Italian Cloud Strategy

Release stabile

italia

08 set 2021

Indice

CAPITOLO 1

Executive summary

The digital transformation of society, accelerated by the still ongoing pandemic emergency, has made a similar transformation of the Public Administration inevitable. The digitalization of the Public Administration is now a priority objective in order to guarantee citizens and businesses more high-quality, efficient and effective public services, as well as to create new development opportunities for the country's digital economy. In this transformative process, the use of Cloud Computing, or Cloud, plays a central role due to its enabling features for simplifying and optimizing the management of IT resources, reducing costs, and introducing new digital technologies.

For this reason, Italy's Cloud Strategy was developed with the aim of providing the strategic direction for the implementation and control of Cloud solutions in the Public Administration. Migration to the Cloud allows public administrations to provide digital services and have secure, efficient, and reliable technological infrastructures, in line with the principles of privacy protection and the recommendations of European and national institutions, while maintaining the necessary guarantees for the country's strategic autonomy, security and national control over data.

In this perspective, Italy's strategy is based on three fundamental pillars.

1. The creation of the National Strategic Hub (NSH), a national infrastructure for the provision of Cloud services, whose management and control are independent from non-EU providers;

2. A qualification process of public Cloud providers and their services to ensure that their characteristics and service levels are in line with the necessary requirements of security, reliability and compliance with relevant regulations and the country's national interests;

3. The development of a methodology for the classification of data and services managed by public administrations to allow their migration towards the most appropriate Cloud solution (NSH or qualified public Cloud).

CAPITOLO 2

1. Introduction

The health emergency has made it even clearer how crucial and strategic digital infrastructures are for our country, on a par with traditional infrastructures such as motorways, railways and the electricity grid. The adoption and diffusion of digital technologies has in fact been accelerated and facilitated by the pandemic, enabling new ways of studying and working remotely.

Among the enablers of the country's digital transformation, a central role is played by Cloud Computing technologies, which make it possible to simplify and optimize the management of IT resources and facilitate the adoption of new digital technologies.

The need for Cloud technologies is set to increase in light of the exponential growth in the volume of data processed[1] and the pervasiveness of digital services requiring computational infrastructures that can be quickly and flexibly expanded and scaled, which is something difficult to achieve using traditional data centres.

The irreversible process of the digital transformation of society has induced a similar transformation of the Public Administration (PA), both to ensure greater quality, efficiency and effectiveness of public services, and to support and create new development opportunities for the country's digital economy.

For the PA, the use of Cloud makes it possible to achieve these objectives with a significant reduction in costs while also helping to increase energy efficiency and environmental sustainability. At the same time, the various architectural paradigms and service delivery models impose the need to adopt an organic national strategy that can guarantee the necessary strategic autonomy and resilience for the country, as well as security and national control of citizens' data and services.

This document aims to set out a strategic plan for the adoption of Cloud Computing in the PA, in light of the emerging opportunities and risks.

[1] From 2018 to 2025, the volume of data is estimated to increase by around 530% (European Commission, European data strategy. Making the EU a role model for an empowered society. Feb. 2020).

CAPITOLO 3

2. Cloud Computing

Cloud Computing is a new paradigm for the use and management of computing resources and computer services delivered on demand via the Internet. Cloud services are offered by means of standardized catalogues. They guarantee services that can be easily and automatically scaled up depending on load peaks (agility, scalability, elasticity), and can operate simultaneously and securely on the data and systems of different users (multi-tenant).

Typically, Cloud services, according to the model of computational resources offered, are divided into three service models:

1. Infrastructural system services so called *Infrastructure-as-a-Service (laaS)* for the provision, for example, of virtualized servers and data storage space;

2. Computational platforms services so called *Platform-as-a-Service (PaaS)* for the provision of pre-configured and managed environments for the development of specific applications, e.g. for software development, data management or containerised applications;

3. Application services so called *Software-as-a-Service (SaaS)* for the delivery of applications to end users, e.g. e-mail or other remote collaboration systems.

These different service models allow users of Cloud services to avoid many of the basic management activities of a data centre's infrastructure (such as management of buildings and physical technological components) and, to simplify the management of initial and operational configurations of applications and platforms, thus. allowing considerable economic savings and greater flexibility in managing the organisations' demand for new computing resources.

Services are typically provided by *Cloud Service Providers (CSPs)* who guarantee their operation according to contractually determined levels (*Service-Level Agreements, SLAs*).

The distribution model of Cloud services can be organised in the following categories: *Public Cloud, Private Cloud, Hybrid Cloud and Multi-Cloud*.

3.1 2.1 Public Cloud

In the *Public Cloud*, the infrastructure is owned by a CSP which, with full control, makes its systems available to users, companies and public bodies in different geographical areas (or regions) of the world, sharing processing capacity, applications and storage. Such a deployment allows users of cloud services to benefit from resilient computing capacities that can be scaled according to actual needs. In the area of public cloud CSPs, a small group of non-European companies (mainly of US origin) operate as market leaders. These companies offer Cloud services with almost unlimited computing capacity through highly sophisticated technological solutions, so-called 'hyperscaler', with high ease of use, configurability and interoperability.

3.2 2.2 Private Cloud

The *Private Cloud* consists of a Cloud environment reserved for an individual customer for its exclusive use.

