree-Law No 82 of 14 June 2021, converted, with amendments, by Law No 109 of 4 August 2021;
   b) 'AgID', the Agency for Digital Italy, as referred to in Article 19 of Decree-Law No 83 of 22 June 2012, converted, with amendments, by Law No 134 of 7 August 2012;
   c) 'central administrations', the central administrations identified by Article 1(3) of Law No 196 of 31 December 2009;
   d) 'local administrations', the local administrations identified by Article 1(3) of Law No 196 of 31 December 2009;
   e) 'administrations', the central administrations referred to in point (c) and the local administrations referred to in point (d);

f) ‘catalogue of cloud infrastructure and services for public administrations’, the catalogue by the ACN, made available through the digital platform, which publishes a list of digital infrastructure for public administrations, cloud service infrastructure for public administrations and cloud services for public administrations, accompanied by relevant descriptive information;
g) ‘cloud computing’, a paradigm that enables network access to a shareable, scalable and elastic set of physical or virtual resources that can be independently activated upon request by the user;
h) ‘administrative data’, information processed by the administration, or by third parties on behalf of the administration;
i) ‘digital administrative data’, administrative data processed through networks and information systems of the administration or of third parties on behalf of the administration;
j) ‘administration services’, services provided to third parties or internally within the administration;
k) ‘digital services’, IT services provided through the administration’s own networks and information systems or through third party networks and information systems on behalf of the administration, to third parties, internally within the administration or in support of administration services, other than basic ICT services;
l) ‘basic ICT services’, IT services provided through networks and information systems supporting digital administration services, such as ICT infrastructure services, ICT security services and connectivity;
m) ‘digital infrastructure for public administrations’, the digital infrastructure through which the digital administration services are provided, including:
    1. ‘Data Processing Centres’ (DPC), i.e., pursuant to Article 33f, paragraph 2, of Decree-Law No 179 of 2012, the sites hosting networks and information systems for the provision of administration internal and external services, which at least includes computing resources, network connection devices and mass storage systems;
    2. the infrastructure promoted by the Presidency of the Council of Ministers referred to in Article 33-*septies*, paragraph 1 of Decree-Law No 179 of 2012;
    3. digital infrastructure components made available to third parties and for the provision of cloud services for the public administration and which may also be used by the digital infrastructure referred to in point 1 (the so-called housing);
    4. digital infrastructure components, possibly made available by third parties, aimed at increasing performance in proximity provision of digital administration services (i.e., proximity infrastructure). Specifically, it can be a single server or another set of connected computing resources, operated within a proximity infrastructure, usually located within a data center operating at the edge of the infrastructure, and thus physically closer to the target users than a cloud node in a centralised data center;
n) Cloud service infrastructure for public administrations, the digital infrastructure referred to in point (m), provided by a digital infrastructure operator, through which cloud services are provided for public administrations;
o) ‘digital infrastructure operator’, a public or private entity which, in compliance with the limits set out in this Regulation, operates a digital infrastructure for public administrations or for the provision of cloud services for public administrations;
p) ‘cloud services’, IT services and computational resources provided through the cloud computing paradigm at the user’s request over the internet by a cloud service provider, differentiated, on the basis of the computational template offered, into three categories of services:
    1) ‘infrastructure systems, known as Infrastructure-as-a-Service (IaaS)’, for the provision, for example, of virtualised servers and data storage space;

2) ‘computational platforms, known as Platform-as-a-Service (PaaS)’, for the provision of pre-configured and administered environments for the development of specific applications, for example for software development, data management or application management;
3) ‘applications, known as Software-as-a-Service (SaaS)’, for the provision of an application to end users, for example e-mail services or other remote collaboration systems. Among the service templates offered by Cloud computing platforms, Software as a Service (SaaS) identifies a class of fully-managed services in which the service manager, i.e., the cloud service provider, takes care of the preparation, configuration, commissioning and maintenance of the same (using its own digital infrastructure or a third party digital infrastructure), leaving the user of the service, or the public administrations, with the sole role of user of the features offered.

q) ‘cloud services for public administrations’, cloud services through which digital administration services are provided;
r) ‘compromise’, the compromising of data or digital services in terms of confidentiality, integrity or availability;
s) ‘qualification of cloud services’, a verification process to ensure that cloud services for public administrations possess the necessary features to process data and services according to their classification, ensuring, in particular, appropriate levels of quality, performance, scalability, portability, and security;
t) ‘adaptation’, the activity preparatory to the transmission to the ACN, by a digital infrastructure operator or a public cloud service provider, of a report on compliance of the digital infrastructure for public administrations, the cloud service infrastructure for public administrations or cloud services for public administrations, with the requirements set out in this Regulation;
u) ‘digital platform’, the digital platform, accessible through the ‘cloud’ section of the ACN’s institutional website, dedicated to the classification of public administration data and services, the adaptation of the digital infrastructure for public administrations and of the cloud service infrastructure for public administrations or of cloud services provided by public operators, and the qualification of cloud services;
v) ‘cloud service provider’, a public or private entity providing a cloud service to public administrations, possibly through the intermediation of distributors, resellers or providers of value-added services offered to the end-user. Distributors, resellers, and providers of value-added services do not assume the status of cloud service providers as long as they do not determine the modalities and means of providing the cloud service;
w) ‘cloud qualification chain’, the relationship between the cloud service for public administration and the platform through which it is provided, in accordance with the procedures described in Annex 4.
x) ‘FNCS’, National Framework for Cybersecurity and Data Protection.

Article 2
(Purpose, object, and scope)

1. This Regulation, in accordance with the provisions of Article 33-*septies*, paragraph 4 of Decree-Law No 179 of 18 October 2012, converted, with amendments, by Law No 221 of 17 December 2012:
   a) establishes the minimum levels of security for public administrations, processing capacity, energy savings and reliability of the digital infrastructure for public administrations and of the cloud service infrastructure for public administrations;
   b) defines the quality, security, performance and scalability, interoperability, and portability

features of cloud services for public administrations;
c) identifies the terms and methods by which administrations must carry out migrations. To this end, it establishes the process and methods for the classification of data and digital services;
d) defines the procedures for qualifying cloud services for public administrations.

2. In addition, this Regulation identifies:
a) the procedures for adapting the digital infrastructure for public administrations and the cloud service infrastructure for public administrations;
b) the procedures for adapting cloud services for public administrations.

CHAPTER II
Characterisation and classification of data and digital services of the public administration

Article 3
(List, characterisation and classification of data and digital services of the public administration)

1. Administrations shall prepare and update a list of their data and digital services, including all the elements necessary for their characterisation for the purpose of their classification.
2. The data and digital services of the administrations referred to in paragraph 1 shall be classified, on the basis of their characterisation, into the following three classes:
a) ‘ordinary’, if the compromise thereof does not lead to the prejudices referred to in points (b) and (c);
b) ‘critical’, if the compromise thereof could result in a prejudice to the maintenance of functions of importance to society, health, public safety, and economic and social well-being of the country;
c) ‘strategic’, if the compromise thereof could lead to a prejudice to national security.
3. Data and digital services subject to the obligations of Decree-Law No 105 of 21 September 2019, converted, with amendments, by Law No 133 of 18 November 2019, are classified as ‘strategic'.
4. Data and digital services subject to the obligations of Legislative Decree No 65 of 18 May 2018 are classified as:
a) ‘critical’, if they are not of national significance;
b) ‘strategic’, if they are of national significance.
5. The data and digital services referred to in paragraphs 3 and 4 are not subject to the listing referred to in paragraph 1.
6. Digital services not yet classified under paragraphs 1 and 2 of this Article cannot be made available to end-users.

Article 4
(Preparation of the list and classification of data and digital services of the public administration)

1. The methods for preparing and updating the list and classification of the data and digital services referred to in Article 3, as well as for the transmission to the ACN, are set out in Annex 1, which forms an integral part of this Regulation.
2. The methods referred to in paragraph 1, made available on the digital platform, shall be elaborated:
a) in relation to the risk and development of the cyber threat;

b) taking into account national, European and international legislation and standards;
c) with regard to the risks to the rights and freedoms of natural persons, when there is personal data, diversified as to the types of personal data involved and the categories of data subjects, in particular if it is data attributable to categories of vulnerable subjects, whether they are special categories of data such as those provided for in Article 9 of Regulation (EU) 2016/679 or personal data relating to criminal convictions and offences referred to in Article 10 of Regulation (EU) 2016/679.

3. The ACN shall update the methods referred to in paragraph 1, on a periodic basis, at least once every two years, in compliance with the provisions of paragraph 2.

Article 5

(Process of transmission of the list and classification of data and digital services of the public administration)

1. The administrations shall update the list and classification of data and digital services referred to in Article 3 and shall transmit them to the ACN in the manner set out in Annex 1, at least once every two years or in the presence of data and digital services additional to those already transmitted and classified, as well as following the updating of the methods referred to in Article 4, in accordance with the time limits set out therein.
2. The ACN shall provide feedback on the compliance of the list and classification of data and digital services referred to in Article 3 with the methods referred to in Article 4, within 90 days of its receipt. The aforementioned time limit may be extended by the ACN, only once and up to a maximum of an additional thirty days, if it is necessary to carry out in-depth studies concerning the process of transmitting the list and classification of data and digital services of the public administration.
3. Where it proves necessary to request supplementary and additional information from the administration that transmitted the list and classification of the data and digital services referred to in Article 3, the time limits laid down in paragraph 2 shall be suspended and shall recommence from the date of receipt of the supplementary and additional information provided within 30 days of the request.
4. At the end of the conformity clearance referred to in paragraph 2, the ACN shall communicate to the digital address of the administration:
   a) the validation of compliance of the list and classification of data and digital services referred to in Article 3;
   b) the validation, with requirements, of compliance of the list and classification of data and digital services referred to in Article 3;
   c) the non-validation, providing the reasons, of compliance of the list and classification of data and digital services referred to in Article 3.
5. In the case referred to in paragraph 4(b), the administration shall, within 30 days, send the ACN the adaptation of the list and classification of data and services to the requirements.
6. In the absence of feedback from the ACN within the time limits set out in paragraphs 2 and 3, the list and classification of data and services shall be deemed validated in accordance with paragraph 4(a).

CHAPTER III
Minimum levels of digital infrastructure for public administrations, cloud service infrastructure for public administrations and cloud service features for public administrations

Article 6

(Criteria for defining the minimum levels of digital infrastructure for public administrations, cloud service infrastructure for public administrations and cloud service features for public administrations)

1. The minimum levels of security, processing capacity, energy savings and reliability of the digital infrastructure for public administrations, cloud service infrastructure for public administrations as well as the cloud service features for public administrations, as referred to in Articles 7 and 8, are defined by the ACN also on the basis of the National Framework for Cybersecurity and Data Protection.
2. The minimum levels of security, processing capacity, energy savings and reliability of the digital infrastructure for public administrations, cloud service infrastructure for public administrations as well as the cloud service features for public administrations, as referred to in Articles 7 and 8, shall be updated regularly, at least once every two years:
   a) in line with the classification of the data and services to be processed;
   b) in relation to the risk and development of the cyber threat;
   c) in view of the progressively adopted national and European certification schemes;
   d) taking into account best practices, guidelines, reference regulatory frameworks, and national, European and international standards;
   e) taking into account the development of the necessary measures and guarantees to ensure an adequate level of protection of personal data.

Article 7
(Minimum levels of digital infrastructure for public administrations and cloud service infrastructure for public administrations)

1. Digital infrastructure for public administrations and cloud service infrastructure for public administrations shall comply with the minimum levels of security, processing capacity, energy savings and reliability set out in Annex 2, which is an integral part of this Regulation.
2. To process data and digital services classified in accordance with Article 3 as:
   a) ‘ordinary’, digital infrastructure for public administrations and cloud service infrastructure for public administrations must comply with the minimum levels set out in Section 2 of Annex 2;
   b) ‘critical’, digital infrastructure for public administrations and cloud service infrastructure for public administrations must comply with the minimum levels set out in Sections 2 and 3 of Annex 2;
   c) ‘strategic’, digital infrastructure for public administrations and cloud service infrastructure for public administrations must comply with the minimum levels set out in Sections 2, 3 and 4 of Annex 2.
3. The minimum levels of security, processing capacity, energy savings and reliability must be ensured entirely by the digital infrastructure or by the components of a digital infrastructure made available by third parties and aimed at providing cloud services for the public administration, which may also be used by digital infrastructure, and jointly by the same operator and the provider of the so-called housing services, through dedicated agreements.
4. The digital infrastructure for public administrations and cloud service infrastructure for public administrations, through which data are processed and digital services subject to Decree-Law No 105 of 2019 are provided, also comply with the cloud requirements laid down in the aforementioned decree.

Article 8
(Cloud service features for public administrations)

1. Cloud services for public administrations shall have the quality, safety, performance and scalability, interoperability and portability characteristics set out in Annex 3, which forms an integral part of this Regulation.
2. To process data and digital services classified in accordance with Article 3 as:
   a) 'ordinary', cloud services for public administrations must comply with the minimum levels set out in Section 2 of Annex 3;
   b) 'critical', cloud services for public administrations must comply with the minimum levels set out in Sections 2 and 3 of Annex 3;
   c) 'strategic', cloud services for public administrations must comply with the minimum levels set out in Sections 2, 3 and 4 of Annex 3.
3. Cloud services for public administrations that process data and provide digital services subject to Decree-Law No 105 of 2019 also comply with the cloud requirements laid down in the aforementioned decree.

CHAPTER IV
Migration of data and digital services of the public administration

Article 9
(Criteria for the migration of data and digital services of the public administration)

1. The administrations, in accordance with the principles of efficiency, effectiveness and cost-effectiveness of administrative action, shall migrate, in compliance with the provisions of Article 33-*septies*, paragraphs 1 and 1*a* of Decree-Law No 179 of 2012, the data and digital services towards digital infrastructure for public administrations which, as a result of the adaptation process referred to in Article 12, comply, in relation to the classification referred to in Article 3, with the minimum levels referred to in Article 7 and the requirements referred to in Article 12, or to cloud services, adapted in accordance with Article 15, or qualified in accordance with Article 17, which, in relation to the classification referred to in Article 3, comply with the features referred to in Article 8 and the requirements set out in Articles 15 and 17.
2. The migration of data and digital services subject to the obligations laid down in Decree-Law No 105 of 2019 and Legislative Decree No 65 of 2018, pursuant to paragraph 1, also takes place in compliance with the provisions of the aforementioned decrees.

Article 10
(Methods for preparing and updating the plan for data and digital services migration)

1. The administrations, following the process of transferring the list and classification of data and digital services referred to in Article 5, shall prepare the migration plan for their data and digital services in accordance with the template adopted by the Department for Digital Transformation, in agreement with the ACN.
2. The template referred to in paragraph 1 shall be made available on the digital platform and through the communication channels of the Department for Digital Transformation and shall apply in accordance with the provisions of Article 27; if deemed necessary, it may be updated in accordance with the methods of the same paragraph 1.
3. In the presence of data and digital services additional to those already classified and communicated in the manner provided for in Article 11 below, the administrations, after

updating the list and classification of data and digital services referred to in Article 3, shall prepare the new migration plan to update the migration plans referred to in paragraph 1.

Article 11
(Modalities and time limits for the migration of data and digital services)

1. The administrations, also for the purpose of verifying the obligations laid down in Article 33-*septies* of Decree-Law No 179 of 2012, shall transmit the migration plans to the Department for Digital Transformation and the AgID, through the dedicated platform made available by the same Department for Digital Transformation.
2. The migration plans drawn up pursuant to Article 10(3) shall be transmitted through the platform referred to in paragraph 1.
3. AgID, DTD and ACN shall access the Platform referred to in paragraph 1, in the manner defined through an agreement or convention agreed upon by the same entities in order to carry out the activities within their competence with respect to the obligations set out in Article 33-septies of Decree-Law No 179 of 2012. Pending the drawing up of said agreement, AgID and DTD shall request from the ACN the list of classified data and digital services referred to in Article 3, the ACN shall request from DTD and AGID the migration plans referred to in Article 10 for the relevant activities.
4. The administrations shall complete the activities provided for in the migration plan, transmitted in accordance with paragraph 1, by 30 June 2026.
5. The Department for Digital Transformation, also using AGID, shall verify that the migration plans comply with the template referred to in Article 10(1) within sixty days from the date of its receipt. The aforementioned time limit may be extended by the Department for Digital Transformation, only once and up to a maximum of a further sixty days, if it is necessary to carry out an in-depth analysis of the migration plan.
6. Where it proves necessary to request supplementary and additional information from the administration that transmitted the migration plan, the time limits laid down in paragraph 4 shall be suspended and shall recommence from the date of receipt of the information provided within 30 days of the request.
7. At the end of the conformity clearance referred to in paragraph 4, the Department for Digital Transformation communicates to the digital address of the administration:
   a) the validation of the migration plan;
   b) the validation, with requirements, of the migration plan;
   c) the non-validation, providing the reasons, of the migration plan.
8. In the case referred to in paragraph 6(b), the administration shall, within thirty days, transmit to the Department for Digital Transformation the adaptation of the migration plan to the requirements.
9. In the absence of feedback from the Department for Digital Transformation within the time limits set out in paragraphs 4 and 5, the migration plan shall be deemed validated in accordance with paragraph 6(a).
10. As part of the migration activities referred to in paragraph 2, public administrations may process their data and services with cloud infrastructure and services already in use until the completion of the migration, in the case of a validated migration plan and, in any case, no later than 30 June 2026.

CHAPTER V
Adaptation of digital infrastructure for public administrations, cloud service infrastructure for public administrations and qualification of cloud services for public administrations

Article 12
(Adaptation of digital infrastructure for public administrations and cloud service infrastructure for public administrations)

1. The requirements for adapting digital infrastructure or cloud service infrastructure for public administrations are divided into the following four levels:
   a) level 1 infrastructure (AI1);
   b) level 2 infrastructure (AI2);
   c) level 3 infrastructure (AI3);
   d) level 4 infrastructure (AI4).
2. The adaptation requirements referred to in paragraph 1 shall be elaborated:
   a) in relation to the risk and development of the technical cyber threat;
   b) taking into account national, European and international legislation and standards;
   c) in view of the progressively adopted national and European certification schemes;
   d) taking into account best practices, guidelines, and reference regulatory frameworks of the sector.
3. For the purpose of the adaptation:
   a) to level 1 (AI1) referred to in paragraph 1, the digital infrastructure for public administrations or the cloud service infrastructure for public administrations must comply with the requirements listed in Section 6 of Annex 4, which forms an integral part of this Regulation;
   b) to level 2 (AI2) referred to in paragraph 1, the digital infrastructure for public administrations or the cloud service infrastructure for public administrations must comply with the requirements listed in Section 7 of Annex 4;
   c) to level 3 (AI3) referred to in paragraph 1, the digital infrastructure for public administrations or the cloud service infrastructure for public administrations must comply with the requirements listed in Section 8 of Annex 4;
   d) to level 4 (AI4) referred to in paragraph 1, the digital infrastructure for public administrations or the cloud service infrastructure for public administrations must comply with the requirements listed in Section 9 of Annex 4.
4. Data and digital services classified, pursuant to Article 3, as:
   a) ‘ordinary’ shall be provided through digital infrastructure for public administrations or cloud service infrastructure for public administrations accredited under the types referred to in points (a), (b), (c) and (d) of paragraph 1;
   b) ‘critical’ shall be provided through digital infrastructure for public administrations or cloud service infrastructure for public administrations accredited under the types referred to in points (b), (c) and (d) of paragraph 1;
   c) ‘strategic’ shall be provided through digital infrastructure for public administrations or cloud service infrastructure for public administrations accredited under the types referred to in points (c) and (d) of paragraph 1.

Article 13
(Modalities and time limits for the adaptation of digital infrastructure for public administrations)

1. Following the adaptation activities referred to in Article 12, digital infrastructure operators shall sign and submit to the ACN a report of compliance with the minimum levels referred to in Article 7 and with the requirements laid down in Article 12, drawn up on the basis of the template made available on the digital platform. This provision shall apply in accordance with the provisions laid down in Article 27.

2. The compliance report for the purpose of the adaptation referred to in paragraph 1 and for the purpose of the promotion referred to in paragraph 8, made pursuant to Presidential Decree No 445 of 28 December 2000, shall be signed by the legal representative of the digital infrastructure operator or by a delegate thereof and shall be submitted electronically in accordance with the provisions laid down in Article 65 of Legislative Decree No 82 of 7 March 2005.
3. Unless there is a reasoned request by the digital infrastructure operator for non-publication, subject to assessment by the ACN, the digital infrastructure for public administrations shall be published in the catalogue of cloud infrastructure and services for public administrations, with the indication ‘adequate digital infrastructure’.
4. The catalogue, made available on the digital platform, shall be updated by the ACN within thirty days of receipt of the compliance report referred to in paragraph 1 without prejudice to the possibility for the ACN itself to request amendments and additions to the report with formal deficiencies. In the latter case, the time limit of thirty days shall start from the receipt by the ACN of the documentation containing the amendments and additions requested.
5. The adjustment shall become valid:
    a. for the cases referred to in paragraph 3, from the moment the ACN acknowledges the request for non-publication referred to in that paragraph;
    b. for the cases referred to in paragraph 4, from the date of publication in the catalogue.
6. In case of use of housing services, the compliance report shall contain evidence of the competence requirements of the third-parties, with the indication of the unique reference to the catalogue, if present, referred to in paragraph 4, of the relevant digital infrastructure for public administrations. This indication is mandatory for compliance reports sent from 01/02/2025 onwards.
7. Where substantial amendments are made to the modalities for adopting the minimum levels referred to in Article 7 and the requirements referred to in Article 12, the digital infrastructure operator shall communicate, in a timely manner and without undue delay, the relevant modalities to the ACN in accordance with this Article, updating, in any case, the above-mentioned compliance report at least every thirty-six months.
8. The request for the transition of a digital infrastructure for public administrations to a different level of adaptation (“promotion”) in accordance with Article 12 shall be made with the same adaptation modalities set out in this Article.

Article 14
(Modalities for adapting cloud service infrastructure for public administrations)

1. For the purpose of adapting a cloud service infrastructure for public administrations, digital infrastructure operators shall sign and submit to the ACN a report of compliance with the requirements set out in Article 12 and with the minimum levels referred to in Article 7, drawn up on the basis of the template made available on the digital platform. This provision shall apply in accordance with the provisions laid down in Article 27.
2. The compliance report for the purpose of the adaptation referred to in paragraph 1 and for the purpose of the promotion referred to in paragraph 8, made pursuant to Presidential Decree No 445 of 28 December 2000, shall be signed by the legal representative of the digital infrastructure operator or by a delegate thereof and shall be submitted electronically in accordance with the provisions laid down in Article 65 of Legislative Decree No 82 of 7 March 2005.
3. Unless there is a reasoned request by the digital infrastructure operator for non-publication, subject to assessment by the ACN, the cloud service infrastructure for public administrations shall be published in the catalogue of cloud infrastructure and services for public

administrations, with the indication ‘adequate cloud service infrastructure’.

4. The catalogue, made available on the digital platform, shall be updated by the ACN within thirty days of receipt of the compliance report referred to in paragraph 1, without prejudice to the possibility for the ACN itself to request amendments and additions to the report with formal deficiencies. In the latter case, the time limit of thirty days shall start from the receipt by the ACN of the documentation containing the amendments and additions requested.
5. The adjustment shall become valid:
    a. for the cases referred to in paragraph 3, from the moment the ACN acknowledges the request for non-publication referred to in that paragraph;
    b. for the cases referred to in paragraph 4, from the date of publication in the catalogue.
6. In case of use of housing services, the compliance report shall contain evidence of the competence requirements of the third-parties, with the indication of the unique reference to the catalogue, if present, referred to in paragraph 4, of the relevant cloud service infrastructure for public administrations. This indication is mandatory for compliance reports sent from 01/02/2025 onwards.
7. Where substantial amendments are made to the modalities for adopting the minimum levels set out in Annex 2, the digital infrastructure operator shall communicate, in a timely manner and without undue delay, the relevant modalities to the ACN in accordance with this Article, updating, in any case, the above-mentioned compliance report at least every thirty-six months.
8. The request for the transition of a cloud service infrastructure for public administrations to a different level of adaptation (‘promotion’) in accordance with Article 12 shall be made with the same adaptation modalities set out in this Article.

Article 15
(Adaptation of cloud services for public administrations)

1. Cloud services for public administrations provided by a public entity, by in-house companies, or, by express regulatory provision, by publicly controlled companies, as defined in Legislative Decree No 175 of 19 August 2016, are subject to the adaptation process.
2. Cloud services for public administrations are divided into the following four levels:
    a) level 1 cloud (AC1);
    b) level 2 cloud (AC2);
    c) level 3 cloud (AC3);
    d) level 4 cloud (AC4).
3. The requirements corresponding to the levels referred to in paragraph 2 shall be elaborated:
    a) in relation to the risk and development of the technical cyber threat;
    b) taking into account national, European and international legislation and standards;
    c) in view of the progressively adopted national and European certification schemes;
    d) taking into account best practices, guidelines, and reference regulatory frameworks of the sector.
4. For the purpose of the adaptation:
    a) to level 1 (AC1) referred to in paragraph 1, the cloud service must comply with the requirements listed in Section 2 of Annex 4;
    b) to level 2 (AC2) referred to in paragraph 1, the cloud service must comply with the requirements listed in Section 3 of Annex 4;
    c) to level 3 (AC3) referred to in paragraph 1, the cloud service must comply with the requirements listed in Section 4 of Annex 4;
    d) to level 4 (AC4) referred to in paragraph 1, the cloud service must comply with the requirements listed in Section 5 of Annex 4.

5. Data and digital services classified, pursuant to Article 3, as:
   a) 'ordinary' may be provided through appropriate cloud services under the types referred to in points (a), (b), (c), and (d) of paragraph 1;
   b) 'critical' may be provided through appropriate cloud services under the types referred to in points (b), (c), and (d) of paragraph 1;
   c) 'strategic' may be provided through appropriate cloud services under the types referred to in points (c) and (d) of paragraph 1.