This may be on-premise, i.e. based on infrastructures that are entirely in the domain of the customer, which holds control and full responsibility for the maintenance and security management of the hosted data and services, or it may be managed at a third party's data centre, where the customer is provided with dedicated resources.

One of the advantages of a Private Cloud is certainly the greater control that the customer can exert (in terms of choice and contractual arrangements) over the characteristics of the Cloud infrastructure and services, especially with regards to security. However, this solution, particularly in the case of on-premise clouds, presents some disadvantages as the infrastructure may not be able to guarantee adequate scalability to handle unforeseen peaks in demand.

3.3 2.3 Hybrid Cloud

A combination of the Public and Private Cloud models, the *Hybrid Cloud*, is a single environment created from several connected environments in which, depending on need, resources from both a private and a public Cloud are made available to users. This model extends the capabilities of a private cloud to use on demand the large-scale resources available on a Public Cloud, t in order to manage, for example, sudden peaks in workload; furthermore, it guarantees savings in terms of the transmission bandwidth needed to exchange data, compared to what would be possible with a connection to a data centre.

3.4 2.4 Multi-Cloud

Multi Cloud refers to a model in which several clouds of the same type (public or private) offered by different providers are used simultaneously to implement certain services or applications.

Unlike the Hybrid Cloud, which involves the creation of a single infrastructure that transparently uses different types of Cloud (public or private), the Multi Cloud model is based on the use of different public or private Cloud environments that are not interconnected. In a Hybrid Cloud environment, the distribution of the use of computational resources between private and public is typically semi-automated and transparent to the user, whereas a Multi Cloud environment presents itself as a set of distinct computational resources that can potentially be integrated at application level.

CAPITOLO 4

3. The Opportunities and Challenges of Cloud Computing

The adoption of new digital technologies, and the challenges arising from it are the subject of important EU regulations such as, among others, Regulations (EU) 2016/679 and 2018/1807 (known as GDPR and free flow of non-personal data), Directive 2016/1148 (known as the NIS Directive), and national security legislation, such as Law 133/2019 (National Security Perimeter for Cyber (Perimetro di Sicurezza Nazionale Cibernetica, PSNC)[2].

4.1 3.1 Technological Autonomy

In order to govern and manage the country's digital transformation processes, as recognised by the main European institutions, autonomy in the control of the digital infrastructure of the Cloud and, consequently, of the storage and processing of data appears to have enormous strategic importance[3].

It is well known, however, that the market shares of European companies' Cloud infrastructures represent a residual value (less than 10%) compared to those held by non-EU companies[4]. However, this criticality is not only limited to digital services and platforms, but also, and most importantly, to the infrastructures that enable them to function.

Given such a contractual weakness of the EU, the massive adoption of Cloud technology for the provision of PA services is subject to risks such as in the case of unilateral changes in the terms of services: increased costs or service interruption, or to actions that are potentially beyond the control of the country. Achieving technological autonomy has important implications, not only in terms of the possibility of exerting direct control over data and services, but also in terms of promoting an ecosystem of technologies (Cloud Computing, IoT, Artificial Intelligence, Quantum Computing) which is essential for the country's development.

[2] Conversion into law, with amendments, of Leg. Decree 21 September 2019, no. 105, on urgent provisions concerning the National Cyber Security Perimeter.

[3] OECD (2019) Regulation and IRC: challenges posed by the digital transformation. 20th meeting of the Regulatory Policy Committee, 17-18 April 2018, OECD Conference Centre, Paris, France.

[4] See, for example, https://www.gartner.com/en/newsroom/press-releases/2019-07-29-gartner-says-worldwide-iaas-public-cloud-services-market-grew-31point3-per and https://www.idc.com/getdoc.jsp?containerId=prUS45552219 and https://www.forbes.com/sites/steveandriole/2019/11/20/forrester-research-gets-cloud–computing-trends-right/#5b30ee4468a2[14].

[14] https://www.forbes.com/sites/steveandriole/2019/11/20/forrester-research-gets-cloud--computing-trends-right/#5b30ee4468a2

4.2 3.2 Control over Data

The operation of cloud services by providers in non-EU countries poses an additional risk due to the regulations in place in those countries. As it is well known, non-EU legislation[5] may allow - provided certain circumstances - unilateral requests to the CSP to provide access to data. These cases involve the possibility for a non-EU country to access data (or data flows) that are particularly sensitive and strategic for the EU Member States' citizens and institutions. In this perspective, within the framework of the strategy, it is necessary to clearly determine - via a classification procedure - the types of data that can be managed by a non-EU provider through a Public Cloud and which data instead will need to be managed by a Cloud provider that meets specific security requirements in order to reduce the risk that the data may be accessible to non-EU governments. The management of such risks does have, inevitably, not only technological but also geopolitical implications that should receive adequate consideration.

4.3 3.3 Aspects of Resilience

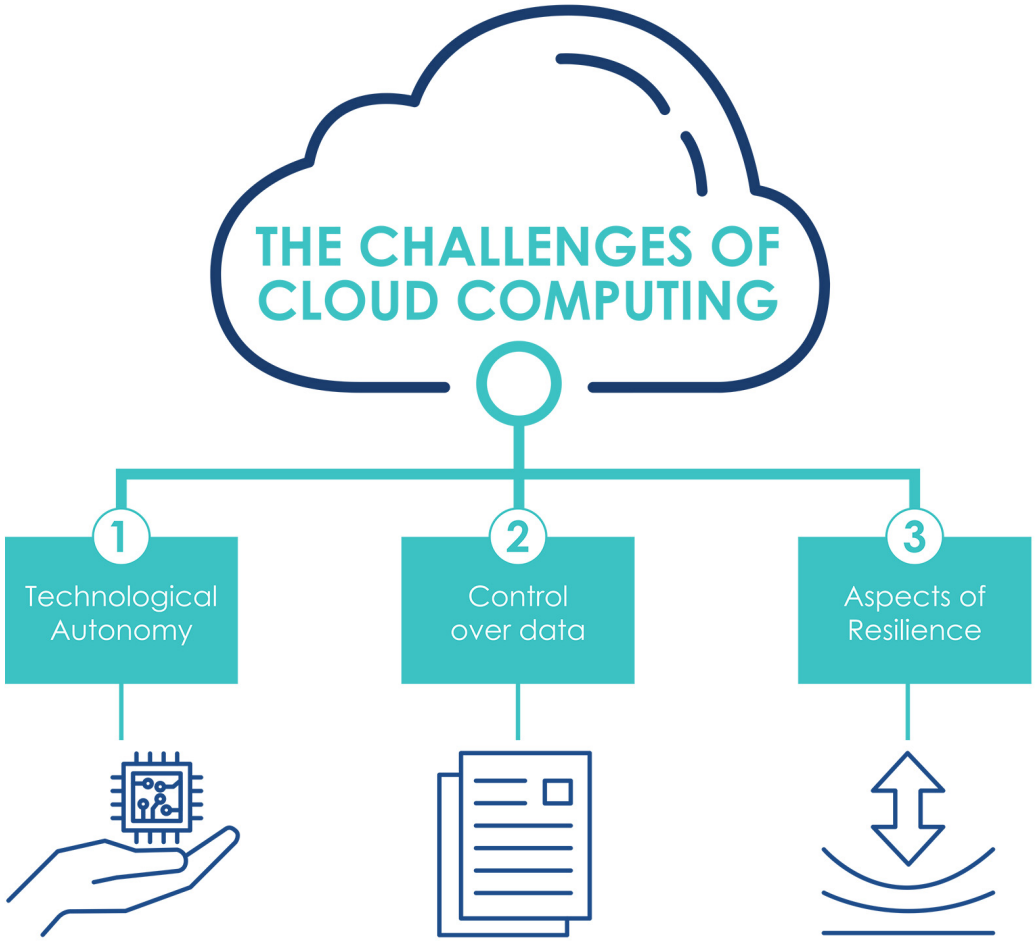
Cloud infrastructures and services supporting PA applications and national essential entities must adopt appropriate procedural and technical security measures, as well as redundancy and interoperability operations. The application of layered security controls (e.g. pseudonymisation, encryption with on-premise key management) in compliance with the specific requirements of the data processed, as well as service continuity and disaster recovery measures available throughout the entire national territory, will increase the level of resilience against incidents such as cyber attacks and breakdowns.

In particular, although international practices and technical standards are widely applied by Cloud service providers, given the criticality of the data and services involved, the Cloud migration strategy requires a certification process of public Cloud providers and their services. The qualification must assess not only the security dimension but also the architectural and organisational aspects which may have negative impacts on the resilience, e.g. vendor lock-in situations. Another important direction, in line with the recent initiatives and directives of the European Digital Agenda[6], is the standardisation, harmonisation and interoperability of Cloud services. Within this context, and with the aim of developing common requirements for a European data infrastructure, the GAIA-X project[7] was launched; since the project's inception Italy had an active involvement in its development. The project, designed for European based companies, has the objective to build an open and resilient digital ecosystem through the federation of cloud services. This ecosystem is built on common standards, ensures transparency and interoperability, capable of connecting centralised and decentralised infrastructures, and transforming them into a homogeneous system.

[5] Examples are the National Intelligence Law of the People's Republic of China, the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) or the Foreign Intelligence Surveillance (FISA).

[6] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en

[7] https://www.data-infrastructure.eu/


THE CHALLENGES OF CLOUD COMPUTING
1
Technological Autonomy
2
Control over data
3
Aspects of Resilience

CAPITOLO 5

4. Cloud Strategy for the Public Administration

Currently, most public services are delivered through PA data centres that often lack sufficient capabilities to ensure adequate standards of reliability and resilience. Achieving and maintaining such standards requires investments and skills that are not currently available in many central and local public administrations. In this context, the Italian Cloud Strategy is intended as an implementation methodology of the "*Cloud-First*" policy, a key pillar of the digitalization process of the PA as identified in the Italian PNRR. This will *guide and encourage the safe, controlled and complete adoption of Cloud technologies for the PA*, with the aim, in the long run, that all the services provided are based on "Cloud-native" applications, i.e. natively developed on the basis of Cloud paradigms.