Article 16
(Modalities and time limits for the adaptation of cloud services for public administrations)

1. The cloud service providers referred to in Article 15(1) shall sign and submit to the ACN a report of compliance with the requirements set out in Article 15 and with the minimum levels referred to in Article 8, drawn up on the basis of the template made available on the digital platform in accordance with the provisions set out in Article 27.
2. The compliance report for the purpose of the adaptation referred to in paragraph 1 and for the purpose of the promotion referred to in paragraph 8, made pursuant to Presidential Decree No 445 of 28 December 2000, shall be signed by the legal representative of the cloud service provider or by a delegate thereof and shall be submitted electronically in compliance with the provisions referred to in Article 65 of Legislative Decree No 82 of 7 March 2005.
3. Unless there is a reasoned request by the cloud service provider for non-publication, subject to assessment by the ACN, the cloud service for public administrations shall be published in the catalogue of cloud infrastructure and services for public administrations, with the indication 'adequate cloud service for public administrations'.
4. The catalogue, made available on the digital platform, shall be updated by the ACN within thirty days of receipt of the compliance report referred to in paragraph 1, without prejudice to the possibility for the ACN itself to request amendments and additions to the report with formal deficiencies. In the latter case, the time limit of thirty days shall start from the receipt by the ACN of the documentation containing the amendments and additions requested.
5. The adjustment shall become valid:
   a. for the cases referred to in paragraph 3, from the moment the ACN acknowledges the request for non-publication referred to in that paragraph;
   b. for the cases referred to in paragraph 4, from the date of publication in the catalogue.
6. In case of use of proximity infrastructure, the compliance report shall contain evidence of the analysis aimed at verifying that the features referred to in Article 8 and the requirements referred to in Article 15 are not adversely affected, also on the basis of the requirements set out in paragraph 2.4 of Annex 4, with the indication of the relevant digital infrastructure for public administrations.
7. Where substantial amendments are made to the modalities for adopting the features set out in Annex 3, the cloud service provider for public administrations shall communicate, in a timely manner and without undue delay, the relevant modalities to the ACN in accordance with this Article, updating, in any case, the above-mentioned compliance report at least every thirty-six months.
8. The request for the transition of a cloud service for public administrations to a different level of adaptation in accordance with Article 15 ("promotion") shall be made with the same adaptation modalities set out in this Article.

Article 17
(Qualification of cloud services for public administrations)

1. Cloud services for public administrations that cloud service providers, other than those referred to in Article 15(1), are required to qualify are divided into the following four levels:
   a) level 1 cloud (QC1);
   b) level 2 cloud (QC2);
   c) level 3 cloud (QC3);
   d) level 4 cloud (QC4).
2. The requirements corresponding to the levels referred to in paragraph 1 shall be elaborated:
   a) in relation to the risk and development of the technical cyber threat;
   b) taking into account national, European and international legislation and standards;
   c) in view of the progressively adopted national and European certification schemes;
   d) taking into account best practices, guidelines, reference regulatory frameworks, and national, European and international standards.
3. For the purpose of qualification:
   a) as level 1 (QC1) referred to in paragraph 1, the cloud service must comply with the requirements listed in Section 2 of Annex 4;
   b) as level 2 (QC2) referred to in paragraph 1, the cloud service must comply with the requirements listed in Section 3 of Annex 4;
   c) as level 3 (QC3) referred to in paragraph 1, the cloud service must comply with the requirements listed in Section 4 of Annex 4;
   d) as level 4 (QC4) referred to in paragraph 1, the cloud service must comply with the requirements listed in Section 5 of Annex 4.
4. Data and digital services classified, pursuant to Article 3, as:
   a) ‘ordinary’ may be provided through accredited cloud services under the types referred to in points (a), (b), (c), and (d) of paragraph 1;
   b) ‘critical’ may be provided through accredited cloud services under the types referred to in points (b), (c) and (d) of paragraph 1;
   c) ‘strategic’ may be provided through accredited cloud services under the types referred to in points (c) and (d) of paragraph 1.

Article 18
(Application for the qualification of cloud services for public administrations)

1. Applications for qualification and those for promotion referred to in paragraph 4, made pursuant to Presidential Decree No 445 of 28 December 2000, shall be signed by the legal representative of the cloud service provider or by a delegate thereof and shall be submitted electronically in accordance with the provisions referred to in Article 65 of Legislative Decree No 82 of 7 March 2005.
2. Cloud service providers other than those referred to in Article 15(1) shall transmit electronically the applications referred to in paragraph 1 with the necessary information, accompanying documentation, when requested, and the modalities indicated on the digital platform in accordance with the provisions referred to in Article 27, developed gradually according to the required qualification level.
3. The necessary information referred to in paragraph 2 shall include, at least:
   a) the type of qualification required as referred to in Article 17;
   b) the underlying cloud service or, where provided without the use of other cloud services, the digital infrastructure or the cloud service infrastructure used, in accordance with Article 20;
   c) a description of the cloud services for which qualification is requested;
   d) an indication of the requirements possessed for the requested qualification and the

relevant documentation;

e) the specification and outcome of the security verification activities carried out by the provider on the service subject to qualification;

f) in the case of requests starting from qualification level 3, the description of the architectural elements of the infrastructure or cloud service.

4. The request for the transition of a cloud service for public administrations to a different level of qualification (‘promotion’) within the meaning of Article 15 shall be made with the same qualification modalities set out in this Article.
5. In case of use of proximity infrastructure, the compliance report shall contain evidence of the analysis aimed at verifying that the features referred to in Article 8 and the requirements referred to in Article 17 are not adversely affected, also on the basis of the requirements set out in paragraph 2.4 of Annex 4, with the indication of the relevant digital infrastructure for public administrations.

Article 19
(Modalities for the qualification of cloud services for public administrations)

1. Within sixty days of receipt of a qualification application from an applicant, submitted according to the modalities referred to in Article 18, the ACN shall verify compliance with the requirements for the qualification levels referred to in Article 17 and the minimum levels referred to in Article 8, in relation to the type of qualification requested.
2. As part of the conformity clearance referred to in paragraph 1, the ACN may:
   a) ask questions;
   b) request integrations, additional information and additional documentation;
   c) carry out technical checks, including security checks aimed at verifying the presence of vulnerabilities in the systems, also through access to the physical and logical infrastructure of the cloud service infrastructure or the cloud service;
   d) hear the applicant.
3. Where it is necessary to carry out in-depth studies, including those referred to in paragraph 2, concerning technical aspects in the context of the conformity clearance, the time limit referred to in paragraph 1 shall be extended up to thirty days, which may be further extended by thirty days in particularly complex cases.
4. Where it is necessary to request information and documentation from the applicant requesting qualification, including those referred to in paragraph 2, the time limits shall be suspended and shall recommence from the date of receipt of the information and documentation provided within 15 days of the request, after which the application is deemed not accepted.
5. At the end of the conformity clearance referred to in this Article, the ACN shall communicate, within 15 days, to the digital address of the applicant:
   a) the rejection, providing the reasons, of the qualification of the cloud service;
   b) the release, with reasoned conditions, of the qualification of the cloud service, specifying its duration;
   c) the release, without conditions, of the qualification of the cloud service, specifying its duration.
6. The qualification has a maximum duration of thirty-six months.
7. Where the ACN intends to proceed pursuant to paragraph 5(a), prior to the formal adoption of the negative measure, it shall inform the applicant, within the period referred to in that paragraph 5, of the grounds for refusing the application. Within ten days of receipt of the notification, the applicant may submit its observations, accompanied, where appropriate, by supporting documentation. The ACN notification shall suspend the time limits for the

conclusion of the proceedings, which shall start to run again 10 days after the submission of the observations or, failing that, from the expiry of the time limits set for the applicant. If the applicant has submitted observations, ACN is required to give reasons for their possible non-acceptance in the justification of the final rejection measure, indicating, if there are any, only the additional grounds for rejection which result from the observations.

8. The ACN, in the cases referred to in points (b) and (c) of paragraph 5, shall publish the cloud service for public administrations in the catalogue of cloud infrastructure and services for public administrations, with the indication ‘cloud service for public administrations qualified with conditions’ or ‘qualified cloud service for public administrations’. The catalogue, made available on the digital platform, shall be updated by the ACN within fifteen days of the end of the conformity clearance referred to in this Article.
9. Taking into account the time limits for the conclusion of the qualification procedure referred to in this Article, where it is necessary to renew the qualification of a cloud service, the relevant applications shall be submitted 90 days before the expiry of the same qualification in accordance with the same rules as those laid down in this Article. The ACN may, in this case, authorise the applicant to continue to operate until the date of conclusion of the renewal procedure. The applicant shall inform the persons with whom it intends to conclude contracts related to the application of this Regulation of this transition period and of the ongoing proceedings.

Article 20
(Monitoring of digital infrastructure, cloud service infrastructure and cloud services for public administrations)

1. Following the adaptation referred to in Articles 13, 14 and 16 or the release of qualifications pursuant to Article 18, the ACN may carry out checks to verify that the requirements laid down in Articles 7, 8, 12, 15 and 17 are met and maintained in relation to the type and level of adaptation or qualification, with the modalities referred to in Article 19(2).
2. If, after the checks carried out pursuant to paragraph 1, profiles relating to non-compliance with the requirements of this Regulation emerge, also following any additional investigation carried out with the collaboration of the interested parties, the ACN requests, prior to the initiation of the revocation procedures, the digital infrastructure operator or the cloud service provider to ensure compliance with the aforementioned requirements within forty-five days of the same request, without prejudice to specific, different needs for which it is necessary to provide for a different time limit.
3. Following the request referred to in paragraph 2, and until the successful verification, by the ACN, of the fulfilment of the same, the digital infrastructure operator or the cloud service provider has the obligation to communicate, to the entities with which it has already in place or with which it intends to enter into contracts related to the application of this Regulation, that it is subject to verification by the ACN. During the verification period, the operator guarantees the continuity of the services provided for in the existing contracts.
4. At the end of the period referred to in paragraph 2, the ACN:
   a) in the case of compliance by the operator, shall inform the same operator of the positive outcome of the checks carried out. The operator, in turn, shall inform the entities with which it has contracts related to the application of this Regulation;
   b) in the case of non-compliance, it shall activate the procedures provided for in Articles 21 and 23.

Article 21

(Revocation of qualification and declaration of inadequacy)

1. In the cases provided for in Article 20(4)(b), the ACN shall either revoke the qualification or declare the inadequacy of the digital infrastructure for public administrations, the cloud service infrastructure for public administrations or the cloud service for public administrations referred to in Article 15.
2. At the same time as the revocation or declaration of inadequacy referred to in paragraph 1, communicated to the digital address of the data subject, the ACN shall mark the digital infrastructure for public administrations, the cloud service infrastructure for public administrations or the cloud service for public administrations, published in the catalogue of cloud infrastructure and services for public administrations, with the indication ‘inadequate infrastructure/service’ or ‘qualification revoked’.
3. The revocation measures and the declarations of inadequacy referred to in paragraph 1 shall, in any case, be published on the digital platform.
4. The digital infrastructure operator and the cloud service provider, following the revocation or declaration of inadequacy referred to in paragraph 1, must:
   a) inform, without delay, any customer administrations of the revocation or declaration of inadequacy;
   b) support any customer administrations in the activities of migration towards another digital infrastructure operator or cloud service provider, chosen by the same customer administration, ensuring easy data export and providing full collaboration for the establishment of communication and migration flows to the infrastructure of the new provider, for the automatic transfer of the data and services provided;
   c) permanently delete, upon successful migration, all administrative data that may be stored or still available.
5. The administrations, in the event of revocation or declaration of inadequacy referred to in paragraph 1, may continue to use the revoked service for a maximum period of six months from the date of revocation or declaration of inadequacy, possibly extendable, upon specific request, in the presence of documented elements of technical complexity, without prejudice to any other determination made by the ACN.

Chapter VI
Transitional and final provisions, entry into force and application of the Regulation

Article 22
(Processing of personal data)

1. Administrations are data controllers of personal data processing carried out within digital infrastructures for public administrations, cloud service infrastructures for public administrations and cloud services for public administrations.
2. Digital infrastructure operators, cloud service providers and other entities involved in the processing of personal data referred to in paragraph 1 or in the public administration’s data and digital services migration activities referred to in Chapter IV, as well as the entities they use for the performance of specific processing activities on behalf of administrations, shall act as data controllers within the meaning of Article 28 of Regulation (EU) 2016/679.
3. The entities referred to in paragraph 2 shall take appropriate technical and organisational measures to ensure timely and adequate information to administrations in the event of a personal data breach, as referred to in Article 33(2) of Regulation (EU) 2016/679.
4. The use of other data controllers by the entities referred to in paragraph 2 shall be regulated in

accordance with Article 28(2) and (4) of Regulation (EU) 2016/679, providing for technical and organisational measures to provide the administrations with appropriate means of monitoring the processing activities carried out under their own responsibility.

5. In the event of a transfer of personal data outside the European Economic Area, the data controllers referred to in paragraphs 2 and 4 shall be required to comply with the instructions of the administrations given pursuant to Article 28(3)(a) of Regulation (EU) 2016/679 and to make available to them any information necessary to assess the effectiveness of the appropriate measures implemented pursuant to Chapter V of Regulation (EU) 2016/679.
6. Without prejudice to the competence of the Guarantor for the protection of personal data for infringements of the provisions of this Article and the obligations to notify the Guarantor for the protection of personal data imposed on the entities referred to in paragraphs 1 and 2, the National Cybersecurity Agency shall communicate to the Guarantor any evidence of possible personal data breaches of which it becomes aware.

Article 23
(Reports to the Agency for Digital Italy)

1. The ACN, in all cases where it detects the failure by the Administrations to comply with the provisions of these Regulations, shall report the infringement found to the Agency for Digital Italy in order to apply Article 33-septies, paragraph 4-quinquies of Decree-Law No 179 of 2012.

Article 24
(Transition to the ordinary regime)

1. From the date of entry into force of this Regulation:
   a) cloud service infrastructure in possession of a valid qualification, issued by the ACN by the date of application of this Regulation, shall be deemed adequate, in accordance with Article 12, for the same level and deadline as provided for by the qualification obtained;
   b) cloud services in possession of a valid qualification, issued by the ACN by the date of application of this Regulation, are deemed qualified, in accordance with Article 17, for the same level and deadline as provided for by the qualification obtained.

Article 25
(Transitional provisions)

1. The lists of data and services referred to in Article 3 and the migration plans referred to in Article 10 transmitted prior to the adoption of this Regulation shall also be deemed to be transmitted for the purposes of this Regulation.
2. Digital infrastructure operators which, in the report submitted by 18 January 2024, as referred to in Article 13(2), stated that they had taken, by 30 September 2023, the decision, in consideration of documented, more complex adaptation measures, to comply with the minimum levels referred to in Article 7 and the requirements referred to in Article 12, shall complete the adaptation activities by 18 October 2024. Until the completion of the adaptation activities, the same operators shall continue to process their data and services with the cloud infrastructure and services already in use.
3. Cloud service providers which, in their report submitted by 18 January 2024 referred to in Article 16(2), stated that they had taken, by 30 September 2023, the decision, in consideration of documented, more complex adaptation measures, to comply with the minimum levels referred to in Article 8 and the requirements referred to in Article 15, shall complete the

adaptation activities by 18 October 2024. Until the completion of the adaptation activities, the same providers shall continue to process their data and services with the cloud infrastructure and services already in use.

Article 26
(Repeals)

1. The following shall be repealed with effect from the date of application of this Regulation:
   a) The Regulation adopted by the Agency for Digital Italy with Decision No 628 of 15 December 2021;
   b) decision No 306 of 18 January 2022 of the National Cybersecurity Agency;
   c) decision No 307 of 18 January 2022 of the National Cybersecurity Agency;
   d) the Decree of the Director-General of the National Cybersecurity Agency of 2 January 2023, Protocol No 29;
   e) the Decree of the Director-General of the National Cybersecurity Agency of 8 February 2023, Protocol No 5489;
   f) the Decree of the Director-General of the National Cybersecurity Agency of 28 July 2023, Protocol No 20610;
   g) the Decree of the Director-General of the National Cybersecurity Agency of 30 January 2024, Protocol No 2927.

Article 27
(Application of the Regulation and requirements)

1. This Regulation shall apply from 1 August 2024. Until that date, the transitional arrangements laid down in Decree No 29 of the Director General of the National Cybersecurity Agency of 2 January 2023 remain in force.
2. The requirements laid down in Articles 7, 8, 12, 15 and 17, referred to in Annexes 2, 3 and 4, shall apply in accordance with the methods and times indicated in the same Annexes.
3. This Regulation is published on the institutional website of the National Cybersecurity Agency (www.acn.gov.it), on the digital platform and will also be communicated by publication in the Official Gazette of the Italian Republic.

REGULATION FOR DIGITAL INFRASTRUCTURE AND CLOUD SERVICES FOR PUBLIC ADMINISTRATION, PURSUANT TO ARTICLE 33-SEPTIES, PARAGRAPH 4, OF DECREE-LAW NO 179 OF 18 OCTOBER 2012, CONVERTED, WITH AMENDMENTS, BY LAW NO 221 OF 17 DECEMBER 2012

ANNEX 1

"METHODS FOR PREPARING THE LIST AND CLASSIFICATION OF DATA AND SERVICES OF THE PUBLIC ADMINISTRATION"

1. **Premise**
   1.1. This Annex defines, in accordance with the provisions of Article 4 of the Regulation, the methods for preparing and updating the list and classification of the data and digital services referred to in Article 3 of the Regulation, as well as the related procedure for transmission to the ACN for the purpose of the conformity clearance pursuant to Article 5 of the Regulation.
   1.2. In order to facilitate administrations in the preparation of the list and classification of their data and digital services, the ACN, on the digital platform referred to in Article 1(1)(z) of the Regulation, makes the following available:
      a) default lists of data and/or services, already accompanied by their classification, for homogeneous groups of administrations, which the individual administration may amend or supplement in accordance with point 2 of this Annex;
      b) questionnaires and classification templates for the possible assessment of the classification of data and/or services to supplement the default lists and for the possible reassessment of the classification of data and/or services in the default lists.
   1.3. The default lists, templates and classification algorithms shall be updated on a regular basis, at least once every two years, according to the methods set out in this Annex. The updating will be communicated via ACN communication channels.
   1.4. In order to prepare and update the default lists, questionnaires and templates, the ACN may use representative groups of homogeneous administrations. The administrations identified by the ACN to form the representative groups of homogeneous administrations shall join on a voluntary basis.

2. **Process of listing and classifying data and digital services**
   2.1. For the preparation and updating of the list and classification of their data and digital services, the administrations shall examine the default list and the relevant classification referred to in point 1.2(a) on the digital platform and, through the functionalities offered by the same digital platform, may:
      a. accept the default list and its classification. In this case, the list and classification referred to in Article 3 of the Regulation shall be deemed validated in accordance with Article 5(4)(a) of the same Regulation;
      b. if they do not process all data and/or digital services in the default list, amend the list by deleting data and services that are not processed. The updating of the list and classification shall be transmitted to the ACN, through the digital platform, for the conformity clearance referred to in Article 5(2) of this Regulation;
      c. if they process additional data and/or digital services than those in the default list, supplement the default list and its classification. In this case, the supplemented list shall be transmitted to the ACN, via the digital platform, together with the questionnaires for the classification referred to in point 1.2(b), filled out in their entirety for each data and digital service processed and not included in the default list. The supplemented list and questionnaires shall be subject to the conformity clearance referred to in Article 5(2) of this Regulation;
      d. if they do not consider the proposed classification for data and/or digital services in the default list to be consistent, change their classification. In this case, the list shall be transmitted to the ACN, via the digital platform, together with the questionnaires referred to in point 1.2(b) filled out in their entirety to change the classification for each data and service processed for which the proposed classification is not considered to be consistent. The list and the new questionnaires shall be subject to the conformity clearance referred to in Article 5(2) of this Regulation.
   2.2. For justified and documented reasons of a regulatory or technical nature, in derogation from point 2.1, the central administrations referred to in Article 1(1)(c) may submit electronically to the ACN, in

compliance with the provisions of Article 65 of Legislative Decree No 82 of 7 March 2005, the listing and classification of their data and digital services, together with the reasons and risk analysis carried out to come to the classification produced, in accordance with the template made available through the ACN communication channels.

REGULATION FOR DIGITAL INFRASTRUCTURE AND CLOUD SERVICES FOR PUBLIC ADMINISTRATION, PURSUANT TO ARTICLE 33-SEPTIES, PARAGRAPH 4, OF DECREE-LAW NO 179 OF 18 OCTOBER 2012, CONVERTED, WITH AMENDMENTS, BY LAW NO 221 OF 17 DECEMBER 2012

ANNEX 2

'MINIMUM LEVELS OF SECURITY AND RELIABILITY, PROCESSING CAPACITY, ENERGY SAVINGS OF DIGITAL INFRASTRUCTURE AND SERVICE INFRASTRUCTURE FOR THE PUBLIC ADMINISTRATION'

Summary

1. Premise and definitions

1.1. This Annex defines, in accordance with the provisions of Articles 6 and 7 of the Regulation, the minimum levels of security and reliability, processing capacity, energy savings of digital infrastructure for public administrations and cloud service infrastructure for public administrations that can host services and digital data, respectively, of the public administration consistently with the relevant classification level referred to in Article 3 of the Regulation.

1.2. The minimum levels are organised on the basis of the subcategories of the National Framework for Cybersecurity and Data Protection, hereinafter referred to as FNCS. For each measure, a more detailed specification is provided of the expected minimum implementation and of the required modalities in order to describe its adoption and demonstrate its implementation.

1.3. The minimum levels of security, processing capacity, energy savings and reliability of the digital infrastructure set out in this Annex shall apply to production environments. The minimum levels of security, processing capacity, energy savings and reliability of pre-production, testing, development and similar environments shall be applied in accordance with the minimum levels of the digital infrastructure set out in this Annex, possibly in relation to a risk analysis aimed at identifying potential impacts on the service and its managed data or on the digital infrastructure related to the production environment.

1.4. For the purposes of this Annex, the following definitions shall apply:

a) ‘Administrative data’ means data provided, stored, sent, received, processed by or on behalf of the Administration by the entity through the Digital Infrastructure;

b) ‘Administrative metadata’ means data collected, obtained or generated by the entity, including in derivative form, from administrative data, as part of the delivery and administration of the Digital Infrastructure. This category includes, for example, the historicisation of system and service events, service configurations, and attributes of the administration’s resources, also resulting from their use;

c) ‘Metadata relating to the operation of the Digital Infrastructure’ means data generated and used by the entity to monitor and ensure the functionality of the Digital Infrastructure, not included in Administrative Metadata or Administrative Data. This category of Metadata, which must therefore not be referable to people, to the entity and cannot in any case allow the extraction - even in part - of administrative data, includes, for example, metrics on performance of use, balancing, etc.

d) ‘external dependence’ means networks, information systems, IT services, physical infrastructure or other services, including those used for maintenance and management purposes, which appertain to other entities, on which the operation of the digital infrastructure depends;

e) ‘internal dependence’ means networks, information systems, IT services, physical infrastructure or other services, including those used for maintenance and management purposes, which are external to the cloud service but appertain to the digital infrastructure operator, on which the operation of the digital infrastructure depends;

f) ‘cyber supply chain’ means the digital infrastructure supply chain.

1.5. With the exception of the cybersecurity organisation, the term ‘organisation’, which appears within the descriptions of the categories and subcategories, shall be understood as referring at least to the infrastructure or staff of the digital infrastructure operator for public administrations or to the cloud service infrastructure for public administrations responsible for its management. In addition, the term ‘entity’ shall be understood as the ‘digital infrastructure operator’.

2. Minimum levels in the case of ordinary data and services

2.1 Reliability

2.1.1) High reliability.

A.AA-01: Infrastructure availability

1_O. *The Digital Infrastructure Availability Index, which refers to the percentage of time in a year in which the infrastructure is accessible and usable, must have been at least equal to:*
a. 99.98 % net of planned downtime;
b. 99.6 % including planned downtime.

A.AA-02: Solutions are available for high-reliability configuration of services

1_O. *The Data Processing Center (DPC) must be equipped with hardware and software solutions (network and security equipment, storage, virtualisation services, etc.) for high-reliability configuration of services. Capabilities and functionalities must also be made available to support high-reliability service configurations such as:*

a. Choice of local data replication for a storage service;

b. Presence of load balancing services;

c. Anti-affinity mechanisms for the distribution of computational instances.

2.1.2) Business Continuity and Disaster Recovery.

A.BC-01: Disaster Recovery solutions are available with guaranteed recovery times

1_O. *Infrastructure Providers: The digital infrastructure shall be equipped with DR solutions, with features consistent with risk analysis, and shall ensure variable recovery times (RTO and RPO) depending on the criticality of the hosted application as defined in the BIA.*

2_O. *With reference to the RTO and RPO values defined in point 1_O, in the event of a disaster, at least the following recovery parameters shall be guaranteed: RTO 48 hours and RPO 48 hours.*

2.1.3) Governance and processes.

A.GP-01: IT Services are managed in accordance with industry standards

1_O. *Processes and procedures are adopted in line with the best practices indicated by ISO/IEC 20000-2.*

A.GP-02: Compliance with mandatory service indicators is ensured

1_O. *For the Data Processing Centre (DPC), the entity must guarantee technical support for emergencies with:*

a. coverage of 24 hours a day, 7 days a week throughout the year;

b. a maximum incident response time (meaning the maximum time between the reporting of an event with a critical impact on the Administration's operations and the entity's response) of 1 hour.

2_O. *The entity must guarantee, for the Data Processing Centre (DPC) services offered, technical support with the following characteristics:*

a. provided, at least in English, from 08.00 to 18.00 (Italian time) on working days

b. preferentially accessible via the following channels: telephone and e-mail address.

At the request of the Administration, the support service is provided at least in Italian.

2.1.4) Performance and Scalability.

A.PS-01: Minimum connectivity features are guaranteed

1_O. *The entity shall provide connectivity over a public network and a private network. The private network shall enable the entity to use dedicated connectivity services with the following guaranteed minimum performance:*

a. 500 Mbps basic bandwidth, with the possibility of increasing the bandwidth up to 10 Gbps.

2.2 Processing capacity

2.2.1) Processing capacity.

CE.CE-01: Processing capacity management in accordance with industry standards or best practices

1_O. *The processing capacity of the Digital Infrastructure is managed through a formal process adhering to the ITIL capacity management best practices or to the ISO/IEC 20000-2 guidelines.*

2.3 Data Center Security

2.3.1) Data Center Security.

S.DC-01: Data Processing Centers (DPCs) comply with minimum levels of physical and infrastructure security

- ***1_O.*** *The entity guarantees operational monitoring within the Data Center for 24 hours a day, 7 days a week throughout the year.*
- ***2_O.*** *The Data Center has been designed and built according to infrastructure reference standards, e.g. ANSI/BICSI 002, TIA-942, EN 50600, Uptime Institute Tier Certification or similar.*
- ***3_O.*** *The entity guarantees the fire-fighting features of the Data Center in accordance with the fire-fighting standards in force.*
- ***4_O.*** *The premises hosting the Data Centres must have raised floors if the power supply and wiring are not overhead.*
- ***5_O.*** *The entity guarantees that all Data Center servers are connected to electrical continuity devices (UPS).*

S.DC-02: Physical and environmental security measures are taken

- ***1_O.*** *There is a detailed document setting out policies and procedures related to the safe movement of physical media. These policies and procedures should be reviewed on at least an annual basis.*
- ***2_O.*** *Surveillance systems are implemented, maintained and adopted outside data centers and at all entry and exit points in order to detect any unauthorised entry attempt.*
- ***3_O.*** *Environmental control systems are implemented, maintained and adopted within the Data Centers in order to monitor and test the adequacy of temperatures and humidity conditions within the area, in compliance with the main industry standards.*

2.4 Energy Savings

2.4.1) Energy savings.