The Cloud Strategy for the PA is therefore based on the following strategic guidelines:

1. **Classification of Data and Services:** definition of a data classification process to guide and support the migration of PA data and services to the Cloud;

2. **Qualification of Cloud Services:** implementation of a systematic process of scrutiny and qualification of Cloud services usable by PA;

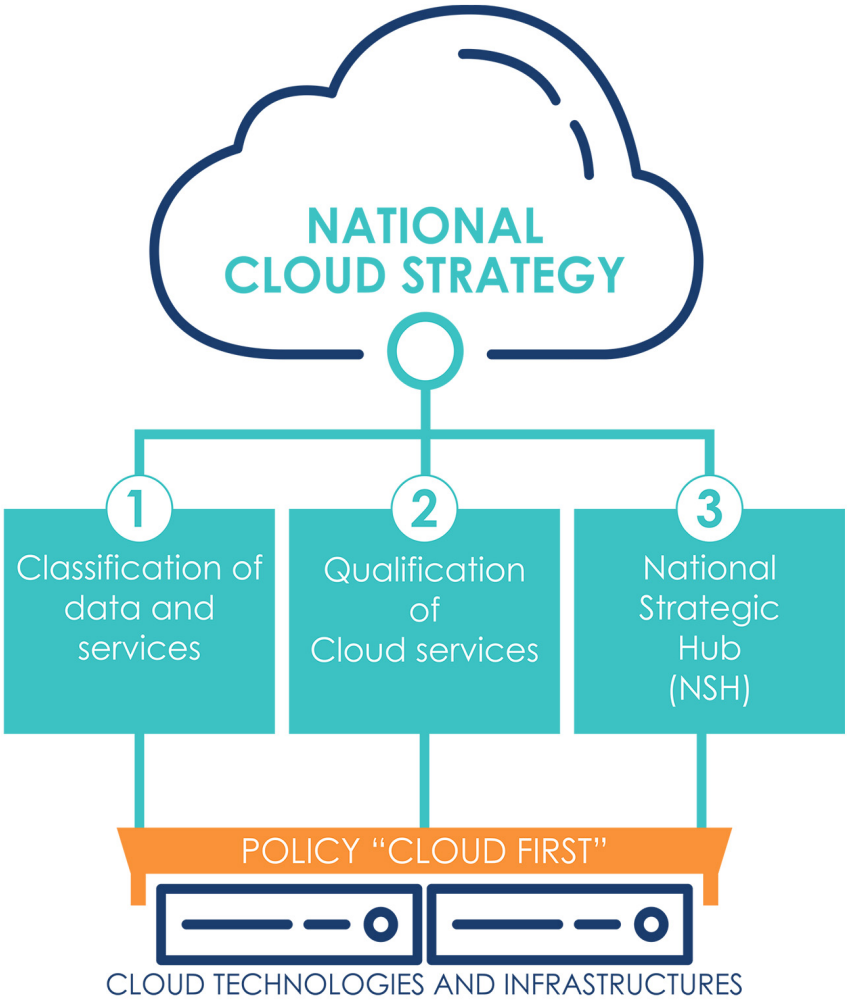
3. **National Strategic Hub:** creation of a national infrastructure for the provision of Cloud services, whose management and control are autonomous from non-EU actors.

The implementation of these macro-actions will make it possible to harmonise and regulate the adoption of the Cloud in the PA, as well as to apply economies of scale to encourage a reduction in management costs by offering more reliable and resilient digital services.

5.1 4.1 Classification of Data and Services

In light of the technological and regulatory challenges concerning the broad spectrum of available Cloud services, Cloud adoption must be adequately regulated so as to mitigate the systemic risks involved. The key element for such regulation is to identify a *systematic process of classification of data and services* managed by PAs, the result of which can be used to standardise and steer the process of migration to the PA Cloud. To this end, the classes of data and services are identified on the basis of the damage that their compromise, in terms of *confidentiality*, *integrity* and *availability*, would cause to the country system. These classes are:

- **Strategic**: data and services which, if compromised, may have an impact on national security;


NATIONAL
CLOUD STRATEGY
1
Classification of data and services
2
Qualification of Cloud services
3
National Strategic Hub (NSH)
POLICY "CLOUD FIRST"
CLOUD TECHNOLOGIES AND INFRASTRUCTURES

- **Critical**: data and services the impairment of which could be detrimental to the maintenance of functions that are important to society, health, safety and the economic and social well-being of the country;
- **Ordinary**: data and services the impairment of which does not cause the interruption of state services nor, in any case, damage the economic and social well-being of the country.

This classification leaves aside specific regulations and security requirements; it only focuses on the possible impact on the country. The application of the classification process, which is outlined below, will allow an informed analysis of the impacts and the applicable class, as well as the identification of the appropriate security and regulatory requirements. For example, data and services related to essential state functions and services, i.e. identified within the scope of the Perimetro Sicurezza Nazionale Cibernetica (PSNC), will be classified as *Strategic*, citizen health data will be classified as *Critical*, while data and services related to institutional web portals will be classified as *Ordinary*.

5.2 4.2 Qualification of Cloud Services

Public administrations acquire Cloud services through procurement procedures which are not flexible enough to keep up with the market development and, most of all, do not allow the appropriate evaluation of the technical and organisational risks involved in adopting a specific service.