RE.GE-01: Energy management conducted in compliance with industry standards

- ***1_O.*** *The entity has formally adopted procedures for the management of the emissions of the gases produced, or for the management of the energy consumed or for the environmental management of its data centers. In this respect, the entity may refer, respectively, to ISO 14064, ISO 50001 and ISO 14001, or equivalent standards.*

RE.GE-02: Annual Assessment of the Energy Efficiency of the Data Center

- ***1_O.*** *The entity determines the energy efficiency of its Data Centers on an annual basis, using the calculation of the Power Usage Effectiveness (PUE) indicator, which must have a maximum value of 1.5.*

  The PUE links the energy expenditure of the infrastructure, including IT equipment, air conditioning and auxiliary installations, to the expenditure on IT equipment only. Specifically, it is calculated as the ratio of energy expenditure incurred for the entire data center infrastructure to that incurred for IT equipment.

2.5 Security

IDENTIFY (ID)

2.5.1) Asset Management (ID.AM): The data, personnel, devices, and systems and facilities necessary for the organisation are identified and managed in accordance with the objectives and risk strategy of the organisation.

ID.AM-01: The systems and physical equipment used in the organisation are registered.

- ***1_O.*** *All systems and physical equipment are registered and there is a list of those approved by actors within the entity.*
- ***2_O.*** *All systems and physical equipment present on the networks are registered and access to the network is*

allowed exclusively to the approved ones.

ID.AM-03: Organisation-related data and communication flows are identified

1_O. *All data and information flows, including outward flows and flows related to the digital infrastructure, are identified, registered and approved by actors within the entity.*

ID.AM-06: Cybersecurity roles and responsibilities are defined and disclosed for all personnel and any relevant third parties (e.g. suppliers, customers, partners)

1_O. *Cybersecurity organisation, also with reference to roles and responsibilities, for all personnel and any third parties is defined and disclosed to the competent bodies of the entity.*

2_O. *Within the scope of the body referred to in point 1_O., a person in charge, and a possible substitute, possessing specific professionalism and expertise in the field of cyber security, shall be appointed with the task of managing the implementation of the provisions of the Regulation, who shall report directly to the hierarchical top of the entity and ensure the effective implementation of the security measures referred to in this Annex.*

3_O. *Within the scope of the body referred to in point 1_O., a technical contact person, and at least one substitute, possessing technical and specialised expertise in the field of cyber security, shall be appointed to carry out the dialogue with CSIRT Italia for the purpose of managing incidents affecting the digital infrastructure.*

4_O. *The person in charge referred to in point 2_O. and the technical contact person referred to in point 3_O. shall operate in close cooperation.*

2.5.2) Governance (ID.GV): Policies, procedures and processes to manage and monitor the organisation's requirements (organisational, legal, risk-related, environmental) are understood and used in cybersecurity risk management.

ID.GV-01: A cybersecurity policy is identified and disclosed

1_O. *There is an updated document describing cybersecurity policies, processes and procedures.*

2.5.3) Risk Assessment (ID.RA): The enterprise understands the cybersecurity risk inherent in the organisation's operations (including mission, functions, image or reputation), the assets, and the individuals.

ID.RA-01: The vulnerabilities of the organisation's resources (e.g. systems, premises, devices) are identified and documented

1_O. *There is an updated security assessment and testing plan describing all activities aimed at assessing the level of cyber security of the Digital Infrastructure and the effectiveness of the technical and procedural security measures, and which also contains the frequency and methods of implementation.*

2_O. *There are procedures, to be updated at least on an annual basis, for the management of risks associated with changes in organizational assets, including applications, systems, infrastructure, configurations, etc., regardless of whether the assets are managed internally or externally (i.e. outsourced).*

ID.RA-05: Threats, vulnerabilities, their likelihood of occurrence and consequent impacts are used to determine the risk

1_O. *The risk analysis shall be carried out on the basis of threats, vulnerabilities, their likelihood of occurrence and the consequent impacts resulting from their exploitation in the light of the threats considered.*

2_O. *The risk analysis takes into account the internal and external dependencies of the Digital Infrastructure.*

3_O. *After identifying all the risk factors and analysing them, a weighting is carried out to determine the level of risk.*

PROTECT (PR)

2.5.4) Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and related resources is limited to authorised personnel, processes and devices, and is managed in a manner consistent with the assessment of the risk of unauthorized access to authorised activities and transactions.

PR.AC-01: Digital identities and login credentials for authorised users, devices and processes are administered, verified, revoked and subject to security audits

- ***1_O.a*** *Access credentials shall be individual for the personnel of the entity and shall comply with the principle of separation of duties. Credentials shall be updated at a rate commensurate with user privileges.*
- ***1_O.b*** *Access credentials shall be individual for the personnel of the entity and for external personnel having access to the infrastructure and shall comply with the principle of separation of duties. Credentials shall be updated at a rate commensurate with user privileges.*
- ***2_O.*** *There are policies and procedures for the management of credentials referred to in point 1_O., which must be updated at least on an annual basis and made available for consultation to the Administration.*
- ***3_O.*** *Mechanisms for managing, storing and reviewing information on credentials, system identity and access level are defined.*
- ***4_O.*** *The credentials shall be updated promptly and without undue delay if there are changes in users (e.g. transfer of personnel).*
- ***5_O.*** *System identities shall be managed by using digital certificates or alternative techniques that ensure an equivalent level of security.*
- ***6_O.*** *There is an updated planning of security audits to verify compliance with the provisions of points 1_O., 2_O., 3_O., 4_O. and 5_O. and there is a register of audits carried out with the relevant documentation.*

PR.AC-02: Physical access to resources is protected and administered

- ***1_O.*** *With reference to the censuses of the ID.AM-01 subcategory, there is an updated, detailed document containing at least:*
  a. the security policies adopted for the protection and administration of physical access;
  b. the processes, methodologies and technologies used that contribute to compliance with security policies.
- ***2_O.*** *A physical security perimeter is defined in order to safeguard personnel, data and information systems.*

PR.AC-03: Remote access to resources is administered

- ***1_O.*** *Remote access is monitored by the cybersecurity organisation.*
- ***2_O.*** *Without prejudice to documented technical limitations, adequate access control measures are implemented, adopting systems of authentication, authorisation and centralised registration/accounting of accesses, supported by authentication systems, whose security is proportional to the risk.*
- ***3_O.*** *A centralised access management model is defined and implemented for processes of authorisation, logging and communication of access to administrative resources and data.*
- ***4_O.*** *There is a log of remote accesses.*
- ***5_O.*** *For remote access, multiple factor authentication methods are used.*

PR.AC-04: Rights of access to resources and their authorisations shall be administered in accordance with the principles of least privilege and separation of duties

- ***1_O.*** *With reference to censuses referred to in the ID.AM category, at least the following are defined:*
  a. the census resources that need to be accessed, for what functions and with what permissions;
  b. user groups and their privileges in relation to the resources they can access and with what permissions;
  c. the assignment of census users to user groups.

2_O. *When implementing access to the information system, principles of separation of duties and least privilege are observed in relation to organisational risk.*

3_O. *Policies, procedures and technical measures for the separation of duties in relation to privileged access are defined and implemented so that administrative access to data, encryption and key management capabilities, and logging capabilities are distinct and separate.*

2.5.5) Awareness and Training (PR.AT): The personnel and third parties are sensitised about cybersecurity and are trained to fulfil their tasks and roles consistently with existing policies, procedures and agreements.

PR.AT-01: The personnel of the entity are informed and trained

1_O. *There is an updated document detailing the contents of the training and education provided to the personnel of the entity and how to verify the acquisition of the contents.*

2_O. *The training and education referred to in point 1_O. provided to the users of the entity, in relation to the roles, shall include, at least, the following topics:*

a. the protection of the confidentiality of clear or encrypted data;

b. the return of company assets at the end of the employment relationship;

c. the definition of roles and responsibilities;

d. policies for access to systems, assets and resources;

e. information and security management policies;

f. processes for communicating roles and responsibilities to employees who have access to information assets;

g. requirements for non-disclosure/confidentiality of information.

PR.AT-02: Privileged users (e.g. System administrators) understand their roles and responsibilities

1_O. *The contents of the instructions provided to the privileged personnel of the entity and the methods for verifying the acquisition of the contents are defined.*

2_O. *The privileges and instructions received shall be defined for each member of the personnel of the entity.*

2.5.6) Data Security (PR.DS): The data is stored and managed in accordance with the organisation's risk management strategy, in order to ensure the integrity, confidentiality and availability of information.

PR.DS-01: Stored data is protected

1_O. *There is an updated document detailing, also in relation to the ID.AM category, at least:*

a. the security policies adopted for the storage and protection of data;

b. the processes, methodologies and technologies used that contribute to compliance with security policies.

2_O. *Administrative data, including security data (such as, but not limited to, access control systems), are processed through facilities located in the territory of the European Union. Unless justified and documented reasons of a regulatory or technical nature, these facilities shall include those assigned to the functions of:*

a. Business Continuity and Disaster Recovery, even if outsourced (e.g. via cloud computing);

b. Content Delivery Network with global geographic distribution.

In this case, the application of the ID.RA-05 measure must appropriately take into account the location outside the European territory, also verifying compliance with the legislation on the protection of personal data.

3_O. *Unlike Metadata relating to the operation of the infrastructure, which can be processed by facilities even located outside the territory of the European Union, Metadata relating to the administration shall be processed by facilities located in the territory of the European Union, unless justified and documented reasons of a regulatory or technical nature. In this case, the application of the ID.RA-05 measure must appropriately take into account the location outside the European territory, also verifying compliance with the legislation on the protection of personal data. In the event of Metadata being transferred to non-EU facilities, the interruption of this communication flow must not however result in non-compliance with the minimum service levels provided for the cloud service.*

4_O. *With reference to point 3_O., in the event that the Metadata relating to the administration are aimed at the provision of IT security services or for the resilience of the digital infrastructure, they may also be processed, in the presence of justified technical reasons and related evidence of their management in accordance with the uniformity of the purposes of the processing, outside the European territory. In this case, the application of the ID.RA-05 measure must appropriately take into account the location outside the European territory, also verifying compliance with the legislation on the protection of personal data. In the case of metadata being transferred to non-EU facilities, the interruption of this communication flow must not however result in non-compliance with the minimum service levels provided for the cloud service.*

PR.DS-05: Protection techniques (e.g. access control) are implemented against data leaks

1_O. *In relation to the ID.AM category, at least the following shall be defined:*

a. the security policies adopted for access to data;

b. the processes, methodologies and technologies used that contribute to compliance with security policies.

2_O. *Data Loss Prevention policies are adopted consistently with the risk assessment.*

PR.DS-06: Data integrity control mechanisms are used to verify the authenticity of software, firmware and information

1_O. *In relation to the ID.AM category, at least the following shall be defined:*

a. the list of data integrity control mechanisms to verify the authenticity of software, firmware and information;

b. the security policies adopted to assign a mechanism to a resource and which of these mechanisms is applied to which resource;

c. the processes, methodologies and technologies used that contribute to compliance with security policies.

2.5.7) Information Protection Processes and Procedures (PR.IP): Security policies (which address the purpose, scope, roles and responsibilities, management commitment and coordination between the various organizational entities), processes and procedures to manage the protection of information systems and assets shall be implemented and adapted over time.

PR.IP-01: Reference practices (so-called baseline) are defined and managed for the configuration of IT and industrial control systems incorporating security principles (e.g. principle of least functionality).

1_O. *Policies and procedures relating to application security shall be defined to provide adequate support for the planning, implementation and maintenance of application security features, which must be reviewed and updated at least on an annual basis.*

PR.IP-04: Information backups are executed, administered and verified

1_Oa. *A backup of the stored data is performed periodically. The confidentiality, integrity and availability of backup data is ensured.*

1_Ob. *A backup is periodically made of the information stored in the cloud necessary for the complete recovery of the system, including administrative data and the data necessary for the restoration of the service. The confidentiality, integrity and availability of backup data is ensured. To this end, it is also ensured that media containing at least one of the copies are not permanently accessible by the system in order to prevent attacks on it from also involving all its backup copies.*

2_O. *The restoration (restore test) of backup copies is periodically verified as a goal (SLO) at least once a year.*

PR.IP-12: A vulnerability management plan is developed and implemented

1_O. *There is an updated document detailing at least:*

a. the security policies adopted to manage vulnerabilities;

b. the processes, methodologies and technologies used that contribute to compliance with security policies.

2_O. *Technical procedures and measures are defined and implemented to update detection tools, threat signatures and indicators of compromise, which must be reviewed and updated frequently or on a weekly basis.*

2.5.8) Maintenance (PR.MA): Maintenance of information systems and industrial control is done in accordance with existing policies and procedures.

PR.MA-02: Remote maintenance of resources and systems is approved, documented and carried out in order to avoid unauthorised access

1_O. *Remote maintenance of resources and systems (including security-related activities) shall be carried out in accordance with the measures set out in subcategory PR.AC-03 and the following points.*

2_O. *All access performed remotely by third-party personnel is authorised by the cybersecurity organisation and limited to essential cases only.*

2.5.9) Protective Technology (PR.PT): Technical security solutions are managed to ensure security and resilience of systems and assets, consistent with related policies, procedures and agreements.

PR.PT-04: Communication and control networks are protected

1_O. *Perimeter systems, such as firewalls, also at the application level, are present, updated, maintained and well configured.*

DETECT (DE)

2.5.10) Security Continuous Monitoring (DE.CM): Information systems and assets are monitored to identify cybersecurity events and to verify the effectiveness of protection measures.

DE.CM-01: Computer network monitoring is carried out to detect potential cybersecurity events

1_O. *Intrusion Detection Systems (IDS) are present.*

2_O. *Processes are present for monitoring events related to the security of applications and the underlying infrastructure.*

DE.CM-04: Malicious code shall be detected

1_O. *Special tools for malware prevention and detection, as well as Endpoint Protection System (EPS), are implemented and used.*

2_O. *There are anti-malware protection policies, which will need to be reviewed at least on an annual basis.*

DE.CM-08: Scans are carried out for the identification of vulnerabilities

1_O. *Based on risk analysis, penetration tests and vulnerability assessments are performed on critical platforms and software applications before they are put into operation.*

2_O. *Penetration tests and vulnerability assessments shall be carried out periodically in relation to the criticality of platforms and software applications, referred to in point 1_O.*

3_O. *There is an updated document showing the type of penetration test and vulnerability assessment envisaged.*

4_O. *There is an updated register of penetration tests and vulnerability assessments carried out together with the relevant documentation.*

2.5.11) Detection Processes (DE.DP): Monitoring processes and procedures shall be adopted, maintained and verified to ensure the understanding of anomalous events.

DE.DP-01: Roles and responsibilities for monitoring processes are well defined in order to ensure accountability

1_O. *The appointments referred to in subcategory ID.AM-06 are disclosed within the entity.*

2_O. *The roles, processes and responsibilities for activities leading to the detection of incidents with an impact on the digital infrastructure are well defined and disclosed to the competent bodies of the entity.*

RESPOND (RS)

2.5.12) Communications (RS.CO): Response activities are coordinated with the internal and external parties (e.g. possible support from law enforcement bodies or law enforcement agencies).

RS.CO-01: The personnel are aware of their role and what they need to do if a response to an incident is necessary

1_O. *The roles and responsibilities for carrying out the phases and processes of responding to an incident are well defined and disclosed to the competent bodies of the entity.*

2.5.13) Analysis (RS.AN): Analyses are carried out to ensure an effective response and support to recovery activities.

RS.AN-05: Processes are defined to receive, analyse and respond to information about vulnerabilities disclosed by sources inside or outside the organisation (e.g. internal testing, security bulletins, or security researchers).

1_O. *The communication channels of the CSIRT Italia referred to in Article 4 of the Decree of the President of the Council of Ministers of 8 August 2019, of the reference Authority of its production sector, as well as of any reference CERT and Information Sharing & Analysis Centre (ISAC) shall be monitored.*

2.5.14) Mitigation (RS.MI): Actions are carried out to prevent the spread of a security event, to mitigate its effects and to resolve the incident.

RS.MI-03: New vulnerabilities are mitigated or documented as an accepted risk

1_O. *Vulnerabilities are mitigated in accordance with the Vulnerability Management Plan (PR.IP-12), i.e. the residual risk resulting from non-mitigation is documented and accepted.*

2_O. *Technical procedures and measures are defined and implemented to allow response actions (scheduled or when emergencies arise) in case of identified vulnerabilities, based on the risk.*

RECOVER (RC)

2.5.15) Recovery Planning (RC.RP): Recovery processes and procedures are performed and maintained to ensure a recovery of the systems or assets involved in a cybersecurity incident.

RC.RP-01: There is a recovery plan, which is executed during or after a cybersecurity incident

1_O. *There is a recovery plan that includes, at least, processes and procedures necessary to restore the normal functioning of the part of the infrastructure affected by a cybersecurity incident.*

3. Minimum levels in the case of critical data and services

3.1 Reliability

3.1.1) Business Continuity and Disaster Recovery.

A.BC-01: Disaster Recovery solutions are available with guaranteed recovery times

3_C. *In the case of administrative critical data and services, the provisions of the requirement referred to in requirement A.BC-01, point 2_O shall not apply. In particular, with reference to requirement A.BC-01, point 1_O., the digital infrastructure shall be equipped with DR solutions, with features consistent with the risk analysis, and at least the following disaster recovery parameters must be ensured: RTO 36 hours and RPO 36 hours.*

3.1.2) Governance and processes.

A.GP-02: Compliance with mandatory service indicators is ensured

3_C. *In the case of administrative critical data and services, the provisions of the requirement set out in point 2_O shall not apply. The support and assistance service is provided, at least in Italian, every day of the year at any time (24 hours a day, 7 days a week throughout the year).*

3.1.3) Performance and Scalability.

A.PS-01: Minimum connectivity features are guaranteed

2_C. *The entity offers protection mechanisms against Denial-of-Service / Distributed Denial-of-Service cyber events.*

3.2 Data Center Security

3.2.1) Data Center Security.

S.DC-03: The design/construction of the Data Center ensures hot maintainability, in accordance with market standards

1_C. *The digital infrastructure must adhere to the parameters of the ANSI/TIA 942B certificate with "Concurrent Maintainability" rating or that of Tier III of the Uptime Institute. Alternatively, it must comply with the construction characteristics of the mechanical, electrical and fire fighting systems set out in Table 1.*

3.3 Security

IDENTIFY (ID)

3.3.1) Asset Management (ID.AM): The data, personnel, devices, and systems and facilities necessary for the organisation are identified and managed in accordance with the objectives and risk strategy of the organisation.

ID.AM-02: Software platforms and applications in use in the organisation are registered

1_C. *All installed software platforms and applications are registered and there is a list of those approved by actors within the entity.*

2_C. *The installation of software platforms and applications is permitted only for approved ones.*

3_C. *There are policies that limit the addition, removal or update, as well as unauthorised management of the organisation's assets.*

ID.AM-06: Cybersecurity roles and responsibilities are defined and disclosed for all personnel and any relevant third parties (e.g. suppliers, customers, partners)

5_C. *The names and contact details of the person in charge referred to in point 2_O. and of the technical contact person referred to in point 3_O. shall be communicated by the entity to the National Cybersecurity Agency (ACN).*

6_C. *There is a list of all internal and external personnel employed in cybersecurity processes with specific roles and responsibilities. The list is disseminated to the competent bodies of the entity.*

7_C. *There is a list of figures similar to the person in charge referred to in point 2_O. and to the technical contact person referred to in point 3_O. at third parties, in relation to the external dependencies, and at the same entity, in relation to the internal dependencies. The competences of the person in charge and of the technical contact person must be reassessed according to the type of dependence. The list is disseminated to the competent bodies of the entity.*

8_C. *The person in charge referred to in point 2_O. shall also ensure cooperation with the National Cybersecurity Agency (ACN), also in relation to the activities related to Article 5 of Decree-Law No 105 of 2019 and the activities of prevention, preparation and management of cyber crises entrusted to the Cybersecurity Unit (NCS) referred to in Decree-Law No 82 of 2021, and the activities of verification and inspection.*

3.3.2) Governance (ID.GV): Policies, procedures and processes to manage and monitor the organisation's requirements (organisational, legal, risk-related, environmental) are understood and used in cybersecurity risk management.

ID.GV-01: A cybersecurity policy is identified and disclosed

2_C. *The document referred to in point 1_O. must be approved by the entity and updated at least on an annual basis or in case of substantial changes within the organisation.*

ID.GV-04: Governance and Risk Managament Processes Include Cybersecurity Risk Management

1_C. *There is a formal Enterprise Risk Management (ERM) program that includes policies and procedures for the identification, assessment, ownership, processing and acceptance of the security and privacy risks of the Infrastructure.*

3.3.3) Risk Assessment (ID.RA): The enterprise understands the cybersecurity risk inherent in the organisation's operations (including mission, functions, image or reputation), the assets, and the individuals.

ID.RA-05: Threats, vulnerabilities, their likelihood of occurrence and consequent impacts are used to determine the risk

4_C. *There is an updated risk assessment document that includes at least:*

a. the identification of threats, both internal and external, appropriately described and assessed and their likelihood of occurrence;

b. vulnerabilities referred to in subcategory ID.RA-1 and in subcategory DE.CM-8;

c. the potential impacts deemed significant on the infrastructure, appropriately described and assessed;

d. risk identification, analysis and weighting.

3.3.4) Supply Chain Risk Management (ID.SC): The organisation's priorities, constraints, risk tolerances and assumptions are established and used to support risk decisions associated with supply chain risk management. The organisation has defined and implemented processes to identify, assess and manage supply chain risk.

ID.SC-01: Risk management processes inherent in the cyber supply chain are identified, well defined, validated, managed and approved by actors within the organisation

1_C. *There is an updated, detailed document describing the processes for managing the risk inherent in the cyber supply chain.*

2_C. *These processes are validated and approved by the entity's top management.*

PROTECT (PR)

3.3.5) Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and related resources is limited to authorised personnel, processes and devices, and is managed in a manner consistent with the assessment of the risk of unauthorized access to authorised activities and transactions.

PR.AC-01: Digital identities and login credentials for authorised users, devices and processes are administered, verified, revoked and subject to security audits

7_C. *There is an updated document detailing at least:*

a. the security policies adopted for the administration, verification, revocation and security audit of digital identities and the procedures set out in points 1_O., 2_O., 3_O., 4_O., 5_O., 6_O.;

b. the security policies adopted for the administration, verification, revocation and security audit of digital identities and access credentials for users;

c. the processes, methodologies and technologies used that contribute to compliance with security policies.

PR.AC-02: Physical access to resources is protected and administered

3_C. *A security perimeter is defined between administrative areas and data storage and processing areas.*

PR.AC-03: Remote access to resources is administered

6_C. *There is an updated document detailing at least:*

a. the security policies adopted for the definition of permitted activities through remote access and the security measures adopted;

b. the processes, methodologies and technologies used that contribute to compliance with security policies.

PR.AC-04: Rights of access to resources and their authorisations shall be administered in accordance with the principles of least privilege and separation of duties

4_C. There is an updated, detailed document containing the processes referred to in point 1_O.

PR.AC-05: Network integrity is protected (e.g. network segregation, network segmentation)

1_C. There are policies and procedures for the security of the network infrastructure, which must be updated at least on an annual basis.

2_C. A plan shall be established for monitoring the availability, quality and adequate capacity of resources in order to provide the required system performance.

PR.AC-07: Authentication methods (e.g. single-factor or multiple-factor authentication) for the entity's users, devices and other assets are commensurate with the risk of the transaction (e.g. risks related to the security and privacy of individuals and other organizational risks)

1_C. Policies and procedures shall be defined and implemented for access to systems, applications and data, including multi-factor authentication at least for privileged users and access to data.

3.3.6) Data Security (PR.DS): The data is stored and managed in accordance with the organisation's risk management strategy, in order to ensure the integrity, confidentiality and availability of information.

PR.DS-01: Stored data is protected

5_C. In the case of administrative critical data and services, the provisions of the requirement referred to in point 4_0 shall not apply. With regard to the processing of Metadata relating to the administration, the provisions of point 3_O. remain in force.

PR.DS-02: Data is protected during transmission

1_C. Secure and encrypted communication channels shall be used when migrating servers, services, applications or data to cloud environments. These channels must only include up-to-date and approved protocols.

2_C. In accordance with the risk analysis referred to in measure ID.RA-05, secure and encrypted communication channels and up-to-date and approved protocols shall be used for data flows and communications referred to in measure ID.AM-03.

PR.DS-03: Physical transfer, removal and destruction of data storage devices shall be managed through a formal process

1_C. In relation to the ID.AM category, at least the following shall be defined:

a. the security policies adopted for the physical transfer, removal and destruction of data storage devices;

b. the processes, methodologies and technologies used that contribute to compliance with security policies.

PR.DS-07: Development and testing environments are separated from the production environment

1_C. In relation to the ID.AM category, at least the following shall be defined:

a. the general architecture by which the environments are separated and, at any points of contact, how the separation is achieved;

b. the security policies adopted to ensure the separation of the development and testing environment from the production environment;

c. the processes, methodologies and technologies used that contribute to compliance with security policies.

3.3.7) Information Protection Processes and Procedures (PR.IP): Security policies (which address the purpose, scope, roles and responsibilities, management commitment and coordination between the various organizational entities), processes and procedures to manage the protection of information systems and assets shall be implemented and adapted over time.

PR.IP-03: Configuration change control processes are in place

1_C. *The following shall be defined:*
- *a. the security policies adopted for updating the configurations of IT and industrial control systems and for controlling changes in the configurations in use compared to those envisaged;*
- *b. the processes, methodologies and technologies used that contribute to compliance with security policies.*

2_C. *A procedure is implemented for managing exceptions, including emergencies, in the change and configuration process.*

3_C. *Plans for restoration to the previous state (the so-called rollback) are defined and implemented in case of errors or security issues.*

PR.IP-04: Information backups are executed, administered and verified

3_C. *There is an updated document detailing, also in relation to the ID.AM category, at least:*
- *a. the security policies adopted for the backup of information;*
- *b. the processes, methodologies and technologies used that contribute to compliance with security policies.*

PR.IP-09: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and administered in the event of an incident/disaster

1_C. *There is an updated, detailed document indicating the expected service levels of the digital infrastructure.*

2_C. *There is an updated, detailed document containing business continuity plans, as well as response plans in the event of incidents, which includes at least:*
- *a. the policies and processes used to identify event priorities;*
- *b. the phases for implementing the plans;*
- *c. the roles and responsibilities of the personnel;*
- *d. communication and reporting flows;*
- *e. the coordination with CSIRT Italia.*

3_C. *There is an updated document listing the education, training and exercise activities carried out.*

4_C. *Business continuity plans shall be tested and communicated to stakeholders.*

5_C. *The documentation referred to in point 2_C. shall be made available, where required, to the Administration and shall be reviewed periodically.*

6_C. *The impact resulting from interruption and possible risks shall be determined in order to establish criteria for developing business continuity strategies and capabilities.*

3.3.8) Maintenance (PR.MA): Maintenance of information systems and industrial control is done in accordance with existing policies and procedures.

PR.MA-01: Maintenance and repair of resources and systems shall be carried out and recorded with controlled and authorised tools

1_C. *In relation to the ID.AM category, the following shall be defined:*
- *a. the security policies adopted for the recording of maintenance and repair of resources and systems;*
- *b. the processes, methodologies and technologies used that contribute to compliance with security policies.*

PR.MA-02: Remote maintenance of resources and systems is approved, documented and carried out in order to avoid unauthorised access

3_C. *Strict protection mechanisms shall be adopted for authentication, identification and event tracking.*

4_C. *Mechanisms for the management and control of privileged users shall be adopted, in terms of temporal limitations and available administrative functions.*

5_C. *All logs relating to remote communication sessions and activities performed on remote systems shall*

be produced and stored on systems separate from those subject to intervention and not accessible by remote users.

3.3.9) Protective Technology (PR.PT): Technical security solutions are managed to ensure security and resilience of systems and assets, consistent with related policies, procedures and agreements.

PR.PT-01: A policy exists and is executed to define, implement and review system logs

1_C. *Logs are stored in a secure, possibly centralised manner for at least 24 months*

2_C. *The following shall be defined:*

a. the security policies adopted for the management of system logs;

b. the processes, methodologies and technologies used that contribute to compliance with security policies with particular regard to the integrity and availability of logs.

PR.PT-04: Communication and control networks are protected

2_C. *Intrusion prevention systems (IPS) are present, updated, maintained and well configured.*

3_C. *The technical tools referred to in points 1_O. and 2_C. shall contribute to compliance with the policies referred to in categories ID.AM, ID.GV, ID.SC, PR.AC and PR.DS.*

PR.PT-05: Mechanisms (e.g. failsafe, load balancing, hot swap) are implemented, which allow resilience requirements to be met both during normal operation and in adverse situations

1_C. *In relation to the plans provided for in the subcategory PR.IP-09:*

a. redundant network, connectivity and application architectures shall be adopted.

2_C. *Mechanisms exist to ensure business continuity, in compliance with the security measures listed herein.*

3_C. *The following shall be defined:*

a. the security policies adopted in relation to points 1_C. and 2_C.;

b. the processes, methodologies and technologies used that contribute to compliance with security policies.

DETECT (DE)

3.3.10) Anomalies and Events (DE.AE): Anomalous activities shall be detected and their potential impact shall be analysed.

DE.AE-03: Event information shall be collected and correlated by multiple sensors and sources

1_C. *In order to promptly detect incidents with an impact on the Digital Infrastructure, technical and procedural tools shall be adopted to:*

a. acquire information from multiple sensors and sources;

b. receive and collect information concerning the security of the digital infrastructure disclosed by CSIRT Italia, from sources internal or external to the entity;

c. analyse and correlate, also in an automated manner, the data and information referred to in points (a) and (b), in order to promptly detect events of interest.

2_C. *The analysis and correlation activities referred to in the previous point shall be monitored and recorded. The relevant documentation, including electronic documentation, shall be stored for at least 24 months.*

3_C. *The following shall be defined:*

a. the policies applied to detect the sensors and sources referred to in point 1_C.(a);

b. the procedures and technical tools for obtaining the information referred to in points 1_C.(a) and (b);

c. the policies, processes and technical tools for the analysis and correlation referred to in point 1_C. (c);

d. the processes and technical tools for the monitoring and recording referred to in point 2_C.

4_C. *There are policies and procedures for the logging, monitoring, security and storage of access logs, which must be updated at least on an annual basis.*

5_C. *An auditing system is adopted for activities related to the detection of security information, monitoring of unauthorised access, change or deletion of data or metadata.*

6_C. *Processes, procedures and technical measures for reporting anomalies and failures of the monitoring system shall be defined and evaluated and capable of providing immediate notification to the responsible entity.*

3.3.11) Security Continuous Monitoring (DE.CM): Information systems and assets are monitored to identify cybersecurity events and to verify the effectiveness of protection measures.

DE.CM-07: Monitoring shall be carried out to detect unauthorised personnel, connections, devices or software

1_C. *With reference to subcategory PR.AC-03, the presence of personnel with potential unauthorised physical or remote access to the resources shall be detected. To this end, there are surveillance and access control systems, including automated systems.*

2_C. *With reference to subcategory ID.AM-01, non-approved devices (including physical devices) shall be detected. To this end, without prejudice to documented technical limitations, at least network access control systems shall be in place.*

3_C. *The technical tools referred to in points 1_C. and 2_C. shall be updated, maintained and well configured, in accordance with the policies set out in the categories PR.AC, PR.DS, PR.IP and PR.MA and contribute to compliance with the policies set out in the categories ID.AM, ID.GV, ID.SC, PR.AC and PR.DS.*

4_C. *There is an updated document describing, at least:*

a. the security policies adopted in relation to points 1_C. and 2_C.;

b. the processes, methodologies and technologies used that contribute to compliance with security policies.

3.3.12) Detection Processes (DE.DP): Monitoring processes and procedures shall be adopted, maintained and verified to ensure the understanding of anomalous events.

DE.DP-01: Roles and responsibilities for monitoring processes are well defined in order to ensure accountability

1_C. *The appointments referred to in subcategory ID.AM-06 are disclosed within the entity.*

2_C. *The roles, processes and responsibilities for activities leading to the detection of incidents with an impact on the digital infrastructure are well defined and disclosed to the competent bodies of the entity.*

3_C. *There is an updated document detailing at least:*

a. the roles, processes and responsibilities referred to in point 2_O.;

b. the processes for the dissemination of appointments, roles and processes referred to in points 1_O. and 2_O.

4_C. *A system is defined and implemented for notifying the Administration of anomalous events involving the applications and the underlying infrastructure, which shall be identified on the basis of previously agreed metrics.*

RESPOND (RS)

3.3.13) Response Planning (RS.RP): Response procedures and processes shall be carried out and maintained to ensure a response to detected cybersecurity incidents.

RS.RP-01: There is a response plan, and this is executed during or after an incident

1_C. *The response plan provides for the timely execution of the evaluation of the events detected through the analysis and correlation referred to in the DETECT (DE) category as well as the immediate dissemination of the results to the competent bodies of the entity, also for the purpose of notification to the Administration and, on a voluntary basis, to the CSIRT Italia, of incidents with an impact on the digital infrastructure.*

3.3.14) Communications (RS.CO): Response activities are coordinated with the internal and external parties (e.g. possible support from law enforcement bodies or law enforcement agencies).

RS.CO-01: The personnel are aware of their role and what they need to do if a response to an incident is necessary

- ***1_C.*** *The roles and responsibilities for carrying out the phases and processes of responding to an incident are well defined and disclosed to the competent bodies of the entity.*
- ***2_C.*** *Exercises are performed periodically.*
- ***3_C.*** *There is an updated document detailing at least:*
  - *a. the phases, processes, roles and responsibilities referred to in points 1_O. and 2_C.;*
  - *b. the processes for the dissemination of the phases, processes, roles and responsibilities referred to in points 1_O. and _C.2;*
  - *c. the procedures for the exercises referred to in point 3.*
- ***4_C.*** *The entity shall notify the Administration of an incident or data breach within 1 hour of the recording and classification of the event.*
- ***5_C.*** *There are policies and procedures for the management of security incidents, E-Discovery and Cloud Forensics, which must be reviewed and updated at least on an annual basis.*

RS.CO-05: Spontaneous sharing of information with stakeholders outside the organisation (information sharing) is implemented to achieve greater awareness of the situation (the so-called situational awareness).

- ***1_C.*** *Contacts shall be established and maintained with interest groups related to the Digital Infrastructure and Cyber Security, as well as with other relevant entities in line with the entity's context in relation to the Digital Infrastructure.*
- ***2_C.*** *Points of contact with applicable regulatory authorities, national and local law enforcement agencies and other legal courts shall be established and maintained.*

3.3.15) Analysis (RS.AN): Analyses are carried out to ensure an effective response and support to recovery activities.

RS.AN-05: Processes are defined to receive, analyse and respond to information about vulnerabilities disclosed by sources inside or outside the organisation (e.g. internal testing, security bulletins, or security researchers).

- ***1_C.*** *The communication channels of the CSIRT Italia referred to in Article 4 of the Decree of the President of the Council of Ministers of 8 August 2019, of the reference Authority of its production sector, as well as of any reference CERT and Information Sharing & Analysis Centre (ISAC) shall be monitored.*
- ***2_C.*** *The results of the evaluations referred to in the subcategory DE.AE-03 and of the penetration tests and vulnerability assessments referred to in the subcategory DE.CM-08 shall be disseminated to the competent bodies of the entity.*
- ***3_C.*** *There is an updated document describing, at least:*
  - *a. the procedures for receiving, analysing and responding at least to the information collected through the activities referred to in points 1_O. and 2_O.;*
  - *b. the processes, roles, responsibilities and technical tools for carrying out the activities referred to in points 1_O. and 2_O.*

RECOVER (RC)

3.3.16) Recovery Planning (RC.RP): Recovery processes and procedures are performed and maintained to ensure a recovery of the systems or assets involved in a cybersecurity incident.

RC.RP-01: There is a recovery plan, which is executed during or after a cybersecurity incident

- ***2_C.*** *The recovery plan shall be tested on a six-monthly basis as part of two annual exercises.*

4. Minimum levels in the case of strategic data and services

4.1 Reliability

4.1.1) Business Continuity and Disaster Recovery.

A.BC-01: Disaster Recovery solutions are available with guaranteed recovery times

4_S. *In the case of administrative strategic data and services, the provisions of the requirement referred to in requirement A.BC-01, point 3_O shall not apply. In particular, with reference to requirement A.BC-01, point 1_O., the digital infrastructure shall be equipped with DR solutions, with features consistent with the risk analysis, and at least the following disaster recovery parameters must be ensured: RTO 24 hours and RPO 24 hours.*

4.2 Security

IDENTIFY (ID)

4.2.1) Asset Management (ID.AM): The data, personnel, devices, and systems and facilities necessary for the organisation are identified and managed in accordance with the objectives and risk strategy of the organisation.

ID.AM-06: Cybersecurity roles and responsibilities are defined and disclosed for all personnel and any relevant third parties (e.g. suppliers, customers, partners)

5_S. *The names and contact details of the person in charge referred to in point 2_O. and of the technical contact person referred to in point 3_O. shall be communicated by the subject to the National Cybersecurity Agency (ACN).*

4.2.2) Governance (ID.GV): Policies, procedures and processes to manage and monitor the organisation's requirements (organisational, legal, risk-related, environmental) are understood and used in cybersecurity risk management.

ID.GV-01: A cybersecurity policy is identified and disclosed

3_S. *Any deviation from the minimum security levels defined internally in the document referred to in point 1_O. shall be identified, managed and, where appropriate, authorised by the entity through a structured governance process.*

4_S. *There is an updated document indicating the planning, roles, implementation, operation, evaluation, and improvement of cybersecurity programs both in relation to internal personnel and any third parties.*

4.2.3) Risk Assessment (ID.RA): The enterprise understands the cybersecurity risk inherent in the organisation's operations (including mission, functions, image or reputation), the assets, and the individuals.

ID.RA-01: The vulnerabilities of the organisation's resources (e.g. systems, premises, devices) are identified and documented

3_S. *Periodic reports must contain at least:*

a. the general description of the types of checks carried out and the results thereof;

b. the detailed description of the vulnerabilities detected and their level of impact on security;

c. the level of exposure of system resources that can be accessed as a result of the exploitation of vulnerabilities.

4_S. *There is a document for correcting vulnerabilities, which also provides for notification to interested parties.*

4.2.4) Supply Chain Risk Management (ID.SC): The organisation's priorities, constraints, risk tolerances and assumptions are established and used to support risk decisions associated with supply chain risk management. The organisation has defined and implemented processes to identify, assess and manage supply chain risk.

ID.SC-01: Risk management processes inherent in the cyber supply chain are identified, well defined, validated, managed and approved by actors within the organisation

3_S. *Within the organisation, the policies and procedures for the definition, implementation and application*

of the Shared Security Responsibility Model (SSRM) with respect to external entities and/or third-party administrations are present and shall be updated at least on an annual basis.

4_S. *The SSRM model shall be applied to the entire cyber supply chain, including digital infrastructure.*

ID.SC-02: Third-party suppliers and partners of IT systems, components and services shall be identified, prioritised and assessed using a cyber supply chain risk assessment process.

1_S. *With regard to the award of supplies, measures shall be taken regarding the security of the supply chain through:*

a. the involvement of the cybersecurity organisation, including the person in charge referred to in subcategory ID.AM-06, point 2_O., in the supply process, already from the design phase;

b. without prejudice to documented technical limitations, the compliance with the fungibility requirement, with the possibility of resorting to another supplier upon expiry;

c. without prejudice to documented technical limitations, the diversification of suppliers and the consequent resilience of the digital infrastructure;

d. the assessment of the technical reliability of third-party suppliers and partners, with reference to best practices in this area and taking into account at least:

1) the quality of the products and cyber security practices of the third party supplier and partners, also considering their control over their supply chain and the priority given to security aspects;

2) the ability of the third party supplier and partners to ensure supply, service and maintenance over time.

2_S. *There is an updated list of third-party suppliers and partners entrusted for the supply of the Digital Infrastructure, as well as external dependencies, accompanied by the relevant documentation of the assessment process referred to in point 1_S.(d).*

3_S. *Where possible and in relation to the criticality, it is recommended to:*

a. assess the technical reliability referred to in point 1_S.(d), also taking into account:

1) the supplier's willingness to share the source code;

2) certifications or evidence useful for assessing the quality of the manufacturer's software development process;

3) the adoption, by the manufacturer, of technical procedures and tools to ensure the authenticity and integrity of the software or firmware installed within information and communication technology goods and systems;

4) the adoption, by the manufacturer, of technical procedures and tools to ensure a unique correspondence between the source code and the installed and executed object code;

b. adopt technical processes and tools to:

1) assess the quality and security of the source code, if made available by the manufacturer;

2) acquire the object code from the information and communication technology goods and systems;

3) confirm the unique correspondence between the source code and the installed and executed object code.

ID.SC-03: Contracts with third party suppliers and partners are used to implement appropriate measures designed to meet the objectives of the organisation's cybersecurity program and cyber supply chain risk management plan

1_S. *The security measures implemented by the entity in relation to internal dependencies are consistent, also in relation to the outcomes of the risk analysis, with the security measures applied to the digital infrastructure. To this end, contracts, agreements or conventions shall be updated accordingly.*

2_S. *The security measures implemented by third party providers of external services are consistent, also in relation to the outcomes of the risk analysis, with the security measures applied to the digital infrastructure. To this end, contracts, agreements or conventions shall be updated accordingly.*

ID.SC-04: Third-party suppliers and partners shall be regularly assessed using audits, checks, or other forms of assessment to confirm compliance with contractual obligations

1_S. *There is an updated document describing the process, methods, frequency of assessments for third-party suppliers and partners, proportionate to the outcomes of the risk analysis carried out.*

2_S. *There is an up-to-date schedule of planned audits, checks, or other forms of assessment, as well as a*

register of those carried out and related documentation.

3_S. *An Audit Management process is defined and implemented in order to allow independent assessments and assurance, in compliance with the main industry standards, at least on an annual basis and according to a risk-taking planning.*

4_S. *Audit and standards assurance policies and procedures must be established, documented, approved, maintained and reviewed at least on an annual basis.*

5_S. *A remediation plan, relating to corrective actions related to non-compliances detected on third party suppliers and partners, is defined, documented, approved, communicated, implemented and maintained.*

PROTECT (PR)

4.2.5) Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and related resources is limited to authorised personnel, processes and devices, and is managed in a manner consistent with the assessment of the risk of unauthorized access to authorised activities and transactions.

PR.AC-03: Remote access to resources is administered

7_S. *Policies and procedures shall be updated at least on an annual basis and made available for consultation, upon specific request, by the entity.*

8_S. *A joint authorisation process with the Administration is defined and implemented in the event that its data is accessed. If this is not possible, the entity shall contact the Administration as quickly as possible informing it of the accesses made.*

9_S. *All operations that provide access to the Administration's data must be managed in line with the user management and logging policies for privileged users.*

PR.AC-04: Rights of access to resources and their authorisations shall be administered in accordance with the principles of least privilege and separation of duties

5_S. *The entity is autonomous in the management of the infrastructure, having its own capabilities to operate the underlying physical and logical infrastructure. For exceptional cases and on the basis of documented technical limitations, the entity may rely on third-party expertise, ensuring, where possible, fungibility.*

PR.AC-05: Network integrity is protected (e.g. network segregation, network segmentation)

3_S. *With reference to censuses referred to in the ID.AM category, there is an updated, detailed document containing at least:*

a. the security policies adopted for segmentation/segregation of networks;

b. the description of the segregated/segmented networks;

c. the processes, methodologies and technologies used that contribute to compliance with security policies;

d. the ways in which network ports, protocols and services in use are limited and/or monitored.

PR.AC-07: Authentication methods (e.g. single-factor or multiple-factor authentication) for the entity's users, devices and other assets are commensurate with the risk of the transaction (e.g. risks related to the security and privacy of individuals and other organizational risks)

2_S. *There is an updated, detailed document that, with reference to the censuses referred to in the ID.AM category and to the risk assessment referred to in the ID.RA category, shall contain at least:*

a. the available authentication methods;

b. their assignment to transaction categories.

4.2.6) Awareness and Training (PR.AT): The personnel and third parties are sensitised about cybersecurity and are trained to fulfil their tasks and roles consistently with existing policies, procedures and agreements.

PR.AT-01: The personnel of the entity are informed and trained

3_S. *For each member of the entity's personnel, there is an up-to-date register, including the instructions*

received.

PR.AT-02: Privileged users (e.g. System administrators) understand their roles and responsibilities

3_S. *There is an updated, detailed document containing the processes referred to in points 1_O. and 2_O.*

4.2.7) Data Security (PR.DS): The data is stored and managed in accordance with the organisation's risk management strategy, in order to ensure the integrity, confidentiality and availability of information.

PR.DS-01: Stored data is protected

6_S. *With regard to access to data by non-EU entities, the entity shall:*

a. report to the National Cybersecurity Agency (ACN) and administration any requests for access to data or metadata by non-EU entities;

b. provide access to administration data or metadata to non-EU entities only after explicit authorisation from the administration.

7_S. *Technical procedures and measures are defined and implemented for the destruction of keys stored outside a secure environment and the revocation of keys stored in hardware security modules (HSMs) when they are no longer needed, in accordance with legal and regulatory requirements.*

8_S. *In the case of administrative strategic data and services, the provisions of the requirement referred to in point 3_O shall not apply. In this respect, all types of metadata must be processed through infrastructure located in the territory of the European Union, with the exception of those necessary for the provision of the services referred to in point 2_O.*

PR.DS-03: Physical transfer, removal and destruction of data storage devices shall be managed through a formal process

2_S. *Remote geolocation capabilities are enabled for all managed mobile devices that, if compromised, may have an impact on the availability, integrity or confidentiality of the infrastructure or services provided by it.*

3_S. *In line with the provisions of point 2_S., adequate techniques for remote deletion of the Administration's data are defined and implemented.*

4_S. *There is an updated, detailed document containing the processes and policies referred to in point 1_C.*

PR.DS-05: Protection techniques (e.g. access control) are implemented against data leaks

3_S. *There is an updated, detailed document containing the processes and policies referred to in point 1_O.*

PR.DS-06: Data integrity control mechanisms are used to verify the authenticity of software, firmware and information

2_S. *There is an updated, detailed document containing the processes and policies referred to in point 1_O.*

PR.DS-07: Development and testing environments are separated from the production environment

2_S. *There is an updated, detailed document containing the processes and policies referred to in point 1_C.*

4.2.8) Information Protection Processes and Procedures (PR.IP): Security policies (which address the purpose, scope, roles and responsibilities, management commitment and coordination between the various organizational entities), processes and procedures to manage the protection of information systems and assets shall be implemented and adapted over time.

PR.IP-01: Reference practices (so-called baseline) are defined and managed for the configuration of IT and industrial control systems incorporating security principles (e.g. principle of least functionality).

2_S. *There is an updated document detailing, also in relation to the ID.AM category, at least:*

a. the security policies adopted for the development of IT system configurations and deployment of the adopted configurations alone;

b. the list of IT system configurations used and the reference to the relevant reference practices;

c. the processes, methodologies and technologies used that contribute to compliance with security policies.

3_S. *Basic requirements for the security of the various applications are defined and documented.*

4_S. *Technical metrics are defined and implemented to monitor the level of adherence to the defined security requirements and compliance obligations.*

5_S. *There is a process of application vulnerability mitigation and recovery for application security, automating repair whenever possible.*

6_S. *There is a process for validating device compatibility with operating systems and applications.*

7_S. *There is a system for managing changes in terms of operating system, patching and/or applications.*

PR.IP-03: Configuration change control processes are in place

4_S. *There is an updated, detailed document containing the processes and policies referred to in point 1_C.*

PR.IP-09: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and administered in the event of an incident/disaster

7_S. *There is an updated, detailed document indicating the service levels expected from the Digital Infrastructure and, if applicable, from the hot-replicas and/or cold-replicas as well as from the disaster recovery site(s).*

8_S. *There is an updated, detailed document containing disaster recovery plans, as well as response and recovery plans in the event of incidents, which shall include at least:*

a. the policies and processes used to identify event priorities;

b. the phases for implementing the plans;

c. the roles and responsibilities of the personnel;

d. communication and reporting flows;

e. the coordination with CSIRT Italia.

9_S. *There is an updated document listing the education, training and exercise activities carried out.*

10_S. *Disaster recovery strategies shall be tested and communicated to stakeholders.*

11_S. *Devices critical to the operation of the infrastructure shall be redundant and, if located in different locations, at a distance in line with industry best practices.*

PR.IP-11: Cybersecurity issues are included in personnel management processes (e.g.: screening, deprovisioning)

1_S. *The entity shall make the methodology used for the verification of the personnel (vetting process methodology) with privileged access to the infrastructure or administrative data available to the administration.*

2_S. *The entity shall make the list of employees with privileged access to the infrastructure or administrative data available to the administration. The administration may unilaterally request the removal of one or more employees from the aforementioned list and the entity shall promptly do so.*

PR.IP-12: A vulnerability management plan is developed and implemented

3_S. *The document referred to in point 1_O. must be updated on a six-monthly basis.*

4_S. *Technical measures are defined and implemented for the identification of updates for applications that use third-party or open libraries, in compliance with internal vulnerability management policies.*

4.2.9) Maintenance (PR.MA): Maintenance of information systems and industrial control is done in accordance with existing policies and procedures.

PR.MA-01: Maintenance and repair of resources and systems shall be carried out and recorded with controlled and authorised tools

2_S. *There is an up-to-date register of maintenance and repairs performed.*

3_S. *There is an updated, detailed document containing the processes and policies referred to in point 1_C.*

4_S. *Based on risk analysis, any update of software deemed critical, without prejudice to justified security-related timeliness, must be verified in the testing environment before actual use in the operational environment, and the relevant object code must be stored for at least 24 months.*

5_S. *Based on the risk analysis referred to in measure ID.RA-05, any hardware or software updating of components deemed critical, without prejudice to justified security-related timeliness, must be verified in the testing environment before actual use in the operational environment and, where appropriate,*

the relevant object code must be stored for at least 24 months. Activities in the testing environment are also aimed at verifying security aspects.

6_S. *Software updates should only be allowed from pre-authorised sources.*

7_S. *All logs relating to maintenance and updating activities must be produced and stored on systems separate from those subject to intervention and not accessible to users who carry out these activities.*

8_S. *There is an updated document describing, at least, the processes and technical tools used to achieve points 5_S., 6_S. and 7_S..*

PR.MA-02: Remote maintenance of resources and systems is approved, documented and carried out in order to avoid unauthorised access

6_S. *There is an updated, detailed document describing, at least, the processes and technical tools used to achieve points 2_O., 3_C., 4_C. and 5_C.*

4.2.10) Protective Technology (PR.PT): Technical security solutions are managed to ensure security and resilience of systems and assets, consistent with related policies, procedures and agreements.

PR.PT-01: A policy exists and is executed to define, implement and review system logs

3_S. *There is an updated, detailed document containing the processes and policies referred to in point 1_C.*

PR.PT-04: Communication and control networks are protected

1_S. *Perimeter systems, such as firewalls, also at the application level, are present, updated, maintained and well configured.*

2_S. *Intrusion prevention systems (IPS) are present, updated, maintained and well configured.*

3_S. *The technical tools referred to in points 1_O. and 2_C. shall contribute to compliance with the policies referred to in categories ID.AM, ID.GV, ID.SC, PR.AC and PR.DS.*

4_S. *The updating, maintenance and configuration of the technical tools referred to in points 1_O. and 2_C. shall be carried out in accordance with the policies set out in the categories PR.AC, PR.DS, PR.IP and PR.MA.*

5_S. *The technical tools referred to in points 1_O. and 2_C. shall also be used for the purposes referred to in the DETECT (DE) function.*

6_S. *There is an updated document describing, at least, the processes and technical tools used to achieve points 1_O., 2_C., 3_C., 4_S and 5_S.*

PR.PT-05: Mechanisms (e.g. failsafe, load balancing, hot swap) are implemented, which allow resilience requirements to be met both during normal operation and in adverse situations

4_S. *In relation to the plans provided for in the subcategory PR.IP-09:*
a. there is a disaster recovery site, with features consistent with the risk analysis.

5_S. *There is an updated, detailed document containing the processes and policies referred to in points 1_C., 2_C., 3_C. and 4_S.*

DETECT (DE)

4.2.11) Anomalies and Events (DE.AE): Anomalous activities shall be detected and their potential impact shall be analysed.

DE.AE-03: Event information shall be collected and correlated by multiple sensors and sources

7_S. *There is a centralised repository containing the entity's user access logs, which is managed directly by the entity and logically segregated from systems to which third parties have direct access.*

8_S. *There is an updated, detailed document containing the processes and policies referred to in point 3_C.*

4.2.12) Security Continuous Monitoring (DE.CM): Information systems and assets are monitored to identify cybersecurity events and to verify the effectiveness of protection measures.