In the context of facilitating and guiding the implementation of the "*Cloud-First*" policy for the PA, it is crucial to provide an *ex-ante qualification schema for Cloud services* that can be purchased by the PA. This qualification, starting from the experience gained by AgID, aims at simplifying and regulating the adoption of Cloud services both from a technical and an administrative point of view. In light of the presented challenges and the spectrum of cloud services considered, the qualification of Cloud services should include the analysis of the following aspects:

1. *Operational management* of Cloud services, with details of the technical and organisational standards[8], and data control measures applied;

2. *Security requirements* applied in data management and service delivery, such as encryption keys management policies and security controls;

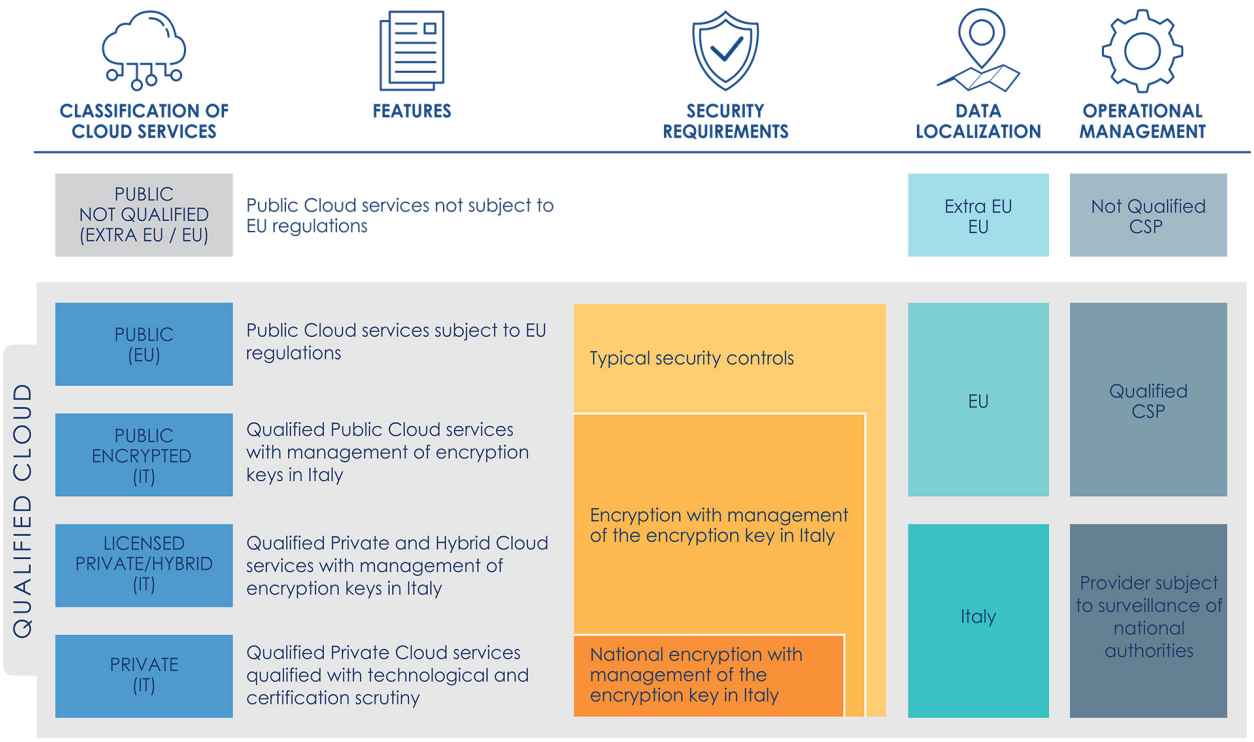
3. *Service conditions* applied to service delivery and reporting, such as availability guarantees and contractual instruments available to administrations.

On the basis of the analysis of the technological and organisational solutions available on the market, the three aspects of the analysis make it possible to identify ex ante the following qualification of Cloud services.

The spectrum of Cloud services varies from:

- *Public Not Qualified (extra-EU / EU)*, for which control tools on data and services are essentially non-existent;
- *Qualified Public Cloud (EU)* services ensuring compliance with relevant legislation (e.g. GDPR and NIS), with technical and organisational security requirements typically through the use of granular encryption systems managed by the CSP provider[9], and allow greater control over the data and services managed;
- The use of solutions based on Public Clouds with on-premise control of security mechanisms, i.e. *Encrypted Public Cloud (IT)*, significantly increases the available level of control over data and services, introducing greater autonomy from non-EU CSPs in the operational management and control of technology infrastructures[10];
- Private and Hybrid Cloud solutions allow additional isolation from the public regions of the main CSPs, ensured through operational management performed by a designated provider under the surveillance and monitoring of the national authorities. These implementations can be divided in two groups: those based on hyperscaler technology licensed from one or more CSPs, i.e. *Licensed Private/Hybrid Cloud (IT)*, and those implemented using commercial technologies that are qualified by means of technological scrutiny and certification procedures, i.e. *Qualified Private Cloud (IT)*.

[8] For example, the international standards ISO 27017/27018, ISO 22301 and CSA STAR.
[9] These services include, for example, the use of key management systems (KMS), based on special hardware modules (i.e. HSM).
[10] For example, by using an on-premise HSM to manage the keys used to encrypt data on the Public Cloud.