DE.CM-01: Computer network monitoring is carried out to detect potential cybersecurity events

3_S. *Incoming and outgoing traffic, the activities of perimeter systems such as routers and firewalls, significant administrative events, as well as executed or failed access to network resources and*

terminals shall be monitored and correlated in order to identify cybersecurity events.

4_S. *The technical tools referred to in points 1_O. and 3_S. shall be updated, maintained and well configured, in accordance with the policies set out in the categories PR.AC, PR.DS, PR.IP and PR.MA and contribute to compliance with the policies set out in the categories ID.AM, ID.GV, ID.SC, PR.AC and PR.DS.*

5_S. *The technical tools referred to in point 1_O. shall also be used for the purposes referred to in category DE.AE.*

6_S. *There is an updated document describing, at least:*

a. the security policies adopted in relation to point 2_O.;

b. the processes, methodologies and technologies used that contribute to compliance with security policies.

DE.CM-04: Malicious code shall be detected

3_S. *Appropriate firewall software is configured on all devices.*

4_S. *Incoming files (via email, downloads, removable devices, etc.) shall be analysed, also via sandbox.*

5_S. *The technical tools referred to in points 1_O., 3_S. and 4_S. shall be updated, maintained and well configured, in accordance with the policies set out in the categories PR.AC, PR.DS, PR.IP and PR.MA and contribute to compliance with the policies set out in the categories ID.AM, ID.GV, ID.SC, PR.AC and PR.DS.*

6_S. *There is an updated document describing, at least:*

a. the security policies adopted in relation to points 1_O., 2_O., 3_S. and 4_S.;

b. the processes, methodologies and technologies used that contribute to compliance with security policies.

DE.CM-07: Monitoring shall be carried out to detect unauthorised personnel, connections, devices or software

5_S. *With reference to subcategory ID.AM-02, without prejudice to documented technical limitations, there are control systems for detecting unapproved software.*

6_S. *With reference to subcategory ID.AM-03, there are control systems for detecting unauthorised connections.*

7_S. *The technical tools referred to in points 5_S. and 6_S. shall be updated, maintained and well configured, in accordance with the policies set out in the categories PR.AC, PR.DS, PR.IP and PR.MA and contribute to compliance with the policies set out in the categories ID.AM, ID.GV, ID.SC, PR.AC and PR.DS.*

8_S. *There is an updated document describing, at least:*

a. the security policies adopted in relation to points 5_S. and 6_S.;

b. the processes, methodologies and technologies used that contribute to compliance with security policies.

RESPOND (RS)

4.2.13) Response Planning (RS.RP): Response procedures and processes shall be carried out and maintained to ensure a response to detected cybersecurity incidents.

RS.RP-01: There is a response plan, and this is executed during or after an incident

2_S. *The policies and procedures for the timely management of security incidents shall be reviewed at least on an annual basis.*

3_S. *The response plan and the policies and procedures referred to in points 1_C. and 2_S. include critical internal departments, the Administration (if affected) and all third parties concerned.*

4_S. *Incident response plans shall be tested and updated at planned intervals or in the event of significant organisational or environmental changes.*

5_S. *The metrics of major cybersecurity incidents shall be defined and monitored.*

6_S. *Processes, procedures and measures to support business processes for the triage of security-related events are defined and implemented.*

7_S. *A Computer Emergency Response Team (CERT) must be implemented to coordinate the incident*

resolution phase in compliance with the ISO/IEC 27035-2 guidelines. In addition, the Administration must be involved at regular intervals to share and review the status of incidents of interest and, where appropriate, to resolve such incidents, also in accordance with the relevant contractual agreements.

4.2.14) Communications (RS.CO): Response activities are coordinated with the internal and external parties (e.g. possible support from law enforcement bodies or law enforcement agencies).

RS.CO-01: The personnel are aware of their role and what they need to do if a response to an incident is necessary

5_S. *There are policies and procedures for the management of security incidents, E-Discovery and Cloud Forensics, which must be reviewed and updated at least on an annual basis.*

6_S. *There is an up-to-date register of the exercises carried out and of the participants, with the relevant lessons learned.*

7_S. *Processes, procedures and technical measures for security breach notifications are defined and implemented.*

8_S. *A mechanism shall be provided for reporting any security breach, whether actual or presumed, including any supply chain breaches, in compliance with SLAs, applicable laws and regulations.*

9_S. *Response activities carried out following an incident shall be communicated to stakeholders internal and external to the organisation, including the organisation's executives and senior management.*
In particular, the recovery activities following an incident shall be communicated to the internal and external parties concerned (e.g. victims, ISPs, owners of the systems attacked, vendors, CERTs/CSIRTs), including the competent bodies of the entity, also for the purpose of possible dialogue with CSIRT Italia.

RECOVER (RC)

4.2.15) Improvements (RC.IM): Recovery plans and related processes shall be improved by taking into account the lessons learned for future activities.

RC.IM-02: Recovery strategies shall be updated

1_S. *The plan referred to in the RC.RP-01 subcategory shall be kept up-to-date also by taking into account the lessons learned during the recovery activities occurred.*

4.2.16) Communications (RC.CO): Recovery activities following an incident shall be coordinated with internal and external parts (e.g. victims, ISPs, owners of attacked systems, vendors, CERTs/CSIRTs).

RC.CO-03: Recovery activities carried out following an incident shall be communicated to stakeholders internal and external to the organisation, including the organisation's executives and senior management.

1_S. *Recovery activities following an incident shall be communicated to the internal and external parties concerned (e.g. victims, ISPs, owners of attacked systems, vendors, CERTs/CSIRTs).*

5. Minimum levels with deferred time limits for adoption

5.1. Please find below the list of requirements which must be complied with six months after the date of application of this Regulation, in addition to those immediately applicable on the date of entry into force:

- A.PS-01.2_C.
- DE.DP-01.1_O.
- DE.DP-01.2_O.
- ID.AM-06.5_C.
- PR.IP-04.1_Ob.
- PR.DS-02.2_C.
- PR.AC-01.1_O.b
- PR.AC-03.5_O.
- PR.PT-04.1_O.
- PR.PT-04.2_C.

- PR.PT-04.3_C.
- RS.AN-05.1_O.
- RS.CO-01.1_O.
- RS.CO-01.5_C..

6. Appendix

Table 1: Construction characteristics of the mechanical, electrical and fire fighting systems

Best practices ANSI/TIA492, National fire legislation

Topic	***Feature***
Protective measures against fire and smoke threats	*Protective measures against fire and smoke threats are implemented.*
Monitoring of operational and environmental parameters	*Data Center utility services and environmental conditions (water, electricity, temperature and humidity controls, telecommunications and connectivity) are protected, monitored, maintained and tested for ongoing effectiveness at scheduled intervals to ensure protection from unauthorised events. If the benchmark values of utility and environmental operating parameters are exceeded, the necessary measures to restore the control range must be initiated in a timely manner.*
Cooling system:	*The entity must ensure that the cooling system manages to keep the temperature under control even during the loss of the main power supply.*
Connectivity system redundancy	*The Data Center has a redundant network connectivity system through the use of at least two separate incoming carriers (multi-carrier connectivity).*
Geographical Site, proximity to waterways	*The distance of the DPC from the waterways is greater than 91 m.*
Geographical Site, proximity to motorway/railway arteries	*The distance of the DPC from motorway and railway arteries is greater than 91 m.*
Geographical Site, proximity to airports	*The distance of the DPC from airports is greater than 1.6 km.*
Proximity of the visitor car park to the perimeter walls of the Data Center	*The visitor car park has protective barriers to prevent the collision of vehicles with the external wall of facilities and computer rooms, at least 9.1 m away.*
Employee car park separated from the visitor car park	*The visitor car park is physically separated from the employee car park by a fence or wall and must have a separate entrance.*
Loading/unloading area separated from the car park	*The loading/unloading area is physically separated from the car park by a fence or wall with separate entrances, or by a system with physical access control, so as to eliminate interference between loading/unloading operations and passing cars.*
Redundant telecommunications wiring and horizontal paths	*Telecommunications wiring and horizontal paths are redundant.*
Fiber Access Wells	*Fiber access wells are at a distance of more than 20 m.*
Redundancy area dedicated to fiber certification with carrier/provider equipment	*The area dedicated to the certification of the fiber with the equipment of the carriers/providers from the entrance wells is redundant with direct and cross connection logic.*
Routers and Switches have redundant power supplies and control stations	*Routers and switches have redundant power supplies and control stations.*
Redundant routers and switches with redundant uplinks	*Routers and switches have redundant uplinks.*
Fire separation of corridors of the computer room and support areas	*Corridors for exiting the computer room and support areas shall be separated with fire-fighting solutions with a resistance of at least REI 60.*
Width of exit corridors	*The width of the exit corridors shall not be less than 1.2 m.*
Shipping area physically separated from other areas of the Data Center	*The shipping area is physically separated from the other areas of the Data Center.*

Number of loading docks in the shipping/receipt area	*There is at least one loading dock in the shipping/receipt area.*
Proximity between fuel storage rooms and generators	*Fuel storage rooms and generators for data rooms and support areas shall be separated from the data rooms and support areas with a compartmentation of at least REI 120. If outside, the requirements of the Fire Brigade shall be complied with.*
Control system, field devices and display devices under continuity	*The control system (CCTV, Access, Anti-intrusion), field devices and display devices are guaranteed continuity with a UPS dedicated to the control and display system or via local batteries on the field devices, with autonomy of 8 hours.*
Physical security personnel	*The physical security guard service is 24h/day.*
Access control at the gates of all the rooms of the Data center	*Control of access to the gates of all the rooms of the Data Center, including the main entrance, is carried out with badges or biometrics; there must be an anti-intrusion system, an open door/window alarm.*
Protective measures for telecommunications equipment racks/cabinets	*Telecommunications equipment racks/cabinets are attached at the base or supported at the top and base or are equipped with seismic platforms or other protective measures.*
Entrance to the building with guardhouse and surveillance desk	*At the entrance to the building there is a guardhouse and a surveillance desk for checking documents and authorisations, adequately protected (level 3 bulletproof glass requirement).*
Entrance to the building with fire doors and windows	*The entrance to the building is protected at least with REI 60 fire doors and windows. A specific permit issued by the Fire Brigade shall be deemed compliant.*
Building entrance protection	*The entrance to the building is protected with single-access interlocked doors, physical anti-climb and anti-passback systems.*
Administrative offices separated from the DPC area	*The administrative offices are separated from the Data Center area.*
Proximity of toilets or refreshment rooms to data rooms	*The toilets or refreshment rooms adjacent to the Data Center shall have an anti-flood system.*
Fire separation of toilets and refreshment rooms from data rooms and support areas	*The toilets and refreshment rooms adjacent to the Data Center are separated at least with REI 60 fire-resistant systems.*
CCTV control to all restricted areas with access via badge doors	*All restricted areas with access via badge doors shall be controlled with CCTV systems.*
CCTV of the gates with access control	*Access control gates shall be controlled with CCTV systems.*
CCTV recording of all activities on all cameras	*The retention period for CCTV recordings is at least 30 days.*
Frequency CCTV images (frame rate)	*The frequency of the CCTV images is at least 20 frames/sec.*
The electrical distribution system allows hot maintenance	*The electrical distribution system allows hot maintenance without exclusions.*
Analysis of the electrical system	*The electrical system has been subjected to analysis accompanied by a project report that must include short circuit power calculation, vertical coordination study, analysis of the electric arc and load flow study.*
Electrical cables for computers and telecommunications equipment	*Electrical cables for computers and telecommunications equipment are redundant with 100 % capacity on the remaining cable(s).*
UPS systems redundancy	*The redundancy of UPS systems is N+ 1.*
Automatic bypass and maintenance bypass	*An automatic bypass powered with dedicated switch and an external bypass switch for total UPS exclusion have been adopted.*
Electrical distribution output from UPS systems	*The electrical panel related to the electrical distribution output from the UPS has removable switches with adjustable long time and instantaneous trip functions.*
Type of batteries of UPS systems	*The batteries have been designed for 5-10 years of average life with static UPS or rotating UPS.*
Minimum battery life of UPS systems	*The minimum battery life is 10 minutes with static UPS or rotating UPS.*
Battery monitoring system for UPS systems	*The battery monitoring system is managed by the UPS at the battery bank level.*
UPS systems topology	*UPSs are redundant and distributed over modules or blocks.*

Bypass procedure for static switch maintenance	*The bypass procedure for maintenance of the switch is manual and guided with a mechanical locking device.*
Transformer	*The transformer is of the K-Rated/Harmonic Canceling type, (or equivalent technology) with high efficiency.*
Atmospheric discharge protection system	*An atmospheric discharge protection system has been adopted.*
Grounding of metal masses in the Computer Room	*The metal masses in the Computer Room have a grounding system.*
Monitored points	*The monitored points are at least the public power grid, the main transformer, the UPS, the generator, the status of the switches, the Static Transfer Switches and the Automatic Transfer Switch, the Power Distribution Units.*
Alarm notification method	*The method of notification of alarms triggered by monitoring takes place at the control room, via pagers, e-mails and/or SMS.*
Battery room separate from the UPS room	*The battery room is not separate from the UPS room unless required by the fire brigade. Separation is preferable.*
Insulated battery packs	*Individual battery packs are insulated from each other.*
Sizing of automatic electric backup generators (Standby generating system)	*The automatic electric backup generators are sized for the load of the entire building and with N+ 1 redundancy*
Single bar generators	*The electrical generators have appropriately sized power bars.*
Load bank availability	*A portable load bank (owned or rented) is available.*
Factory Acceptance Testing (FAT) on electrical equipment	*UPSs and generators have undergone factory acceptance tests (FTAs).*
In-production test procedure for electrical equipment	*The electrical equipment has been tested in production at component and system level using an appropriate procedure.*
Electrical equipment operating and maintenance personnel	*The electrical equipment operating and maintenance personnel is present on site on a 24/7 basis.*
Preventive maintenance of electrical equipment	*The generator and UPSs are subject to preventive maintenance.*
Operational staff training programme	*A training programme for operational staff has been established in relation to the regular operation of the equipment.*
Redundancy of mechanical equipment	*Mechanical equipment (e.g. air conditioning units, dry coolers, pumps, evaporative towers, capacitors) has a redundancy of N+ 1, in order to ensure hot maintenance operations. Redundancy features also apply to support areas that are not critical to the continuity of computer room operations. The manoeuvres to ensure hot maintenance can be manual.*
Passage of pipes not relating to the data center within the data center space	*The passage of pipes not relating to the Data Center within the DPC room is not permitted.*
Air pressure in the Computer Room and relevant areas	*The pressure inside the Computer Room and in areas relevant to the Computer Room is greater than that in the other areas.*
Drain wells in the Computer Room	*Inside the Computer room there are drain wells for condensation, for any humidification systems and for the sprinkler system, if present.*
Power supply to mechanical systems	*Mechanical systems shall be powered by the generator in the absence of the public power grid.*
Humidity control in the Computer Room	*Air humidity is monitored inside the Computer Room.*
Internal units of water cooling systems	*Internal units of water-cooled systems are redundant (each 5-8 units installed must be provided with an additional unit).*
Power supply to mechanical equipment	*The power supply to the systems is redundant (N+ 1) and configured to ensure hot maintenance.*
HVAC control system	*The ventilation and air conditioning control system is designed to ensure hot maintenance.*
Water-cooled systems, Restoration of the water level in the circuits	*For water-cooled systems, the restoration of the water level in the circuits must have two points of connection to the water supply network.*
Amount of fuel for the generators	*The amount of fuel for the generators guarantees an autonomy of 48 hours (subject to possession of a specific permit issued by the Fire Brigade).*
Fuel tanks for the generators	*There are multiple fuel tanks for the generators.*

Fuel pumping and piping for the generators	*Fuel pumping and piping for the generators are provided for each generator.*
Fire-fighting system	*There is a Sprinkler system for detecting and extinguishing fires in the office part of the building, or according to the requirements of the Fire Brigade.*
VESDA smoke detection for Computer Rooms and Entrance Rooms with active equipment or equivalent system	*In the computer rooms and in the entrance room, the fire-fighting system uses VESDA technology or an equivalent system for smoke detection.*
Automatic gas fire extinguishing for Computer Room and Entrance Room.	*In the computer rooms and in the entrance room there is an automatic gas fire extinguishing system, with the presence of active equipment.*
Anti-flooding system for Computer Room and Entrance Room with active equipment	*In the computer rooms and in the entrance room there is an anti-flooding system, with the presence of active equipment.*

REGULATION FOR DIGITAL INFRASTRUCTURE AND CLOUD SERVICES FOR PUBLIC ADMINISTRATION, PURSUANT TO ARTICLE 33-SEPTIES, PARAGRAPH 4, OF DECREE-LAW NO 179 OF 18 OCTOBER 2012, CONVERTED, WITH AMENDMENTS, BY LAW NO 221 OF 17 DECEMBER 2012

ANNEX 3

"BASIC QUALITY, SECURITY, PERFORMANCE AND SCALABILITY, INTEROPERABILITY, AND PORTABILITY FEATURES OF CLOUD SERVICES FOR PUBLIC ADMINISTRATION"

Summary

1. **Premise and definitions**

1.1. This Annex defines, in accordance with the provisions of Article 6 of the Regulation, the basic quality, security, performance and scalability, interoperability, and portability features of cloud services for public administrations that may host services and digital data, respectively, of the public administration classified, in accordance with the process referred to in Article 5 of the Regulation, as ordinary, critical or strategic.

1.2. The basic features are organised on the basis of the subcategories of the National Framework for Cybersecurity and Data Protection (hereinafter FNCS) and defined by taking into account the CSA Cloud Control Matrix (CCM). For each measure, a more detailed specification is provided of the expected minimum implementation and of the required modalities in order to describe its adoption and demonstrate its implementation.

1.3. The basic quality, security, performance and scalability, interoperability, and portability features of cloud services set out in this Annex shall apply to production environments. The basic quality, security, performance and scalability, interoperability, and portability features of pre-production, testing, development and similar environments shall be applied in accordance with the basic features set out in this Annex, where appropriate, in relation to a risk analysis aimed at identifying potential impacts on the service and its managed data or on the digital infrastructure related to the production environment.

1.4. For the purposes of this Annex, the following definitions shall apply:

a) 'administrative data' means data provided, stored, sent, received, processed by or on behalf of the administration by the entity through the cloud service;

b) 'administration metadata' means data collected, obtained or generated by the entity, including in derivative form, from administrative data, as part of the delivery and administration of the cloud service. This category includes, for example, the historicisation of system and service events, service configurations, and attributes of the administration's resources, also resulting from their use;

c) 'Metadata relating to the operation of the Cloud Service' means data generated and used by the entity to monitor and ensure the functionality of the Cloud Service, not included in the Administrative Metadata or Administrative Data. This category of Metadata, which must therefore not be referable to people, to the entity and cannot in any case allow the extraction - even in part - of administrative data, includes, for example, metrics on performance of use, balancing, etc.

d) 'external dependence' means networks, information systems, IT services, physical infrastructure or other services, including those used for maintenance and management purposes, which appertain to other entities, on which the operation of the digital infrastructure depends;
e) 'internal dependencies' means networks, information systems, IT services, physical infrastructure or other services, including those used for maintenance and management purposes, which are external to the cloud service, but appertain to the cloud service provider, on which the operation of the digital infrastructure depends;
f) 'cyber supply chain' means the digital infrastructure supply chain.

1.5. With the exception of the cybersecurity organisation, the term 'organisation', which appears within the descriptions of the categories and subcategories, shall be understood as referring at least to the infrastructure or staff of the cloud service provider responsible for its management. In addition, the term 'entity' shall be understood as 'cloud service provider'.

2. Basic features provided for in the case of ordinary data and services

2.1 Interoperability and portability

2.1.1) Interoperability

IP.IN-01: APIs are available for application functionality

1_O. *The SaaS service exposes to the Administration appropriate SOAP and/or REST APIs associated with application functionality, providing in particular the traceability of available versions and the traceability of requests received and processed. In addition, technical documentation on the exposed APIs and endpoints is available and can be used by the Administration. [SaaS].*

2.1.2) Remote management.

IP.GR-01: APIs are available for remote management of the service lifecycle

1_O. *Consistent with the type of cloud service provided, its environment must be accessible through API interfaces for remote service management, ensuring that the exposed APIs enable the implementation of tools for the automatic and remote management of the cloud service lifecycle.*

2_O. *Technical documentation on the exposed APIs and the SOAP and/or REST endpoints is available and can be used by the Administration.*

3_O. *With reference to points 1_O. and 2_O., the different versions of the APIs must be backward compatible with the one available at the time of the formalisation of the contract with the purchaser Administration.*

2.1.3) Portability

IP.PO-01: Features/APIs are available for data import/export

1_O. *Features and/or APIs are available to allow massive data export and import, ensuring the use of non-proprietary open formats.*

IP.PO-02: Data interoperability and portability shall be managed through regularly updated procedures and policies. Data portability involves the application of secure network protocols and access to data at the end of contractual relationships is managed through specific agreements.

1_O. *Interoperability and portability policies and procedures shall be established, which shall be reviewed and updated at least on an annual basis, including requirements for:*
a. Communications between application interfaces;
b. Interoperability of the processing of information;
c. Portability of application development;
d. Exchange, use, portability, integrity and persistence of information/data. [PaaS, SaaS].

2_O. *Encrypted and standardised network protocols are implemented for data management, import and*

export. [PaaS, SaaS].

3_O. *Provisions specifying the Administration's access to data at the end of the contract are included in the agreements, including:*

a. Data format;

b. How long the data will be stored for;

c. Scope of the data stored and made available to the Administration;

d. Data deletion policy. [PaaS, SaaS].

2.2 Performance and scalability

2.2.1) Features of the service.

PS.CA-01: The cloud service has typical features and complies with industry standards

1_O. *The cloud service shall ensure at least the following features, as per NIST SP 800-145:*

a. self-service provisioning: the cloud service unilaterally provides IT resources (for example, servers and cloud storage), as needed and automatically, without resorting to human interaction. The cloud service unilaterally meets the requests of the Administration for computational (or IT) resources, without explicit verification or approval;

b. access to the network: the cloud service offers multiple network connectivity options; at least one of which is based on the public network (e.g. the Internet);

c. elasticity: the entity implements automatic service provisioning and de-provisioning mechanisms, without prejudice to documented technical limitations, offering appropriate tools to the Administration.

2.2.2) Scalability of the service.

PS.SC-01: Transparency on modalities and mechanisms of scalability

1_O. *The entity communicates to the Administration:*

a. the scalability mechanism offered (e.g. automatic and configurable, native, manual);

b. the type (horizontal and/or vertical);

c. the maximum load conditions that can be borne by the service (e.g. number of concurrent users and/or volume of processable requests);

d. configuration modes (e.g. on the basis of monitoring metrics, planned over time);

e. the minimum response time of the service to the request for new resources (e.g. activation of new resources).

2_O. *The supplier makes available to the Administration transparent information about any additional ancillary features available for the service and configurable by the purchaser Administration to manage scalability and obtain better parameters.*

3_O. *For all the APIs exposed by the cloud service, compliance with the Interoperability Model, defined by AgID with the guidelines adopted pursuant to current legislation, must be declared.*

If the APIs displayed are compliant, the API specifications shall be shared in a machine readable format compatible with the indications of the interoperability model (e.g. OpenAPI3 for REST APIs, WSDL for SOAP APIs).

2.3 Quality

2.3.1) Service Level (SLA).

QU.LS-01: Compliance with mandatory service indicators is ensured, the methods for sharing the levels of service availability and any compensatory penalties are disclosed.

1_O. *The entity guarantees adherence to the objectives (Minimum Service Level Objective (SLO) corresponding to the following service level indicators (SLIs) and guarantees compliance therewith in contractual relationships in the form of service level agreements (SLAs):*

a. 99 % availability, where availability is understood as the percentage of time in a month in which the cloud service is accessible and usable, specifying that the total time of the reference period, which serves as the basis for calculating the percentage, does not take into account catastrophic events (catastrophic events are events that make the infrastructure used for the provision of the service

unavailable for an extended period of time and upon occurrence of which the Disaster Recovery solution is activated);

b. 'Technical support for emergencies', relating to the time at which the technical support service is operational for emergencies: 24 hours a day, 7 days a week throughout the year;

c. a maximum incident response time (meaning the maximum time between the reporting of an event with a critical impact on the Administration's operations and the entity's response) of 1 hour;

d. 'minor release', understood as the minimum period of notice provided to give notice, with release notes, to the Minor Release Administration (Minor Release is understood as changes to the service that mainly concern corrections of software malfunctions – bugs – or in any case the addition of new backward compatible features): 3 days;

e. 'major release', understood as the minimum period of notice provided to give notice, with release notes, to the Major Release Administration (Major Release is understood as changes to the service that concern a substantial evolution of the functionality of the service compared to the previous version): 1 month.

2_O. *Relative to those referred to in point 1_O., the entity may notify the administration of any further ones, or indicate new ones, which may be included as contractual commitments with specific Minimum Service Level Objective (SLO) in the contractual relationships.*

3_O. *The entity ensures that the method of sharing information on the guaranteed expected service levels (SLA) of the cloud service with the administration (e.g. periodic reports) is defined and that, should any change to the guaranteed service levels be required after the start of the supply, this must be notified in advance to the administration in order to obtain its approval.*

QU.LS-02: There are limitations for Service Level Agreements (SLAs) to prevent impacts on administration environments

1_O. *Within the Service Level Agreements (SLAs) between the entity and the administration there are limitations with regard to changes that directly impact on the environments and/or tenants owned by the administration.*

QU.LS-03: There are minimal contents and features for Service Level Agreements

1_O. *Each SLA between the entity and the administration shall take into account the following:*

a. Scope, characteristics and location of the business relationship and services offered;

b. Information security requirements (including the SSRM – Shared Security Responsibility Model, if applicable);

c. Change Management Process;

d. Logging and Monitoring;

e. Incident management and reporting procedures;

f. Right to audit and evaluation by third parties;

g. Methods of termination of service;

h. Interoperability and portability requirements;

i. Data confidentiality.

QU.LS-04: A monitoring service (alarms and parameters) is available and any native integrations with market leader solutions are disclosed

1_O. *The entity makes available to the administration access to one or more monitoring tools for the cloud service. They must allow collection, monitoring, filtering, reporting through default or parametrizable parameters and allow the administration to set custom alarms. The maximum granularity of operations must not exceed one minute (e.g., it must be possible to filter or collect events every minute). In addition, the entity specifies the possible availability of third-party APIs and monitoring tools natively integrated with the qualified service.*

2.3.2) Service quality (SE).

QU.SE-01: Systems for the management of the IT service and quality are adopted in accordance with industry standards

1_O. *The cloud service quality management system is formally adopted by the entity in accordance with*

UNI EN ISO 9001:2015-Quality Management Systems.