The qualified Cloud services shall be used, according to the data classification outcome, enforcing the following constraints:

- The Qualified and Encrypted Public Cloud offerings shall host *ordinary* data and services;
- The Encrypted Public Cloud, the Licensed Private/Hybrid Cloud shall host *critical* data and services;
- The Licensed Private/Hybrid and Qualified Private Cloud shall host *strategic* data and services.

The process of qualification of Cloud services, in order to simplify the adoption of Cloud services in the PA should end with the creation of an *electronic marketplace of qualified Cloud services*[11]. This marketplace should be the means by which administrations are guided, in accordance with the data and services classification process, in the choice of the Cloud services that are most suitable for them and can be purchased through simplified and pre-negotiated administrative tools.

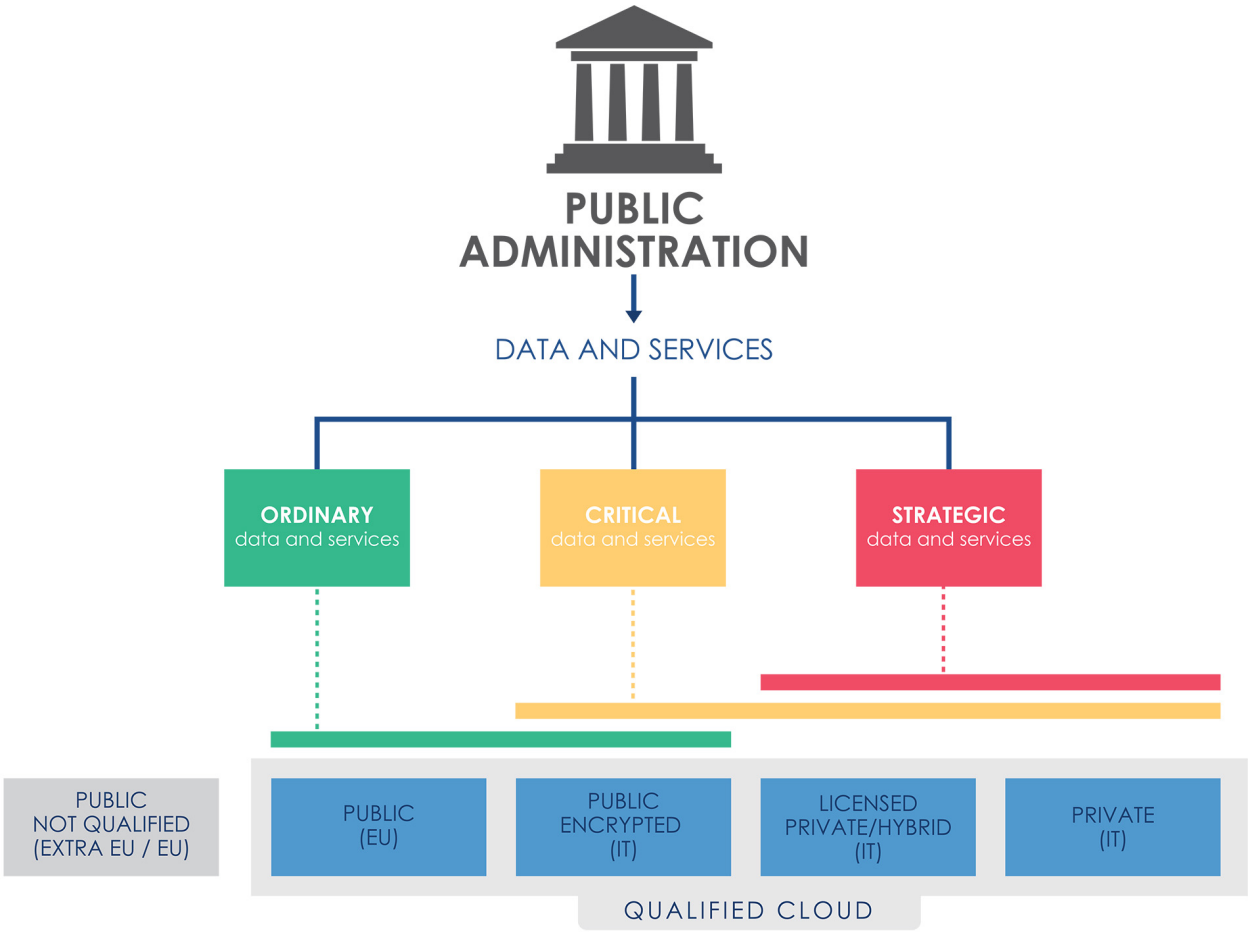
5.3 4.3 The National Strategic Hub

The rationalisation and enhancement of security and reliability of the PA's multiple data centres involves the development of a new IT infrastructure that is able to serve the multiple PAs located throughout the country: *the National Strategic Hub (NSH, known in Italian as "Polo Strategico Nazionale" - PSN)*[12].

The NSH aims to equip the PA with Cloud technologies and infrastructures that can benefit from the highest guarantees of reliability, resilience and independence. To this end, the NSH will be geographically distributed throughout the

[11] This proposal is similar to what has already been successfully implemented in other countries, e.g. the UK Digital Marketplace https://www.digitalmarketplace.service.gov.uk

[12] As provided for in Article 33-septies, paragraph 4, of the Decree-Law of 18 October 2012, no. 179, converted, with amendments, by Law No. 179 of 17 December 2012. 221.