2_O. *The IT service management system of the cloud service is formally adopted by the entity in accordance with ISO/IEC 20000-1:2018-IT Service Management System.*

QU.SE-02: An adequate assistance and support service is provided

1_O. *Support and technical assistance to the administration for the cloud service is guaranteed.*

2_O. *The support and assistance service referred to in point 1_O. is provided at least in English from 08.00 to 18.00 (Italian time) on working days. At the request of the Administration, the support and assistance service referred to in point 1_O. is provided at least in Italian and/or for a longer time to cover all days of the year at any time (24 hours a day, 7 days a week throughout the year).*

3_O. *The support and assistance service referred to in point 1_O. shall be accessible at least by telephone and e-mail.*

4_O. *The support and assistance service referred to in point 1_O. also provides a support system for problem resolution (also called 'troubleshooting') available to the Administration, making it available, upon request of the administration, through APIs in order to allow programmatic interaction with problem management systems (Case Management System).*

QU.SE-03: The entity shall declare the frequency of updating of the service

1_O. *The entity must declare the expected frequency of updating of the qualified cloud service (e.g. frequency of scheduled releases).*

QU.SE-04: Guidelines and recommendations on the secure use of cloud solutions

1_O. *Guidelines for the secure management of the cloud service under qualification must be made available to the administration, addressing, where applicable, the following aspects:*

a. Instructions for a secure configuration;

b. Information on known vulnerabilities and updating mechanisms;

c. Error management and logging mechanisms;

d. Authentication mechanisms;

e. Roles and rights, including combinations resulting in high risk;

f. Services and functions for the administration of the service by privileged users;

g. The guidelines are provided and maintained in the manner and timing referred to in measure IP.GR-01.

2.4 Security

IDENTIFY (ID)

2.4.1) Asset Management (ID.AM): The data, personnel, devices, and systems and facilities necessary for the organisation are identified and managed in accordance with the objectives and risk strategy of the organisation.

ID.AM-01: The systems and physical equipment used in the organisation are registered.

1_O. *All systems and physical equipment are registered and there is a list of those approved by actors within the entity.*

2_O. *All systems and physical equipment present on the networks are registered and access to the network is allowed exclusively to the approved ones.*

ID.AM-02: Software platforms and applications in use in the organisation are registered

1_O. *All installed software platforms and applications are registered and there is a list of those approved by actors within the entity.*

2_O. *The installation of software platforms and applications is permitted only for approved ones.*

3_O. *There are policies that limit the addition, removal or update, as well as unauthorised management of the organisation's assets.*

ID.AM-03: Organisation-related data and communication flows are identified

1_O. *All data and information flows, including outward flows and flows related to the cloud service, are*

identified, registered and approved by actors within the entity.

ID.AM-06: Cybersecurity roles and responsibilities are defined and disclosed for all personnel and any relevant third parties (e.g. suppliers, customers, partners)

- ***1_O.*** *Cybersecurity organisation, also with reference to roles and responsibilities, for all personnel and any third parties is defined and disclosed to the competent bodies of the entity.*
- ***2_O.*** *Within the scope of the body referred to in point 1_O., a person in charge, and a possible substitute, possessing specific professionalism and expertise in the field of cyber security, shall be appointed with the task of managing the implementation of the provisions of the Regulation, who shall report directly to the hierarchical top of the entity and ensure the effective implementation of the security measures referred to in this Annex.*
- ***3_O.*** *Within the scope of the body referred to in point 1_O., a technical contact person, and at least one substitute, possessing technical and specialised expertise in the field of cyber security, shall be appointed to carry out the dialogue with CSIRT Italia for the purpose of managing incidents affecting the cloud service.*
- ***4_O.*** *The person in charge referred to in point 2_O. and the technical contact person referred to in point 3_O. shall operate in close cooperation.*

2.4.2) Governance (ID.GV): Policies, procedures and processes to manage and monitor the organisation's requirements (organisational, legal, risk-related, environmental) are understood and used in cybersecurity risk management.

ID.GV-01: A cybersecurity policy is identified and disclosed

- ***1_O.*** *There is an updated document describing cybersecurity policies, processes and procedures.*
- ***2_O.*** *The Document referred to in point 1_O. must be approved by the entity and updated at least on an annual basis or in case of substantial changes within the organisation.*

ID.GV-04: Governance and risk management processes include cybersecurity risk management

- ***1_O.*** *The updated document describing risk management processes includes the part related to cybersecurity risks.*
- ***2_O.*** *There is a formal Enterprise Risk Management (ERM) program that includes policies and procedures for the identification, assessment, ownership, processing and acceptance of the security and privacy risks of the cloud.*

2.4.3) Risk Assessment (ID.RA): The enterprise understands the cybersecurity risk inherent in the organisation's operations (including mission, functions, image or reputation), the assets, and the individuals.

ID.RA-01: The vulnerabilities of the organisation's resources (e.g. systems, premises, devices) are identified and documented

- ***1_O.*** *There is an updated security assessment and testing plan describing all activities aimed at assessing the level of cyber security of the cloud service and the effectiveness of the technical and procedural security measures, and which also contains the frequency and methods of implementation.*
- ***2_O.*** *There are procedures, to be updated at least on an annual basis, for the management of risks associated with changes in organizational assets, including applications, systems, infrastructure, configurations, etc., regardless of whether the assets are managed internally or externally (i.e. outsourced).*

ID.RA-05: Threats, vulnerabilities, their likelihood of occurrence and consequent impacts are used to determine the risk

- ***1_O.*** *The risk analysis shall be carried out on the basis of threats, vulnerabilities, their likelihood of occurrence and the consequent impacts resulting from their exploitation in the light of the threats considered.*
- ***2_O.*** *The risk analysis takes into account the internal and external dependencies of the cloud service.*
- ***3_O.*** *After identifying all the risk factors and analysing them, a weighting is carried out to determine the level of risk.*

2.4.4) Supply Chain Risk Management (ID.SC): The organisation's priorities, constraints, risk tolerances and assumptions are established and used to support risk decisions associated with supply chain risk management. The organisation has defined and implemented processes to identify, assess and manage supply chain risk.

ID.SC-01: Risk management processes inherent in the cyber supply chain are identified, well defined, validated, managed and approved by actors within the organisation

- ***1_O.*** *The processes for managing the risk inherent in the cyber supply chain are defined.*
- ***2_O.*** *These processes are validated and approved by the entity's top management.*

PROTECT (PR)

2.4.5) Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and related resources is limited to authorised personnel, processes and devices, and is managed in a manner consistent with the assessment of the risk of unauthorized access to authorised activities and transactions.

PR.AC-01: Digital identities and login credentials for authorised users, devices and processes are administered, verified, revoked and subject to security audits

- ***1_O.*** *Access credentials are individual for the staff of the entity or those involved in the administration of the service and comply with the principle of separation of duties. Credentials shall be updated at a rate commensurate with user privileges.*
- ***2_O.*** *There are policies and procedures for the management of credentials referred to in point 1_O., which must be updated at least on an annual basis and made available for consultation to the Administration.*
- ***3_O.*** *Mechanisms for managing, storing and reviewing information on credentials, system identity and access level are defined.*
- ***4_O.*** *The credentials shall be updated promptly and without undue delay if there are changes in users (e.g. transfer of personnel).*
- ***5_O.*** *System identities shall be managed by using digital certificates or alternative techniques that ensure an equivalent level of security.*
- ***6_O.*** *There is an updated planning of security audits to verify compliance with the provisions of points 1_O., 2_O., 3_O., 4_O. and 5_O. and there is a register of audits carried out with the relevant documentation.*

PR.AC-03: Remote access to resources is administered

- ***1_O.*** *Remote access is monitored by the cybersecurity organisation.*
- ***2_O.*** *Without prejudice to documented technical limitations, adequate access control measures are implemented, adopting systems of authentication, authorisation and centralised registration/accounting of accesses, supported by authentication systems, whose security is proportional to the risk.*
- ***3_O.*** *A centralised access management model is defined and implemented for processes of authorisation, logging and communication of access to administrative resources and data.*
- ***4_O.*** *There is a log of remote accesses.*
- ***5_O.*** *For remote access, multiple factor authentication methods are used.*

PR.AC-04: Rights of access to resources and their authorisations shall be administered in accordance with the principles of least privilege and separation of duties

- ***1_O.*** *With reference to censuses referred to in the ID.AM category, at least the following are defined:*
  - *a. the census resources that need to be accessed, with reference to the category ID.AM, for what functions and with what permissions;*
  - *b. user groups and their privileges in relation to the resources they can access and with what permissions;*
  - *c. the assignment of census users to user groups.*
- ***2_O.*** *When implementing access to the information system, principles of separation of duties and least privilege are observed in relation to organisational risk.*

3_O. *Policies, procedures and technical measures for the separation of duties in relation to privileged access are defined and implemented so that administrative access to data, encryption and key management capabilities, and logging capabilities are distinct and separate.*

PR.AC-05: Network integrity is protected (e.g. network segregation, network segmentation)

1_O. *There are policies and procedures for the security of the network infrastructure, which must be updated at least on an annual basis.*

2_O. *There is a planning for monitoring the availability, quality and adequate capacity of resources in order to provide the required system performance.*

PR.AC-07: Authentication methods (e.g. single-factor or multiple-factor authentication) for the entity's users, devices and other assets are commensurate with the risk of the transaction (e.g. risks related to the security and privacy of individuals and other organizational risks)

1_O. *Policies and procedures shall be defined and implemented for access to systems, applications and data, including multi-factor authentication at least for privileged users and access to data.*

2_O. *In relation to the cloud service, the Administration must be guaranteed multi-factor authentication features or the use of third-party multi-factor authentication solutions. Transparent information on available multi-factor authentication features must be made available to the National Cybersecurity Agency (ACN) and the Administration, with specifications on the mechanisms used for authentication (e.g. email, SMS or biometric check).*

2.4.6) Awareness and Training (PR.AT): The personnel and third parties are sensitised about cybersecurity and are trained to fulfil their tasks and roles consistently with existing policies, procedures and agreements.

PR.AT-01: The personnel of the entity are informed and trained

1_O. *There is an updated document detailing the contents of the training and education provided to the personnel of the entity and how to verify the acquisition of the contents.*

2_O. *The training and education referred to in point 1_O. provided to the users of the entity, in relation to the roles, shall include, at least, the following topics:*

a. the protection of the confidentiality of clear or encrypted data;

b. the return of company assets at the end of the employment relationship;

c. the definition of roles and responsibilities;

d. policies for access to systems, assets and resources;

e. information and security management policies;

f. processes for communicating roles and responsibilities to employees who have access to information assets;

g. requirements for non-disclosure/confidentiality of information.

PR.AT-02: Privileged users (e.g. System administrators) understand their roles and responsibilities

1_O. *The contents of the instructions provided to the privileged personnel of the entity and the methods for verifying the acquisition of the contents are defined.*

2_O. *The privileges and instructions received shall be defined for each member of the personnel of the entity.*

2.4.7) Data Security (PR.DS): The data is stored and managed in accordance with the organisation's risk management strategy, in order to ensure the integrity, confidentiality and availability of information.

PR.DS-01: Stored data is protected

1_O. *Administrative data, including security data (such as, but not limited to, access control systems), are processed through facilities located in the territory of the European Union. Unless justified and documented reasons of a regulatory or technical nature, these facilities shall include those assigned to the functions of:*

a. Business Continuity and Disaster Recovery, even if outsourced (e.g. via cloud computing);

b. Content Delivery Network with global geographic distribution.

In this case, the application of the ID.RA-05 measure must appropriately take into account the location

outside the European territory, also verifying compliance with the legislation on the protection of personal data.

2_O. *Unlike Metadata relating to the operation of the Service, which can be processed by facilities even located outside the territory of the European Union, Metadata relating to the administration shall be processed by facilities located in the territory of the European Union, unless justified and documented reasons of a regulatory or technical nature. In this case, the application of the ID.RA-05 measure must appropriately take into account the location outside the European territory, also verifying compliance with the legislation on the protection of personal data. In the event of Metadata being transferred to non-EU facilities, the interruption of this communication flow must not however result in non-compliance with the minimum service levels provided for the cloud service.*

3_O. *With reference to point 2_O., in the event that the Metadata relating to the administration are aimed at the provision of IT security services or for the resilience of the digital infrastructure, they may also be processed, in the presence of justified technical reasons and related evidence of their management in accordance with the uniformity of the purposes of the processing, outside the European territory. In this case, the application of the ID.RA-05 measure must appropriately take into account the location outside the European territory, also verifying compliance with the legislation on the protection of personal data. In the case of metadata being transferred to non-EU facilities, the interruption of this communication flow must not however result in non-compliance with the minimum service levels provided for the cloud service.*

4_O. *Also in relation to the ID.AM category, at least the following shall be defined:*

a. the security policies adopted for the storage and protection of data;

b. the processes, methodologies and technologies used that contribute to compliance with security policies.

5_O. *With reference to cryptographic keys:*

a. there is an updated document detailing encryption procedures, ciphering and key management, which must be updated at least on an annual basis, with a precise indication of roles and responsibilities;

b. periodic verification of encryption and key management systems, policies and processes is envisaged in response to increased risk exposure, assessed by audits to be carried out at least annually or after any security event;

c. the generation of cryptographic keys is envisaged through the use of cryptographic libraries, with an indication of the algorithm and the random number generator used;

d. there are mechanisms for the rotation of cryptographic keys according to the period of validity thereof, taking into account possible risks and regulatory and legal requirements.

6_O. *With reference to the cryptographic keys, at the request of the administration, the entity guarantees:*

a. autonomous management by the administration;

b. the generation of secret and private cryptographic keys for a unique purpose.

7_O. *Processes, procedures and technical measures are in place to revoke and remove cryptographic keys before the end of their validity period, when a key is compromised, or if an entity is no longer part of the organisation, in accordance with legal and regulatory requirements, consistent with the provisions in points 5_O. and 6_O.*

8_O. *Processes, procedures and measures are defined and implemented for the creation, deactivation of keys at the time of expiry, any suspensions and management mechanisms for cryptographic keys, consistent with the provisions in points 5_O. and 6_O.*

PR.DS-02: Data is protected during transmission

1_O. *Secure and encrypted communication channels shall be used when migrating servers, services, applications or data to cloud environments. These channels must only include up-to-date and approved protocols.*

PR.DS-03: Physical transfer, removal and destruction of data storage devices shall be managed through a formal process

1_O. *In relation to the ID.AM category, the following shall be defined:*

a. the security policies adopted for the physical transfer, removal and destruction of data storage

devices;

b. the processes, methodologies and technologies used that contribute to compliance with security policies.

PR.DS-05: Protection techniques (e.g. access control) are implemented against data leaks

1_O. *In relation to the ID.AM category, at least the following shall be defined:*

a. the security policies adopted for access to data;

b. the processes, methodologies and technologies used that contribute to compliance with security policies.

2_O. *Data Loss Prevention policies are adopted consistently with the risk assessment.*

PR.DS-06: Data integrity control mechanisms are used to verify the authenticity of software, firmware and information

1_O. *In relation to the ID.AM category, at least the following shall be defined:*

a. the list of data integrity control mechanisms to verify the authenticity of software, firmware and information;

b. the security policies adopted to assign a mechanism to a resource and which of these mechanisms is applied to which resource;

c. the processes, methodologies and technologies used that contribute to compliance with security policies.

PR.DS-07: Development and testing environments are separated from the production environment

1_O. *In relation to the ID.AM category, the following shall be defined:*

a. the general architecture by which the environments are separated and, at any points of contact, how the separation is achieved;

b. the security policies adopted to ensure the separation of the development and testing environment from the production environment;

c. the processes, methodologies and technologies used that contribute to compliance with security policies.

2.4.8) Information Protection Processes and Procedures (PR.IP): Security policies (which address the purpose, scope, roles and responsibilities, management commitment and coordination between the various organizational entities), processes and procedures to manage the protection of information systems and assets shall be implemented and adapted over time.

PR.IP-01: Reference practices (so-called baseline) are defined and managed for the configuration of IT and industrial control systems incorporating security principles (e.g. principle of least functionality).

1_O. *Policies and procedures relating to application security shall be defined to provide adequate support for the planning, implementation and maintenance of application security features, which must be reviewed and updated at least on an annual basis. [IaaS, SaaS].*

PR.IP-03: Configuration change control processes are in place

1_O. *The following shall be defined:*

a. the security policies adopted for updating the configurations of IT and industrial control systems and for controlling changes in the configurations in use compared to those envisaged;

b. the processes, methodologies and technologies used that contribute to compliance with security policies.

2_O. *A procedure is implemented for managing exceptions, including emergencies, in the change and configuration process.*

3_O. *Plans for restoration to the previous state (the so-called rollback) are defined and implemented in case of errors or security issues.*

PR.IP-04: Information backups are executed, administered and verified

1_O. *Also in relation to the ID.AM category, at least the following shall be defined:*

a. the security policies adopted for the backup of information;

b. the processes, methodologies and technologies used that contribute to compliance with security policies.

2_Oa. *A backup of the data stored in the cloud is performed periodically. The confidentiality, integrity and availability of backup data is ensured.*

2_Ob. *A backup is periodically made of the information stored in the cloud necessary for the complete recovery of the system, including administrative data and the data necessary for the restoration of the service. The confidentiality, integrity and availability of backup data is ensured. To this end, it is also ensured that media containing at least one of the copies are not permanently accessible by the system in order to prevent attacks on it from also involving all its backup copies.*

3_O. *Backup copies of information, software and system images of the cloud service are protected by adopting state-of-the-art cryptographic standards and industry best practices and stored regularly on remote sites (in compliance with the provisions of the PR.DS category). When backups are transmitted to a remote site over a network, transmission must be protected by adopting state-of-the-art cryptographic standards and industry best practices.*

4_O. *The restoration (restore test) of backup copies is periodically verified as a goal (SLO) at least once a year.*

PR.IP-09: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and administered in the event of an incident/disaster

1_O. *The impact resulting from business disruptions and possible risks shall be determined in order to establish criteria for developing business continuity strategies and capabilities.*

2_O. *There is an updated, detailed document containing business continuity plans, as well as response plans in the event of incidents, which includes at least:*

a. the policies and processes used to identify event priorities;

b. the phases for implementing the plans;

c. the roles and responsibilities of the personnel;

d. communication and reporting flows;

e. the coordination with CSIRT Italia.

3_O. *There is an updated document listing the education, training and exercise activities carried out.*

4_O. *Business continuity plans shall be tested and communicated to stakeholders.*

5_O. *The documentation referred to in point 2_O. shall be made available, where required, to the Administration and periodically reviewed.*

PR.IP-12: A vulnerability management plan is developed and implemented

1_O. *There is an updated document detailing at least:*

a. the security policies adopted to manage vulnerabilities;

b. the processes, methodologies and technologies used that contribute to compliance with security policies.

2_O. *Technical procedures and measures are defined and implemented to update detection tools, threat signatures and indicators of compromise, which must be reviewed and updated frequently or on a weekly basis. [SaaS].*

2.4.9) Maintenance (PR.MA): Maintenance of information systems and industrial control is done in accordance with existing policies and procedures.

PR.MA-01: Maintenance and repair of resources and systems shall be carried out and recorded with controlled and authorised tools

1_O. *Also in relation to the ID.AM category, at least the following shall be defined:*

a. the security policies adopted for the recording of maintenance and repair of resources and systems;

b. the processes, methodologies and technologies used that contribute to compliance with security policies.

PR.MA-02: Remote maintenance of resources and systems is approved, documented and carried out in order to avoid unauthorised access

- ***1_O.*** *Remote maintenance of resources and systems (including security-related activities) shall be carried out in accordance with the measures set out in subcategory PR.AC-03 and the following points.*
- ***2_O.*** *All access performed remotely by third-party personnel is authorised by the cybersecurity organisation and limited to essential cases only.*
- ***3_O.*** *Strict protection mechanisms shall be adopted for authentication, identification and event tracking.*
- ***4_O.*** *Mechanisms for the management and control of privileged users shall be adopted, in terms of temporal limitations and available administrative functions.*
- ***5_O.*** *All logs relating to remote communication sessions and activities performed on remote systems shall be produced and stored on systems separate from those subject to intervention and not accessible by remote users.*

2.4.10) Protective Technology (PR.PT): Technical security solutions are managed to ensure security and resilience of systems and assets, consistent with related policies, procedures and agreements.

PR.PT-01: A policy exists and is executed to define, implement and review system logs

- ***1_O.*** *Logs are stored in a secure, possibly centralised manner for at least 24 months.*
- ***2_O.*** *The following shall be defined:*
  - *a. the security policies adopted for the management of system logs;*
  - *b. the processes, methodologies and technologies used that contribute to compliance with security policies with particular regard to the integrity and availability of logs.*

PR.PT-04: Communication and control networks are protected

- ***1_O.*** *Perimeter systems, such as firewalls, also at the application level (including Web Application Firewall), are present, updated, maintained and well configured.*

PR.PT-05: Mechanisms (e.g. failsafe, load balancing, hot swap) are implemented, which allow resilience requirements to be met both during normal operation and in adverse situations

- ***1_O.*** *In relation to the plans provided for in the subcategory PR.IP-09:*
  - *a. redundant network, connectivity and application architectures shall be adopted.*
- ***2_O.*** *Mechanisms are in place to ensure continuity of service, in compliance with the established security measures.*
- ***3_O.*** *The following shall be defined:*
  - *a. the security policies adopted in relation to points 1_O. and 2_O;*
  - *b. the processes, methodologies and technologies used that contribute to compliance with security policies.*

DETECT (DE)

2.4.11) Anomalies and Events (DE.AE): Anomalous activities shall be detected and their potential impact shall be analysed.

DE.AE-03: Event information shall be collected and correlated by multiple sensors and sources

- ***1_O.*** *In order to promptly detect incidents with an impact on the cloud service, technical and procedural tools shall be adopted to:*
  - *a. acquire information from multiple sensors and sources;*
  - *b. receive and collect information related to the security of the cloud service disclosed by CSIRT Italia, from sources internal or external to the entity;*
  - *c. analyse and correlate, also in an automated manner, the data and information referred to in points a. and b., in order to promptly detect events of interest.*
- ***2_O.*** *The analysis and correlation activities referred to in the previous point shall be monitored and recorded. Documentation, including electronic documentation, relating to the analysis and investigation of the event is stored for at least 24 months.*
- ***3_O.*** *The following shall be defined:*
  - *a. the policies applied to detect the sensors and sources referred to in point 1_O.(a);*

b. the procedures and technical tools for obtaining the information referred to in point 1_O.(a) and (b);

c. the policies, processes and technical tools for the analysis and correlation referred to in point 1_O. (c);

d. the processes and technical tools for the monitoring and recording referred to in point 2_O.

4_O. *There are policies and procedures for the logging, monitoring, security and storage of access logs, which must be updated at least on an annual basis.*

5_O. *An auditing system is adopted for the detection of security information, monitoring of unauthorised access, change or deletion of data or metadata.*

6_O. *Processes, procedures and technical measures for reporting anomalies and failures of the monitoring system shall be defined and evaluated and capable of providing immediate notification to the responsible entity.*

7_O. *As part of the logging and monitoring activities, error management and logging tools are provided in relation to the cloud service, which allow the Administration to define the desired retention period and to obtain information about the security status of the cloud service and the data and functions it provides. The information shall be sufficiently detailed to allow verification of the following aspects, insofar as it is applicable to the cloud service:*

a. What data, services or functions available to the user within the cloud service have been accessed, by whom, and when (Audit Logs);

B. Malfunctions during the processing of automatic or manual actions.

8_O. *For the service subject to qualification, there must be the guarantee of the possibility to integrate the logs into the SIEM management and monitoring system of the Administration and that the log files can be easily exported by the Administration, preferably through API.*

2.4.12) Security Continuous Monitoring (DE.CM): Information systems and assets are monitored to identify cybersecurity events and to verify the effectiveness of protection measures.

DE.CM-01: Computer network monitoring is carried out to detect potential cybersecurity events

1_O. *Intrusion Detection Systems (IDS) are present.*

2_O. *Processes are present for monitoring events related to the security of applications and the underlying infrastructure.*

3_O. *An access monitoring system is provided in order to detect suspicious activities and establish a defined process for taking appropriate and timely actions in response to detected anomalies.*

DE.CM-04: Malicious code shall be detected

1_O. *Special tools for malware prevention and detection, as well as Endpoint Protection System (EPS), are implemented and used.*

2_O. *There are anti-malware protection policies, which will need to be reviewed at least on an annual basis.*

DE.CM-08: Scans are carried out for the identification of vulnerabilities

1_O. *Based on risk analysis, penetration tests and vulnerability assessments are performed on critical platforms and software applications before they are put into operation.*

2.4.13) Detection Processes (DE.DP): Monitoring processes and procedures shall be adopted, maintained and verified to ensure the understanding of anomalous events.

DE.DP-01: Roles and responsibilities for monitoring processes are well defined in order to ensure accountability

1_O. *The appointments referred to in subcategory ID.AM-06 are disclosed within the entity.*

2_O. *The roles, processes and responsibilities for activities leading to the detection of incidents with an impact on the cloud service are well defined and disclosed to the competent bodies of the entity.*

3_O. *There is an updated document detailing at least:*

a. the roles, processes and responsibilities referred to in point 2_O.;

b. the processes for the dissemination of appointments, roles and processes referred to in points 1_O. and 2_O.

4_O. *A system is defined and implemented for notifying the Administration of anomalous events involving the applications and the underlying infrastructure, which shall be identified on the basis of previously agreed metrics [PaaS, SaaS].*

RESPOND (RS)

2.4.14) Response Planning (RS.RP) Response procedures and processes shall be carried out and maintained to ensure a response to detected cybersecurity incidents.

RS.RP-01: There is a response plan, and this is executed during or after an incident

1_O. *The response plan provides for the timely execution of the evaluation of the events detected through the analysis and correlation referred to in the DETECT category (DE) as well as the immediate dissemination of the results to the competent bodies of the entity, also for the purpose of notification to the Administration and, on a voluntary basis, to the CSIRT Italia, of incidents with an impact on the cloud service.*

2.4.15) Communications (RS.CO): Response activities are coordinated with the internal and external parties (e.g. possible support from law enforcement bodies or law enforcement agencies).

RS.CO-01: The personnel are aware of their role and what they need to do if a response to an incident is necessary

1_O. *The roles and responsibilities for carrying out the phases and processes of responding to an incident are well defined and disclosed to the competent bodies of the entity.*

2_O. *Exercises are performed periodically.*

3_O. *There is an updated document detailing at least:*

a. the phases, processes, roles and responsibilities referred to in points 1_O. and 2_O.;

b. the processes for the dissemination of the phases, processes, roles and responsibilities referred to in points 1_O. and 2_O.;

c. the procedures for the exercises referred to in point 2_O.

4_O. *The entity shall notify the Administration of an incident or data breach within 1 hour of the recording and classification of the event.*

RS.CO-05: spontaneous sharing of information with stakeholders outside the organisation (information sharing) is implemented to achieve greater awareness of the situation (the so-called situational awareness).

1_O. *Contacts shall be established and maintained with interest groups related to the cloud and cyber security, as well as with other relevant entities in line with the entity's context.*

2_O. *Points of contact with applicable regulatory authorities, national and local law enforcement agencies and other legal courts shall be established and maintained.*

2.4.16) Analysis (RS.AN): Analyses are carried out to ensure effective response and support to recovery activities.

RS.AN-05: Processes are defined to receive, analyse and respond to information about vulnerabilities disclosed by sources inside or outside the organisation (e.g. internal testing, security bulletins, or security researchers).

1_O. *The results of the evaluations referred to in the subcategory DE.AE-3 and of the penetration tests and vulnerability assessments referred to in the subcategory DE.CM-08 shall be disseminated to the competent bodies of the entity.*

2_O. *The communication channels of the CSIRT Italia referred to in Article 4 of the Decree of the President of the Council of Ministers of 8 August 2019, of the reference Authority of its production sector, as well as of any reference CERT and Information Sharing & Analysis Centre (ISAC) shall be monitored.*

3_O. *There is an updated document describing, at least:*

a. the procedures for receiving, analysing and responding at least to the information collected through the activities referred to in points 1_O. and 2_O.;

b. the processes, roles, responsibilities and technical tools for carrying out the activities referred to in points 1_O. and 2_O.

2.4.17) Mitigation (RS.MI) Actions are performed to prevent the spread of a security event, to mitigate its effects and to resolve the incident.

RS.MI-03: New vulnerabilities are mitigated or documented as an accepted risk

1_O. *Vulnerabilities are mitigated in accordance with the Vulnerability Management Plan (PR.IP-12), i.e. the residual risk resulting from non-mitigation is documented and accepted.*

RECOVER (RC)

2.4.18) Recovery Planning (RC.RP): Recovery processes and procedures are performed and maintained to ensure a recovery of the systems or assets involved in a cybersecurity incident.

RC.RP-01: There is a recovery plan, which is executed during or after a cybersecurity incident

1_O. *There is a recovery plan that includes, at least, the processes and procedures necessary to restore the normal functioning of the cloud services affected by a cybersecurity incident.*

3. Basic features provided for in the case of critical data and services

3.1 Quality

3.1.1) Service quality (SE)

QU.SE-02: An adequate assistance and support service is provided

5_C. *In the case of administrative critical data and services, the provisions of measure QU.SE-02, point 2_O, shall not apply. The support and assistance service referred to in point 1_O. is provided, at least in Italian, every day of the year at any time (24 hours a day, 7 days a week throughout the year).*

3.2 Security

IDENTIFY (ID)

3.2.1) Asset Management (ID.AM): The data, personnel, devices and systems and facilities necessary for the organisation are identified and managed in accordance with the organisation's objectives and risk strategy.

ID.AM-06: Cybersecurity roles and responsibilities are defined and disclosed for all personnel and any relevant third parties (e.g. suppliers, customers, partners)

5_C. *The names and contact details of the person in charge referred to in point 2_O. and of the technical contact person referred to in point 3_O. shall be communicated by the subject to the National Cybersecurity Agency (ACN).*

6_C. *There is a list of all internal and external personnel employed in cybersecurity processes with specific roles and responsibilities. The list is disseminated to the competent bodies of the entity.*

7_C. *There is a list of figures similar to the person in charge referred to in point 2_O. and to the technical contact person referred to in point 3_O. at third parties, in relation to the external dependencies, and at the same entity, in relation to the internal dependencies. The competences of the person in charge and of the technical contact person must be reassessed according to the type of dependence. The list is disseminated to the competent bodies of the entity.*

8_C. *The person in charge referred to in point 2_O. shall also ensure cooperation with the National Cybersecurity Agency (ACN), also in relation to the activities related to Article 5 of Decree-Law 105/2019 and to the activities of prevention, preparation and management of cyber crises entrusted to the Cybersecurity Unit (NCS) referred to in Decree-Law 82 of 2021.*

3.2.2) Governance (ID.GV) The policies, procedures and processes to manage and monitor the organisation's requirements (organisational, legal, risk-related, environmental) are understood and used in cybersecurity risk management.

ID.GV-01: A cybersecurity policy is identified and disclosed

3_C. *Any deviation from the minimum security levels defined internally in the document referred to in point 1_O. shall be identified, managed and, where appropriate, authorised by the entity through a structured governance process.*

4_C. *There is an updated document indicating the planning, roles, implementation, operation, evaluation, and improvement of cybersecurity programs both in relation to internal personnel and any third parties.*

3.2.3) Risk Assessment (ID.RA): The enterprise understands the cybersecurity risk inherent in the organisation's operations (including mission, functions, image or reputation), the assets, and the individuals.

ID.RA-01: The vulnerabilities of the organisation's resources (e.g. systems, premises, devices) are identified and documented

3_C. *The periodic reports of the checks and tests referred to in point 1_O. must contain at least:*

a. the general description of the types of checks carried out and the results thereof;

b. the detailed description of the vulnerabilities detected and their level of impact on security;

c. the level of exposure of system resources that can be accessed as a result of the exploitation of vulnerabilities.

4_C. *There is a document for correcting vulnerabilities, which also provides for notification to interested parties.*

ID.RA-05: Threats, vulnerabilities, their likelihood of occurrence and consequent impacts are used to determine the risk

4_C. *There is an updated risk assessment document that includes at least:*

a. the identification of threats, both internal and external, appropriately described and assessed and their likelihood of occurrence;

b. vulnerabilities referred to in subcategory ID.RA-1 and in subcategory DE.CM-8;

c. the potential impacts deemed significant on the cloud service, appropriately described and assessed;

d. risk identification, analysis and weighting.

3.2.4) Supply Chain Risk Management (ID.SC): The organisation's priorities, constraints, risk tolerances and assumptions are established and used to support risk decisions associated with supply chain risk management. The organisation has defined and implemented processes to identify, assess and manage supply chain risk.

ID.SC-01: Risk management processes inherent in the cyber supply chain are identified, well defined, validated, managed and approved by actors within the organisation

3_C. *Within the organisation, the policies and procedures for the definition, implementation and application of the Shared Security Responsibility Model (SSRM) with respect to external entities and/or third-party administrations are present and shall be updated at least on an annual basis.*

4_C. *The SSRM model shall be applied to the entire cyber supply chain, including other cloud services used by the organisation.*

5_C. *A clear definition of the sharing of responsibilities is provided.*

ID.SC-02: Third-party suppliers and partners of IT systems, components and services shall be identified, prioritised and assessed using a cyber supply chain risk assessment process.

1_C. *With regard to the award of supplies for cloud services, measures shall be taken with regard to the security of the cyber supply chain through:*

a. the involvement of the cybersecurity organisation, including the person in charge referred to in subcategory ID.AM-06, point 2_O., in the supply process, already from the design phase;

b. without prejudice to documented technical limitations, the compliance with the fungibility requirement, with the possibility of resorting to another supplier upon expiry;

c. *without prejudice to documented technical limitations, the diversification of suppliers and the consequent resilience of the cloud service;*

d. *the assessment of the technical reliability of third-party suppliers and partners, with reference to best practices in this area and taking into account at least:*

1) *the quality of the products and cyber security practices of the third party supplier and partners, also considering their control over their supply chain and the priority given to security aspects;*

2) *the ability of the third party supplier and partners to ensure supply, service and maintenance over time.*

2_C. *There is an updated list of third party suppliers and partners entrusted for the supply of cloud services, as well as external dependencies, accompanied by the relevant documentation of the assessment process referred to in point 1_C.*

ID.SC-03: Contracts with third party suppliers and partners are used to implement appropriate measures designed to meet the objectives of the organisation's cybersecurity program and cyber supply chain risk management plan

1_C. *The security measures implemented by the entity in relation to internal dependencies are consistent, also in relation to the outcomes of the risk analysis, with the security measures applied to the cloud service. To this end, contracts, agreements or conventions shall be updated accordingly.*

ID.SC-04: Third-party suppliers and partners shall be regularly assessed using audits, checks, or other forms of assessment to confirm compliance with contractual obligations

1_C. *There is an updated document describing the process, methods, frequency of assessments for third-party suppliers and partners, proportionate to the outcomes of the risk analysis carried out.*

2_C. *There is an up-to-date schedule of planned audits, checks, or other forms of assessment, as well as a register of those carried out and related documentation.*

3_C. *An Audit Management process is defined and implemented in order to allow independent assessments and assurance, in compliance with the main industry standards, at least on an annual basis and according to a risk-taking planning.*

4_C. *Audit and standards assurance policies and procedures must be established, documented, approved, maintained and reviewed at least annually.*

5_C. *A remediation plan, relating to corrective actions related to non-compliances detected on third party suppliers and partners, is defined, documented, approved, communicated, implemented and maintained.*

PROTECT (PR)

3.2.5) Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and related resources is limited to authorised personnel, processes and devices, and is managed in a manner consistent with the assessment of the risk of unauthorized access to authorised activities and transactions.

PR.AC-01: Digital identities and login credentials for authorised users, devices and processes are administered, verified, revoked and subject to security audits

7_C. *There is an updated document detailing at least:*

a. *the security policies adopted for the administration, verification, revocation and security audit of digital identities and the procedures set out in points 1_O., 2_O., 3_O., 4_O., 5_O., 6_O.;*

b. *the security policies adopted for the administration, verification, revocation and security audit of digital identities and access credentials for users;*

c. *the processes, methodologies and technologies used that contribute to compliance with security policies.*

PR.AC-03: Remote access to resources is administered

6_C. *There is an updated document detailing at least:*

a. *the security policies adopted for the definition of permitted activities through remote access and the security measures adopted;*

b. *the processes, methodologies and technologies used that contribute to compliance with security*

policies.

PR.AC-04: Rights of access to resources and their authorisations shall be administered in accordance with the principles of least privilege and separation of duties

4_C. *There is an updated, detailed document containing the processes referred to in point 1_O.*

3.2.6) Awareness and Training (PR.AT): The personnel and third parties are sensitised about cybersecurity and are trained to fulfil their tasks and roles consistently with existing policies, procedures and agreements.

PR.AT-01: The personnel of the entity are informed and trained

3_C. *For each member of the entity's personnel, there is an up-to-date register, including the instructions received.*

3.2.7) Data Security (PR.DS): The data is stored and managed in accordance with the organisation's risk management strategy, in order to ensure the integrity, confidentiality and availability of information.

PR.DS-01: Stored data is protected

9_C. *In the case of administrative critical data and services, the provisions of the requirement set out in point 6_O shall not apply. With reference to cryptographic keys, the entity guarantees the autonomous management by the Administration and the generation of secret and private cryptographic keys for a unique purpose and ensures compliance with the requirements set out in points 7_O. and 8_O. consistently.*

10_C. *There is an updated document detailing, also in relation to the ID.AM category, at least:*
a. the security policies adopted for the storage and protection of data;
b. the processes, methodologies and technologies used that contribute to compliance with security policies.

11_C. *The cloud service supports a Bring Your Own Key (BYOK) encryption mechanism, which allows the Administration to independently generate at least the root key, through an HSM hosted, alternately, at:*
a. its own infrastructure;
b. infrastructure made available by the supplier to the Administration in a dedicated manner;
c. infrastructure of a third party chosen by the Administration.

12_C. *In the case of administrative critical data and services, the provisions of the requirement referred to in point 3_0 shall not apply. With regard to the processing of metadata relating to the administration, the provisions of point 2_O. remain in force.*

13_C. *Technical procedures and measures are defined and implemented for the destruction of keys stored outside a secure environment and the revocation of keys stored in hardware security modules (HSMs) when they are no longer needed, in accordance with legal and regulatory requirements.*

14_C. *The entity shall provide the secure key import functionality referred to in point 12_C. into the cloud, for the performance of all key management and encryption operations in the cloud.*

PR.DS-02: Data is protected during transmission

2_C. *In accordance with the risk analysis referred to in measure ID.RA-05, secure and encrypted communication channels and up-to-date and approved protocols shall be used for data flows and communications referred to in measure ID.AM-03.*

PR.DS-03: Physical transfer, removal and destruction of data storage devices shall be managed through a formal process

2_C. *Remote geolocation capabilities are enabled for all managed mobile devices that, if compromised, may have an impact on the availability of the service or on the availability, integrity or confidentiality of the data connected to it.*

3_C. *In line with the provisions of point 2_C., adequate techniques for remote deletion of the Administration's data are defined and implemented.*

3.2.8) Information Protection Processes and Procedures (PR.IP): Security policies (which address the purpose, scope, roles and responsibilities, management commitment and coordination between the various organizational entities), processes and procedures to manage the protection of information systems and assets shall be implemented and adapted over time.

PR.IP-01: Reference practices (so-called baseline) are defined and managed for the configuration of IT and industrial control systems incorporating security principles (e.g. principle of least functionality).

2_C. *There is an updated document detailing, also in relation to the ID.AM category, at least:*
- *a. the security policies adopted for the development of IT system configurations and deployment of the adopted configurations alone;*
- *b. the list of IT system configurations used and the reference to the relevant reference practices;*
- *c. the processes, methodologies and technologies used that contribute to compliance with security policies. [SaaS].*

3_C. *Basic requirements for the security of the various applications are defined and documented.*

4_C. *Technical metrics are defined and implemented to monitor the level of adherence to the defined security requirements and compliance obligations.*

5_C. *There is a mitigation and recovery process for application security, automating automated vulnerability mitigation whenever possible.*

6_C. *There is a process for validating device compatibility with operating systems and applications [PaaS, SaaS].*

7_C. *There is a system for managing changes in terms of operating system, patching and/or applications [PaaS, SaaS].*

PR.IP-02: A process is implemented for managing the life cycle of systems (System Development Life Cycle)

1_C. *Guidelines and technical/organisational measures are implemented for the secure development of the cloud service, in accordance with the OWASP guidelines on security in software development (requirements, design, implementation, testing and verification). Reports on OWASP tests performed must be made available to the National Cybersecurity Agency (ACN) and the Administration, ensuring the absence of 'high' or 'critical' vulnerabilities.*

PR.IP-04: Information backups are executed, administered and verified

5_C. *There is an updated document detailing, also in relation to the ID.AM category, at least:*
- *a. the security policies adopted for the backup of information;*
- *b. the processes, methodologies and technologies used that contribute to compliance with security policies.*

6_C. *There is an updated, detailed document containing the processes referred to in point 1_O.*

PR.IP-09: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and administered in the event of an incident/disaster

6_C. *There is an updated, detailed document indicating the service levels expected from the cloud service and, if applicable, from the hot-replicas and/or cold-replicas as well as from the disaster recovery site(s).*

7_C. *There is an updated, detailed document containing disaster recovery plans, as well as response and recovery plans in the event of incidents, which shall include at least:*
- *a. the policies and processes used to identify event priorities;*
- *b. the phases for implementing the plans;*
- *c. the roles and responsibilities of the personnel;*
- *d. communication and reporting flows;*
- *e. the coordination with CSIRT Italia.*

8_C. *There is an updated document listing the education, training and exercise activities carried out.*

9_C. *Disaster recovery strategies shall be tested and communicated to stakeholders.*

10_C. *Devices critical to the operation of the cloud service shall be redundant and, if located in different locations, at a distance in line with industry best practices.*

PR.IP-12: A vulnerability management plan is developed and implemented

- ***3_C.*** *Technical measures are defined and implemented for the identification of updates for applications that use third-party or open libraries, in compliance with internal vulnerability management policies.*
- ***4_C.*** *The document referred to in point 1_O. of measure PR.IP-12 must be updated on a six-monthly basis.*

3.2.9) Maintenance (PR.MA): Maintenance of information systems and industrial control is done in accordance with existing policies and procedures.

PR.MA-01: Maintenance and repair of resources and systems shall be carried out and recorded with controlled and authorised tools

- ***2_C.*** *There is an updated, detailed document containing the processes and policies referred to in point 1_O.*
- ***3_C.*** *The activities referred to in point 1_O. are also aimed at verifying security aspects.*
- ***4_C.*** *Software updates are only permitted from pre-authorised sources.*
- ***5_C.*** *All logs related to maintenance and updating activities are produced and stored on systems separate from those subject to intervention and not accessible to users who carry out these activities.*
- ***6_C.*** *There is an updated document describing, at least, the processes and technical tools used to achieve points 3_C., 4_C. and 5_C..*

3.2.10) Protective Technology (PR.PT): Technical security solutions are managed to ensure security and resilience of systems and assets, consistent with related policies, procedures and agreements.

PR.PT-04: Communication and control networks are protected

- ***2_C.*** *Intrusion prevention systems (IPS) are present, updated, maintained and well configured.*
- ***3_C.*** *The technical tools referred to in points 1_O. and 2_C. shall contribute to compliance with the policies referred to in categories ID.AM, ID.GV, ID.SC, PR.AC and PR.DS.*

PR.PT-05: Mechanisms (e.g. failsafe, load balancing, hot swap) are implemented, which allow resilience requirements to be met both during normal operation and in adverse situations

- ***4_C.*** *In relation to the plans provided for in the subcategory PR.IP-09:*
  a. there is a disaster recovery site, with features consistent with the risk analysis.

DETECT (DE)

3.2.11) Anomalies and Events (DE.AE): Anomalous activities shall be detected and their potential impact shall be analysed

DE.AE-03: Event information shall be collected and correlated by multiple sensors and sources

- ***9_C.*** *There is a centralised repository containing the entity's user access logs, which is managed directly by the entity and logically segregated from systems to which third parties have direct access.*

3.2.12) Security Continuous Monitoring (DE.CM): Information systems and assets are monitored to identify cybersecurity events and to verify the effectiveness of protection measures

DE.CM-01: Computer network monitoring is carried out to detect potential cybersecurity events

- ***4_C.*** *Incoming and outgoing traffic, the activities of perimeter systems such as routers and firewalls, significant administrative events, as well as executed or failed access to network resources and terminals shall be monitored and correlated in order to identify cybersecurity events.*
- ***5_C.*** *The technical tools referred to in points 1_O., 2_O., 3_O. and 4_C. shall be updated, maintained and well configured, in accordance with the policies set out in the categories PR.AC, PR.DS, PR.IP and PR.MA and contribute to compliance with the policies set out in the categories ID.AM, ID.GV, ID.SC, PR.AC and PR.DS.*
- ***6_C.*** *The technical tools referred to in points 1_O., 2_O., 3_O. and 4_C. shall also be used for the purposes referred to in category DE.AE.*
- ***7_C.*** *There is an updated document describing, at least:*
  a. the security policies adopted in relation to points 1_O., 2_O., 3_O. and 4_C. ;
  b. the processes, methodologies and technologies used that contribute to compliance with security policies.

DE.CM-04: Malicious code shall be detected

- ***3_C.*** *Appropriate firewall software is configured on all devices.*
- ***4_C.*** *Incoming files (via email, downloads, removable devices, etc.) shall be analysed, also via sandbox.*
- ***5_C.*** *The technical tools referred to in points 1_O., 3_O. and 4_C. shall be updated, maintained and well configured, in accordance with the policies set out in the categories PR.AC, PR.DS, PR.IP and PR.MA and contribute to compliance with the policies set out in the categories ID.AM, ID.GV, ID.SC, PR.AC and PR.DS.*
- ***6_C.*** *There is an updated document describing, at least:*
  a. the security policies adopted in relation to points 1_O., 3_C. and 4_C. ;
  b. the processes, methodologies and technologies used that contribute to compliance with security policies.

DE.CM-07: Monitoring shall be carried out to detect unauthorised personnel, connections, devices or software

- ***1_C.*** *With reference to subcategory PR.AC-03, the presence of personnel with potential unauthorised physical or remote access to the resources shall be detected. To this end, there are surveillance and access control systems, including automated systems.*
- ***2_C.*** *With reference to subcategory ID.AM-01, non-approved devices (including physical devices) shall be detected. To this end, without prejudice to documented technical limitations, at least network access control systems shall be in place.*
- ***3_C.*** *The technical tools referred to in points 1_O. and 2_C. shall be updated, maintained and well configured, in accordance with the policies set out in the categories PR.AC, PR.DS, PR.IP and PR.MA and contribute to compliance with the policies set out in the categories ID.AM, ID.GV, ID.SC, PR.AC and PR.DS.*
- ***4_C.*** *There is an updated document describing, at least:*
  a. the security policies adopted in relation to points 1_O. and 2_C.;
  b. the processes, methodologies and technologies used that contribute to compliance with security policies.

DE.CM-08: Scans are carried out for the identification of vulnerabilities

- ***1_C.*** *Based on risk analysis, penetration tests and vulnerability assessments are performed on critical platforms and software applications before they are put into operation.*
- ***2_C.*** *Penetration tests and vulnerability assessments shall be carried out periodically in relation to the criticality of the platforms and software applications referred to in point 1_O.*
- ***3_C.*** *There is an updated document showing the type of penetration test and vulnerability assessment envisaged.*
- ***4_C.*** *There is an updated register of penetration tests and vulnerability assessments carried out together with the relevant documentation.*

RESPOND (RS)

3.2.13) Response Planning (RS.RP) Response procedures and processes shall be carried out and maintained to ensure a response to detected cybersecurity incidents.

RS.RP-01: There is a response plan, and this is executed during or after an incident

- ***2_C.*** *The policies and procedures for the timely management of security incidents shall be reviewed at least on an annual basis.*
- ***3_C.*** *The response plan and the policies and procedures referred to in points 1_O. and 2_C. include critical internal departments, the Administration (if affected) and all third parties concerned.*
- ***4_C.*** *Incident response plans shall be tested and updated at planned intervals or in the event of significant organisational or environmental changes.*
- ***5_C.*** *The metrics of major cybersecurity incidents shall be defined and monitored.*
- ***6_C.*** *Processes, procedures and measures to support business processes for the triage of security-related events are defined and implemented.*
- ***7_C.*** *A Computer Emergency Response Team (CERT) must be implemented to coordinate the incident resolution phase in compliance with the ISO/IEC 27035-2 guidelines. In addition, the Administration*

must be involved at regular intervals to share and review the status of incidents of interest and, where appropriate, to resolve such incidents, also in accordance with the relevant contractual agreements.

3.2.14) Communications (RS.CO): Response activities are coordinated with the internal and external parties (e.g. possible support from law enforcement bodies or law enforcement agencies).

RS.CO-01: The personnel are aware of their role and what they need to do if a response to an incident is necessary

5_C. *There is an up-to-date register of the exercises carried out and of the participants, with the relevant lessons learned.*

6_C. *There are policies and procedures for the management of security incidents, E-Discovery and Cloud Forensics, which must be reviewed and updated at least on an annual basis.*

7_C. *Processes, procedures and technical measures for security breach notifications are defined and implemented.*

8_C. *A mechanism shall be provided for reporting any security breach, whether actual or presumed, including any supply chain breaches, in compliance with SLAs, applicable laws and regulations.*

9_C. *Response activities carried out following an incident shall be communicated to stakeholders internal and external to the organisation, including the organisation's executives and senior management.*
In particular, the recovery activities following an incident shall be communicated to the internal and external parties concerned (e.g. victims, ISPs, owners of the systems attacked, vendors, CERTs/CSIRTs), including the competent bodies of the entity, also for the purpose of possible dialogue with CSIRT Italia.

3.2.15) Mitigation (RS.MI) Actions are performed to prevent the spread of a security event, to mitigate its effects and to resolve the incident.

RS.MI-03: New vulnerabilities are mitigated or documented as an accepted risk

1_C. *Vulnerabilities are mitigated in accordance with the Vulnerability Management Plan (PR.IP-12), i.e. the residual risk resulting from non-mitigation is documented and accepted.*

2_C. *Technical procedures and measures are defined and implemented to allow response actions (scheduled or when emergencies arise) in case of identified vulnerabilities, based on the risk.*

RECOVER (RC)

3.2.16) Recovery Planning (RC.RP): Recovery processes and procedures are performed and maintained to ensure a recovery of the systems or assets involved in a cybersecurity incident

RC.RP-01: There is a recovery plan, which is executed during or after a cybersecurity incident

2_C. *The recovery plan shall be tested on a six-monthly basis as part of two annual exercises.*

3.2.17) Communications (RC.CO): Recovery activities following an incident shall be coordinated with internal and external parts (e.g. victims, ISPs, owners of attacked systems, vendors, CERTs/CSIRTs).

RC.CO-03: Recovery activities carried out following an incident shall be communicated to stakeholders internal and external to the organisation, including the organisation's executives and senior management.

1_C. *Recovery activities following an incident shall be communicated to the internal and external parties concerned (e.g. victims, ISPs, owners of attacked systems, vendors, CERTs/CSIRTs).*

4. Basic features provided for in the case of strategic data and services

4.1 Security

IDENTIFY (ID)

4.1.1) Supply Chain Risk Management (ID.SC): The organisation's priorities, constraints, risk tolerances and assumptions are established and used to support risk decisions associated with supply chain risk management. The organisation has defined and implemented processes to identify, assess and manage supply chain risk

ID.SC-01: Risk management processes inherent in the cyber supply chain are identified, well defined, validated, managed and approved by actors within the organisation

6_S. *There is a document containing the processes referred to in points 1_O. and 2_O.*

ID.SC-02: Third-party suppliers and partners of IT systems, components and services shall be identified, prioritised and assessed using a cyber supply chain risk assessment process.

3_S. *Where possible and in relation to the criticality, it is recommended to:*

a. assess the technical reliability referred to in point 1_C.(d), also taking into account:

1) the supplier's willingness to share the source code;

2) certifications or evidence useful for assessing the quality of the manufacturer's software development process;

3) the adoption, by the manufacturer, of technical procedures and tools to ensure the authenticity and integrity of the software or firmware installed within information and communication technology goods and systems;

4) the adoption, by the manufacturer, of technical procedures and tools to ensure a unique correspondence between the source code and the installed and executed object code;

b. adopt technical processes and tools to:

1) assess the quality and security of the source code, if made available by the manufacturer;

2) acquire the object code from the information and communication technology goods and systems;

3) confirm the unique correspondence between the source code and the installed and executed object code.

ID.SC-03: Contracts with third party suppliers and partners are used to implement appropriate measures designed to meet the objectives of the organisation's cybersecurity program and cyber supply chain risk management plan

2_S. *The security measures implemented by third party providers of external services are consistent, also in relation to the outcomes of the risk analysis, with the security measures applied to the cloud service. To this end, contracts, agreements or conventions shall be updated accordingly.*

PROTECT (PR)

4.1.2) Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and related resources is limited to authorised personnel, processes and devices, and is managed in a manner consistent with the assessment of the risk of unauthorized access to authorised activities and transactions.