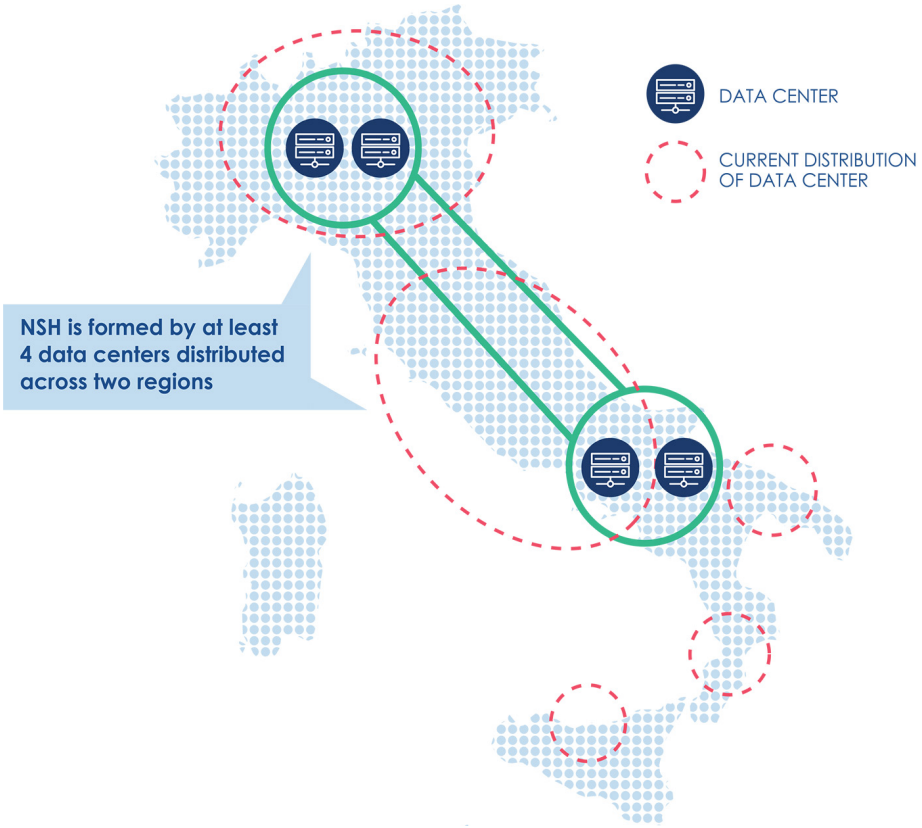

PUBLIC ADMINISTRATION
DATA AND SERVICES
ORDINARY data and services
CRITICAL data and services
STRATEGIC data and services
PUBLIC NOT QUALIFIED (EXTRA EU / EU)
PUBLIC (EU)
PUBLIC ENCRYPTED (IT)
LICENSED PRIVATE/HYBRID (IT)
PRIVATE (IT)
QUALIFIED CLOUD

country and located at the most suitable sites[13], in order to ensure adequate levels of business continuity and fault tolerance. The operational management of the NSH will be entrusted to qualified national providers on the basis of appropriate technical and organisational requirements. The providers will have to ensure control over the data in accordance with the relevant legislation, and it should help the PA to negotiate appropriate contractual conditions with Cloud Service Providers.

The NSH should allow the PA to guarantee, by design, compliance with security requirements, e.g. PSNC and NIS, and should enable the migration - which may in a first phase be performed via a *lift-and-shift* process - to IaaS and PaaS Cloud service models.

According to the classification provided in the previous section, the NSH will offer the *Encrypted Public Cloud (IT)* services, i.e. it will support for instance, on-premise encryption tools integrated on a Public Cloud for the PA, and the spectrum of private Cloud services, i.e. the *Licensed Private/Hybrid Cloud (IT)* and the *Qualified Private Cloud (IT)*.

In accordance with the classification and qualification procedures, the aim of the NSH is to support central administrations and the main local administrations, e.g. regional PA, local health authorities and metropolitan cities.



[13] Examples include the physical security levels of data centers, mitigation of natural disaster risk and integration with multiple connectivity sources.