PR.AC-03: Remote access to resources is administered

7_S. *Policies and procedures shall be updated at least on an annual basis and made available for consultation, upon specific request, by the Administration.*

8_S. *A joint authorisation process with the Administration is defined and implemented in the event that its data is accessed. If this is not possible, the entity shall contact the Administration as quickly as possible informing it of the accesses made.*

9_S. *All operations that provide access to the Administration's data must be managed in line with the user management and logging policies for privileged users.*

PR.AC-04: Rights of access to resources and their authorisations shall be administered in accordance with the principles of least privilege and separation of duties

5_S. *All privileged activities (e.g. installation of updates) and access to Administration data by the personnel of the entity and third parties must be authorised by the cybersecurity organisation and*

limited to essential cases only.

PR.AC-05: Network integrity is protected (e.g. network segregation, network segmentation)

3_S. *With reference to censuses referred to in the ID.AM category, there is an updated, detailed document containing at least:*

a. the security policies adopted for segmentation/segregation of networks;

b. the description of the segregated/segmented networks;

c. the processes, methodologies and technologies used that contribute to compliance with security policies;

d. the ways in which network ports, protocols and services in use are limited and/or monitored.

PR.AC-07: Authentication methods (e.g. single-factor or multiple-factor authentication) for the entity's users, devices and other assets are commensurate with the risk of the transaction (e.g. risks related to the security and privacy of individuals and other organizational risks)

3_S. *There is an updated, detailed document that, with reference to the censuses referred to in the ID.AM category and to the risk assessment referred to in the ID.RA category, shall contain at least:*

a. the available authentication methods;

b. their assignment to transaction categories.

4.1.3) Awareness and Training (PR.AT): The personnel and third parties are sensitised about cybersecurity and are trained to fulfil their tasks and roles consistently with existing policies, procedures and agreements.

PR.AT-02: Privileged users (e.g. System administrators) understand their roles and responsibilities

3_S. *There is an updated, detailed document containing the processes referred to in points 1_O. and 2_O.*

4.1.4) Data Security (PR.DS): The data is stored and managed in accordance with the organisation's risk management strategy, in order to ensure the integrity, confidentiality and availability of information.

PR.DS-01: Stored data is protected

15_S. *With regard to access to data by non-EU entities, the entity shall:*

a. report to the National Cybersecurity Agency (ACN) and administration any requests for access to data or metadata by non-EU entities;

b. provide access to Administration data or metadata to non-EU entities only after explicit authorisation from the administration.

16_S. *There is an updated document describing which locations and infrastructure the cloud service is provided from. The entity shall make the list available to the administration.*

17_S. *In the case of administrative strategic data and services, the provisions of the requirement referred to in point 2_0 shall not apply. In this respect, all types of metadata must be processed through infrastructure located in the territory of the European Union, with the exception of those necessary for the provision of the services referred to in point 1_O.*

PR.DS-03: Physical transfer, removal and destruction of data storage devices shall be managed through a formal process

4_S. *There is an updated, detailed document containing the processes and policies referred to in point 1_O.*

PR.DS-05: Protection techniques (e.g. access control) are implemented against data leaks

3_S. *There is an updated, detailed document containing the processes and policies referred to in point 1_O.*

PR.DS-06: Data integrity control mechanisms are used to verify the authenticity of software, firmware and information

2_S. *There is an updated, detailed document containing the processes and policies referred to in point 1_O.*

PR.DS-07: Development and testing environments are separated from the production environment

2_S. *There is an updated, detailed document containing the processes and policies referred to in point 1_O.*

4.1.5) Information Protection Processes and Procedures (PR.IP): Security policies (which address the purpose, scope, roles and responsibilities, management commitment and coordination between the various organizational entities), processes and procedures to manage the protection of information systems and assets shall be implemented and adapted over time.

PR.IP-03: Configuration change control processes are in place

4_S. *There is an updated, detailed document containing the processes and policies referred to in point 1_O.*

4.1.6) Maintenance (PR.MA): Maintenance of information systems and industrial control is done in accordance with existing policies and procedures.

PR.MA-01: Maintenance and repair of resources and systems shall be carried out and recorded with controlled and authorised tools

7_S. *There is an up-to-date register of maintenance and repairs performed.*

8_S. *Based on risk analysis, any update of software deemed critical, without prejudice to justified security-related timeliness, shall be verified in the testing environment before actual use in the operational environment.*

9_S. *The object code relating to the updates referred to in point 4_C. shall be kept for at least 24 months.*

PR.MA-02: Remote maintenance of resources and systems is approved, documented and carried out in order to avoid unauthorised access

6_S. *There is an updated, detailed document describing, at least, the processes and technical tools used to achieve points 2_O., 3_O., 4_O. and 5_O.*

4.1.7) Protective Technology (PR.PT): Technical security solutions are managed to ensure security and resilience of systems and assets, consistent with related policies, procedures and agreements.

PR.PT-01: A policy exists and is executed to define, implement and review system logs

3_S. *There is an updated, detailed document containing the processes and policies referred to in point 2_O.*

PR.PT-04: Communication and control networks are protected

1_S. *Perimeter systems, such as firewalls, also at the application level (including Web Application Firewall), are present, updated, maintained and well configured.*

2_S. *Intrusion prevention systems (IPS) are present, updated, maintained and well configured.*

3_S. *The technical tools referred to in points 1_O. and 2_C. shall contribute to compliance with the policies referred to in categories ID.AM, ID.GV, ID.SC, PR.AC and PR.DS.*

4_S. *The updating, maintenance and configuration of the technical tools referred to in points 1_O. and 2_C. shall be carried out in accordance with the policies set out in the categories PR.AC, PR.DS, PR.IP and PR.MA.*

5_S. *The technical tools referred to in points 1_O. and 2_C. shall also be used for the purposes referred to in the DETECT (DE) function.*

6_S. *There is an updated document describing, at least, the processes and technical tools used to achieve points 1_O., 2_C., 3_C. and 4_S.*

PR.PT-05: Mechanisms (e.g. failsafe, load balancing, hot swap) are implemented, which allow resilience requirements to be met both during normal operation and in adverse situations

5_S. *There is an updated, detailed document containing the processes and policies referred to in point 2_O.*

DETECT (DE)

4.1.8) Anomalies and Events (DE.AE): Anomalous activities shall be detected and their potential impact shall be analysed.

DE.AE-03: Event information shall be collected and correlated by multiple sensors and sources

10_S. *There is an updated, detailed document containing the processes and policies referred to in point 3_O.*

4.1.9) Security Continuous Monitoring (DE.CM): Information systems and assets are monitored to identify cybersecurity events and to verify the effectiveness of protection measures.

DE.CM-07: Monitoring shall be carried out to detect unauthorised personnel, connections, devices or software

5_S. *With reference to subcategory ID.AM-02, without prejudice to documented technical limitations, there are control systems for detecting unapproved software.*

6_S. *With reference to subcategory ID.AM-03, there are control systems for detecting unauthorised connections.*

7_S. *The technical tools referred to in points 5_S. and 6_S. shall be updated, maintained and well configured, in accordance with the policies set out in the categories PR.AC, PR.DS, PR.IP and PR.MA and contribute to compliance with the policies set out in the categories ID.AM, ID.GV, ID.SC, PR.AC and PR.DS.*

8_S. *There is an updated document describing, at least:*

a. the security policies adopted in relation to points 5_S. and 6_S.;

b. the processes, methodologies and technologies used that contribute to compliance with security policies.

RECOVER (RC)

4.1.10) Improvements (RC.IM): Recovery plans and related processes shall be improved by taking into account the lessons learned for future activities.

RC.IM-02: Recovery strategies shall be updated

1_S. *The plan referred to in the RC.RP-01 subcategory shall be kept up-to-date also by taking into account the lessons learned during the recovery activities occurred.*

5. Basic features with deferred time limits for application

5.1. Please find below the list of requirements valid six months after the date of application of this Regulation:

- DE.CM-08.1_O.
- PR.AC-03.5_O.
- PR.IP-04.2_Ob.
- PR.PT-04.1_O.
- PR.PT-04.2_C.
- PR.PT-04.3_C.
- RS.MI-03.1_O.

REGULATION FOR DIGITAL INFRASTRUCTURE AND CLOUD SERVICES FOR PUBLIC ADMINISTRATIONS, PURSUANT TO ARTICLE 33-SEPTIES, PARAGRAPH 4, OF DECREE-LAW NO 179 OF 18 OCTOBER 2012, CONVERTED, WITH AMENDMENTS, BY LAW NO 221 OF 17 DECEMBER 2012

ANNEX 4

'REQUIREMENTS FOR THE ADAPTATION AND QUALIFICATION OF DIGITAL INFRASTRUCTURE, CLOUD SERVICE INFRASTRUCTURE AND CLOUD SERVICES FOR PUBLIC ADMINISTRATION'

Summary

1. **Premise**

1.1. This Annex defines, in accordance with the provisions of Article 13 of the Regulation, the requirements for adaptation, pursuant to Article 15 of the Regulation, and for qualification, pursuant to Article 17 of the Regulation, of cloud services for public administrations that may

host services and digital data, respectively, of the public administration classified, in accordance with the process referred to in Article 5 of the Regulation, as ordinary, critical or strategic.

2. **Requirements for the adaptation and qualification of level 1 cloud services (AC1 and QC1)**

2.1. **Features of the cloud services**

For the purposes of level 1 qualification (AC1 and QC1), compliance with the quality, security, performance and scalability, interoperability and portability features referred to in Annex 3 to this Regulation is required for cloud services for public administrations that can process data and services classified as **ordinary,** as well as with the additional requirements defined in sections, 2.2 to 2.6 below.

2.2. **Qualification adaptation chain for cloud services**

Cloud services for public administrations adequate in accordance with Article 14 of the Regulation or qualified in accordance with Article 17 of the Regulation are provided, as an underlying level, through a qualified or adequate public administration cloud service or an adequate cloud service digital infrastructure or infrastructure.

In order to adapt in accordance with Article 14 of the Regulation or to obtain one of the qualifications referred to in Article 17 of the Regulation for a specific level, a cloud service for public administrations of the type Infrastructure-as-a-Service (IaaS) must be provided through:

a) an IaaS cloud service, which is adequate or qualified for the same level or higher;
b) a digital infrastructure for public administrations or a cloud service infrastructure for public administrations, which are adequate in accordance with Article 12 of the Regulation, for the same level or higher, where the underlying level is not a service referred to in point (a).

In order to adapt in accordance with Article 14 of the Regulation or to obtain one of the qualifications referred to in Article 17 of the Regulation for a specific level, a Platform-as-a-Service (PaaS) cloud service must be provided, alternatively, through:

a) a PaaS service, which is adequate or qualified for the same level or higher;
b) an IaaS service, which is adequate or qualified for the same level or higher, where the underlying level is not a service referred to in point (a);
c) a digital infrastructure for public administrations or a cloud service infrastructure for public administrations, which are adequate in accordance with Article 12 of the Regulation, for the same level or higher, where the underlying level is not a service referred to in point (b).

In order to adapt in accordance with Article 14 of the Regulation or to obtain one of the qualifications referred to in Article 17 of the Regulation for a specific level, a Software-as-a-Service (SaaS) cloud service must be provided, alternatively, through:

a) a SaaS service, which is adequate or qualified for the same level or higher;
b) an underlying SaaS service, a PaaS service, which is adequate or qualified for the same level or higher, where the underlying level is not a service referred to in point (a);
c) an IaaS service, which is adequate or qualified for the same level or higher, where the underlying level is not a service referred to in point (b);
d) a digital infrastructure for public administrations or a cloud service infrastructure for public administrations, which are adequate in accordance with Article 12 of the Regulation, for the same level or higher, where the underlying level is not a service referred to in point (c).

2.3. **Certifications required for private providers in case of qualification of cloud services**

For the purposes of level 1 qualification (QC1) the following are required:

- a self-certification that certifies compliance with ISO 9001 standard – Quality Management Systems (QMS). The relevant scope must expressly include at least the

phases of provision of the service subject to qualification and the provision of the technical assistance service to the Italian Public Administration;

- the ISO/IEC 27001 certification – Information Security Management System (SGSI) with ISO/IEC 27017 and ISO/IEC 27018 extensions for the cloud service subject to qualification, the scope of which must cover at least the processes related to the design and delivery of the cloud services subject to qualification. As an alternative to the above requirement it is possible to submit the *Cloud Security Alliance — Star Level 2* certification.

For requests submitted six months after the date of application of this Regulation, certifications must be issued by a certifying body accredited by a national accreditation body of a Member State of the European Union or beneficiary of a mutual recognition agreement with the Italian national accreditation body.

The certifications will possibly need to be renewed in order to cover the entire qualification period without interruption.

2.4. **Additional requirements for proximity cloud services**

With regard to cloud services that are provided in proximity, the cloud service provider shall ensure the implementation of the following additional requirements:

- in addition to the central component, which must comply with all the requirements for qualification or adaptation of the cloud service, pursuant to Articles 17 and 14 of the Regulation, including the qualification chain with respect to an adequate digital infrastructure or cloud service infrastructure, the cloud service may provide for local components on adequate digital infrastructure, cloud service infrastructure or proximity infrastructure;
- in the case of a solution that allows the application data to be written locally (the so-called caching), such data is transferred without undue delay, also through operations scheduled to manage massive jobs (e.g. scheduled jobs), to one or more Cloud repositories. The primary data, which the application must use and the correctness of which it must verify, must be the data present on the central component, while the data present locally must be exclusively of a temporary nature and for use and consumption for ordinary management. In particular, by virtue of the nature of the solution, it must provide for the storage of the processed data only for the time necessary for the purpose or configurable by the administrators;
- where there is no justified technical or regulatory justification, all CRUD operations (create, read, update, and delete) on the information must be done directly on the central component, which then, if necessary, propagates it on the local systems;
- the operating methods described in the previous points must be verified by deleting the data stored locally and then retrieving the same information from the central component, copying locally only what is strictly necessary;
- the architectural solution must be designed and implemented without compromising the security requirements for data protection, even at the local network level. In addition, once the management has been completed, it must be possible to delete the data without undue delay.

2.5. **Additional requirements in case of adaptation of cloud services**

MON-01: Census of use of cloud services *[Requirement applicable from 01/02/2025]*

1_O. *The entity with qualified or adequate services communicates to the ACN, every six months, the list of administrations that use its cloud services, according to the methods made available on the digital platform.*

2.6. **Additional requirements in case of qualification of cloud services**

MON-01: Census of use of cloud services *[Requirement applicable from 01/02/2025]*

1_O. *The entity with qualified or adequate services communicates to the ACN, every six months, the list of administrations that use its cloud services, according to the methods made available on the digital platform.*

QU.LS-01: Compliance with mandatory service indicators is ensured, the methods for sharing the levels of service availability and any compensatory penalties are disclosed.

4_O. *The entity shall ensure the application of compensatory penalties to be paid to the administration in case of breach of the service levels guaranteed by the contract for the provision of the qualified service. The methods of quantification and the conditions for the recognition of compensatory penalties shall be included in the contract and shall be aligned with market values and conditions for similar services or belonging to the same category.*

5_O. *For each contract, the entity shall have adequate insurance guarantees to ensure the performance of all the activities referred to in Article 21.*

QU.PR-01: Tracking, reporting and transparency of costs and their processing

1_O. *The entity makes available to the administration tools (eg a dashboard) and APIs that allow the acquisition of detailed information on the metrics for calculating the costs of the cloud service (the so-called 'billing') to make the calculation transparent to the administration. The metrics for calculating cloud service costs must be expressed synthetically or detailed by cost type (e.g. cloud resource).*

2_O. *The tools and APIs referred to in point 1_O. allow billing reports to be filtered and created with details of costs per hour, day or month, for each account or product of the cloud service in use. The tracking and updating of cost information must be updated at least once every hour.*

QU.PR-02: Cost notification and monitoring

1_O. *The entity offers the administration a cost monitoring system that allows alerts with notifications to be set to alert the administration in case the use of the cloud service approaches or exceeds the set budget/thresholds.*

QU.PR-03: Minimum requirements for price specifications

1_O. *The entity shall specify to the administration its pricing method and model for the provision of the cloud service, which must ensure maximum commercial flexibility and support scalability and growth.*

2_O. *The entity shall provide the administration with:*

a. a document containing the terms and conditions, specifying in particular whether prices are provided for a pay-as-you-go service and whether policies for dynamic adjustment of prices to the market are in place;

b. a document containing the prices (references to prices to the public are allowed provided that, upon request, a complete list/price document is available).

3. Requirements for adaptation and qualification of Level 2 cloud services (AC2 and QC2)

For level 2 qualification (AC2 and QC2), compliance with the requirements for Level 1 qualification (AC1 and QC1) and additional requirements defined in sections 3.1 and 3.2 below is required.

3.1. Features of the cloud services

Compliance with the quality, security, performance and scalability, interoperability and portability features referred to in Annex 3 to this Regulation is required for cloud services for public administrations that can process data and services classified as **critical** pursuant to Article 3 of the Regulation.

3.2. Certifications required in case of qualification of cloud services

For the purposes of level 2 qualification (QC2) the following are required:

- a self-certification certifying compliance with ISO 22301 standard — *Business Continuity Management System* for the cloud service subject to qualification;
- a self-certification certifying compliance with ISO 20000 standard — *Service Management System* for the cloud service subject to qualification.

4. **Requirements for adaptation and qualification of Level 3 cloud services (AC3 and QC3)**

For level 3 qualification (AC3 and QC3), compliance with the requirements for Level 2 qualification (AC2 and QC2) and additional requirements defined in sections 4.1 and 4.2 below is required.

4.1. **Features of the cloud services**

Compliance with the quality, security, performance and scalability, interoperability and portability features referred to in Annex 3 to this Regulation is required for cloud services for public administrations that can process data and services classified as **strategic** pursuant to Article 3 of the Regulation.

4.2. **Certifications required in case of qualification of cloud services**

For the purposes of Level 3 qualification (QC3) the following are required:

- ISO 22301 certification — *Business Continuity Management System* for the cloud service subject to qualification;
- ISO*/IEC* 20000 certification (*Service Management*) for the cloud service subject to qualification;
- *Cloud Security Alliance — Star Level 2* certification.

For requests submitted six months after the date of application of this Regulation, certifications must be issued by a certifying body accredited by a national accreditation body of a Member State of the European Union or beneficiary of a mutual recognition agreement with the Italian national accreditation body.

The certifications will possibly need to be renewed in order to cover the entire qualification period without interruption.

5. **Requirements for adaptation and the qualification of Level 4 Cloud Services (AC4 and QC4)**

For level 4 qualification (AC4 and QC4), compliance with the requirements for level 3 qualification (AC3 and QC3) and the requirements defined in section 5.1 below is required.

5.1. **Additional security requirements**

ID.AM-03: Organisation-related data and communication flows are identified

2_SS. *All cloud service delivery flows are subject to approval, monitoring and control procedures agreed with the administration.*

PR.DS-01: Stored data is protected

18_SS. *The cloud service supports a Hold Your Own Key (HYOK) encryption mechanism, which allows the administration to generate and manage all encryption keys independently through an HSM hosted, alternately, at:*
a. its own infrastructure;
b. infrastructure made available by the supplier to the administration in a dedicated manner at a third party chosen by the administration.

19_SS. *The administration shall have exclusive access to the keys referred to in point 1 and to the clear data of the administration.*

20_SS. *The cloud service provider provides the administration with a dedicated HSM service.*

21_SS. *The cloud service provider is autonomous in providing the cloud service, having its own capabilities to operate the underlying physical and logical infrastructure. For exceptional cases and on the basis of documented technical limitations, the cloud service provider may rely on third-party expertise,*

ensuring, where possible, fungibility.

PR.IP-11: Cybersecurity issues are included in personnel management processes (e.g.: screening, deprovisioning)

1_SS. *The cloud service provider shall make the methodology used for the verification of the personnel (vetting process methodology) with privileged access to the cloud service or administrative data available to the administration.*

2_SS. *The cloud service provider shall make the list of employees with privileged access to the cloud service or administrative data available to the administration. The administration may unilaterally request the removal of one or more employees from the aforementioned list and the cloud service provider shall promptly do so.*

6. Requirements for adaptation of a digital infrastructure or a level 1 cloud service infrastructure (AI1)

For the purposes of level 1 (AI1) adaptation, compliance with the minimum levels set out in Annex 2 to this Regulation is required for digital infrastructure or cloud service infrastructure for public administrations that can process data and services classified as **ordinary** in accordance with Article 3, as well as with the additional requirements defined in Sections 6.1, 6.2 and 6.3 below.

6.1. Certifications required in case of adaptation of cloud service infrastructure for public administrations by private entities

For the purpose of adapting a level QI1 cloud service infrastructure, not for housing, the following shall be required:

- ISO 9001 certification – Quality Management Systems (QMS) for the digital infrastructure subject to qualification. Its scope must include at least the provision of technical assistance service to customers;
- ISO/IEC 27001 certification – Information Security Management System (SGSI), the scope of which must cover at least the processes related to the management and maintenance of the infrastructure subject to qualification.

For requests submitted six months after the date of application of this Regulation, certifications must be issued by a certifying body accredited by a national accreditation body of a Member State of the European Union or beneficiary of a mutual recognition agreement with the Italian national accreditation body.

The certifications will possibly need to be renewed in order to cover the entire qualification period without interruption.

6.2. Additional requirements in case of adaptation of digital infrastructure by public entities, in-house entities, or publicly controlled companies managing the digital infrastructure of the public administration by express regulatory provision

MON-01: Census of use of infrastructure *[Requirement applicable from 01/02/2025]*

1_O. *The entity with adequate infrastructure communicates to the ACN, every six months, the list of administrations that use its digital infrastructure, according to the methods made available on the digital platform.*

S.DC-04: Data centre – title deeds of the premises

1_O. *The Administration must demonstrate that the properties in which the Data Centres are located are exclusively available to the Authority on the basis of one of the following title deeds:*

a. properties;

b. lease/loan from another PA or State Property;

c. real estate lease-purchase agreement;

d. private lease or possession with "rent to buy" or "lien agreement" contracts.

6.3. **Additional requirements in case of adaptation of cloud service infrastructure for public administrations for private entities**

MON-01: Census of use of infrastructure *[Requirement applicable from 01/02/2025]*

1_O. *The entity with adequate infrastructure communicates to the ACN, every six months, the list of administrations that use its digital infrastructure, according to the methods made available on the digital platform.*

QU.LS-01: Compliance with mandatory service indicators is ensured, the methods for sharing the levels of service availability and any compensatory penalties are disclosed.

1_O. *The entity shall ensure the application of compensatory penalties to be paid to the administration in the event of a breach of the service levels guaranteed by the infrastructure supply contract. The methods of quantification and the conditions for the recognition of compensatory penalties shall be included in the contract and shall be aligned with market values and conditions for similar services or belonging to the same category.*

2_O. *For each contract, the entity shall have adequate insurance guarantees to ensure the performance of all the activities provided for in Article 21 of the Regulation.*

6.4. **Additional requirements in case of adaptation of proximity infrastructure**

Without prejudice to the need to ensure data protection requirements, where they exist, due to the specificities of the proximity infrastructure or the nature of the support provided to cloud services for public administrations, specific technical reasons requiring derogations, even partial, from the minimum levels set out in Annex 2, the digital infrastructure operator shall provide detailed evidence of this in the compliance report referred to in Articles 13 and 14 of the Regulation, also describing the possible alternative way in which it achieves a similar objective and any related risk analyses. In any case, the digital infrastructure operator shall ensure at least compliance with the minimum levels set out in Annex 2 below:

- on ‘Processing Capacity’, par. 2.2;
- on 'Data Center Security’, par. 2.3 and 3.2;
- on 'Energy savings’, par. 2.4.
- on ‘Security’, par. 2.5, 3.3 and 4.2, consistent with the required level of adaptation, as per Article 12 of the Regulation, with the exception of requirements PR.IP-04, PR.IP-09 and PR.PT-05.

7. **Requirements for adaptation of a digital infrastructure or a level 2 cloud service infrastructure (AI2)**

For level 2 adaptation (AI2), compliance with the requirements for level 1 adaptation (AI1) and additional requirements defined in sections 7.1 and 7.2 below is required.

7.1.**Minimum levels of digital infrastructure**

For the purposes of level 2 adaptation (AI2), compliance with the minimum levels set out in Annex 2 to this Regulation is also required for digital infrastructure or cloud service infrastructure for public administration that can process data and services classified as **critical** pursuant to Article 3 of the Regulation.

7.2. **Certifications required in case of adaptation of cloud service infrastructure for public administrations by private entities**

For the purpose of level 2 adaptation (AI2) of a cloud service infrastructure, not for housing, a self-certification certifying compliance with ISO 22301 standard — Business Continuity Management System is required for the digital infrastructure subject to qualification.

8. **Requirements for adaptation of a digital infrastructure or a level 3 cloud service infrastructure (AI3)**

For level 3 adaptation (AI3), compliance with the requirements for level 2 adaptation (AI2) and additional requirements defined in sections 8.1 and 8.2 below is required.

8.1. **Minimum levels of digital infrastructure**

For the purposes of level 3 adaptation (AI3), compliance with the minimum levels set out in Annex 2 to this Regulation is also required for digital infrastructure or cloud service infrastructure for public administration that can process data and services classified as **strategic** pursuant to Article 3 of the Regulation.

8.2. **Certifications required in case of adaptation of cloud service infrastructure for public administrations by private entities**

For the purpose of level 3 adaptation (AI3) of a cloud service infrastructure, not for housing, the ISO 22301 certification — *Business Continuity Management System* is required for the infrastructure subject to qualification.

For requests submitted six months after the date of application of this Regulation, certifications must be issued by a certifying body accredited by a national accreditation body of a Member State of the European Union or beneficiary of a mutual recognition agreement with the Italian national accreditation body.

In the case of adaptation of proximity infrastructure, it is possible to derogate from compliance with this requirement, by describing, in the relevant compliance report, the justified technical and organisational reasons why it is not possible to comply with this provision, together with a description, accompanied by a related risk analysis, regarding alternative ways to support the *Business Continuity* requirements.

The certifications will possibly need to be renewed in order to cover the entire qualification period without interruption.

9. **Requirements for adaptation of a digital infrastructure or a level 4 cloud service infrastructure (AI4)**

For level 4 adaptation (AI4), compliance with the requirements for level 3 adaptation (AI3) and the requirements set out in section 9.1 is required.

9.1. **Additional security requirements**

PR.IP-11: Cybersecurity issues are included in personnel management processes (e.g.: screening, deprovisioning)

1_SS. *The digital infrastructure operator shall make the methodology used for the verification of the personnel (vetting process methodology) with privileged access to the infrastructure or administrative data available to the administration.*

2_SS. *The digital infrastructure operator shall make the list of employees with privileged access to the infrastructure or administrative data available to the administration. The administration may unilaterally request the removal of one or more employees from the aforementioned list and the cloud service provider shall promptly do so.*