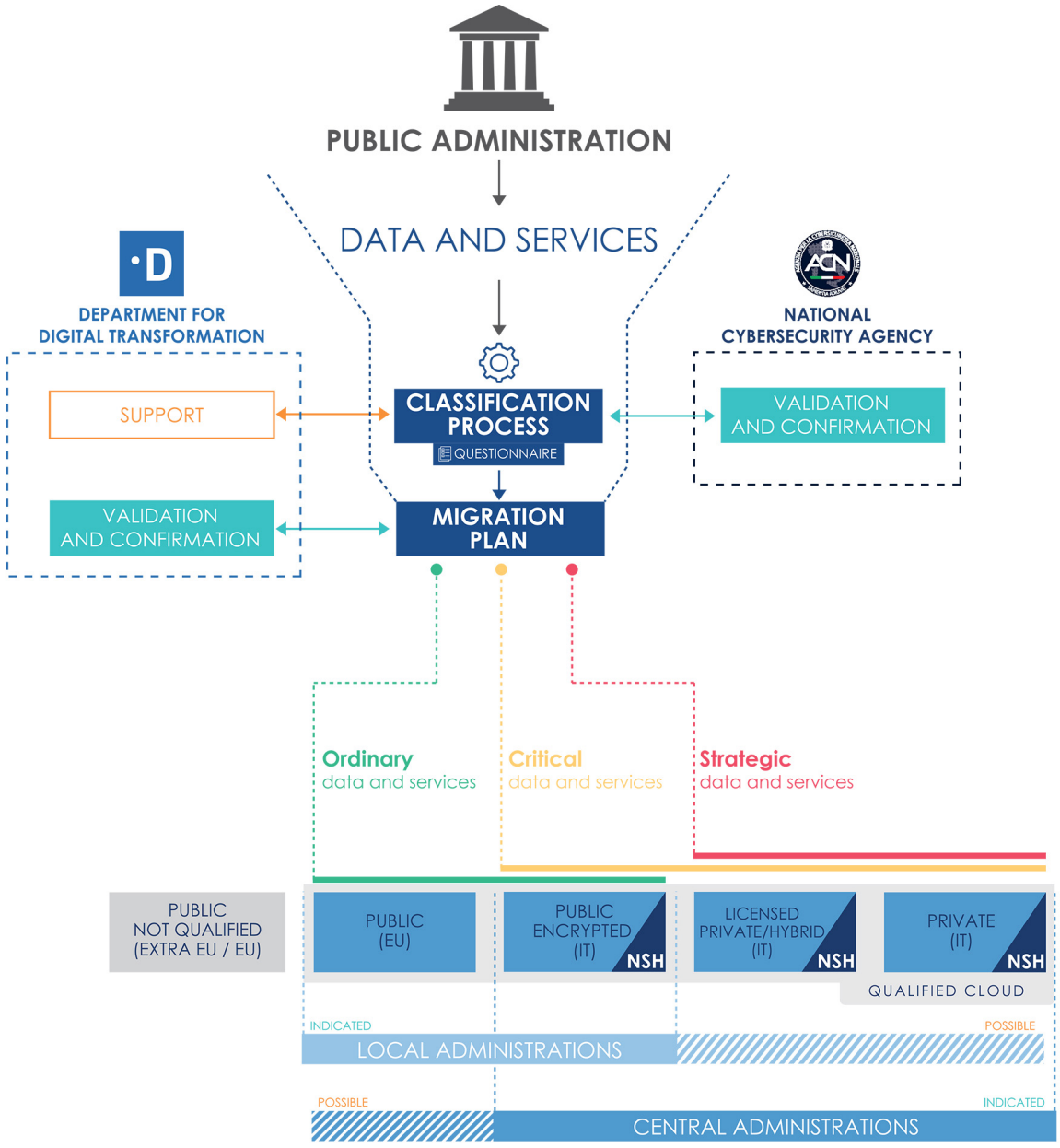
CAPITOLO 6

5. Public Administration's Migration to the Cloud

The migration to Cloud services or the NSH will be governed through a centralised, smooth and uniform process for all administrations.

Migration plans will then be defined according to the result of the classification of data and services. The classification and the migration plans will be defined on the basis of appropriately defined questionnaires, and will be supported, for their respective profiles, by the National Cybersecurity Agency (ACN) and the Department for Digital Transformation (DTD).

This process cannot be separated from the public sector's accountability; it will start with identifying and cataloguing the data and services managed by each PA; consequently it will apply a categorisation on the basis of the impact of potential data breach, regulatory constraints and security. The migration plan will be validated and confirmed by the Department and the Agency in order to ensure enforcement of the national Cloud strategy.


PUBLIC ADMINISTRATION
DATA AND SERVICES
DEPARTMENT FOR DIGITAL TRANSFORMATION
NATIONAL CYBERSECURITY AGENCY
SUPPORT
CLASSIFICATION PROCESS
QUESTIONNAIRE
VALIDATION AND CONFIRMATION
VALIDATION AND CONFIRMATION
MIGRATION PLAN
Ordinary data and services
Critical data and services
Strategic data and services
PUBLIC NOT QUALIFIED (EXTRA EU / EU)
PUBLIC (EU)
PUBLIC ENCRYPTED (IT)
NSH
LICENSED PRIVATE/HYBRID (IT)
NSH
PRIVATE (IT)
NSH
QUALIFIED CLOUD
INDICATED
POSSIBLE
LOCAL ADMINISTRATIONS
POSSIBLE
INDICATED
CENTRAL ADMINISTRATIONS

CAPITOLO 7

6. Adopting the Cloud Strategy

The Italian Cloud Strategy will be divided into subsequent phases according to the timeline proposed below:

PHASE 1 - *Publication of the call for tenders for the implementation of the NSH*: By the end of 2021 at the latest, the call for tenders for the implementation of the NSH will be published.

PHASE 2 - *Procurement contract awarding and implementation of the NSH*: The awarding of the tender should take place by the end of 2022 at the latest.

PHASE 3 - *Migration of administrations*: Starting from the end of 2022 at the latest, the migration of PAs to the NSH should begin and be completed by the end of 2025. During the migration phase, priority will be given to those Central Public Administrations that currently operate with their own data centres, classified as Category B, by AgID's census of PA ICT assets (e.g. data centers with structural and/or organisational deficiencies or that do not guarantee service continuity).