Technical Specification

ISO/IEC TS 10866

First edition
2024-11

Information technology — Cloud computing and distributed platforms — Framework and concepts for organizational autonomy and digital sovereignty

Technologies de l'information — Informatique en nuage et plates-formes distribuées — Cadre et concepts relatifs à l'autonomie organisationnelle et à la souveraineté numérique

Reference number
ISO/IEC TS 10866:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 38, *Cloud computing and distributed platforms*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

Organizational autonomy and digital sovereignty are important, complex and evolving subject areas whose implications have expanded in recent years, as organizations of all types address the challenges inherent to supplying and procuring digital capabilities in evolving environments.

Government objectives and policies can often be addressed through public or private partnerships, as these governments increasingly rely on industry to help address these goals to increase their prosperity while maintaining an appropriate degree of control and independence.

Since the same issues of independence and freedom of action and choice also apply to organizations – including private, public sector and not-for-profit – it is possible that such organizations will need to consider their own independence to achieve their goals.

This document defines a framework for understanding and evaluating the implications of digital sovereignty requirements and restrictions on the organization. It describes how the organization can configure its digital platform to appropriately balance those requirements with its own need for organizational autonomy to achieve its goals. The framework may be used by the organization itself, or by the policy makers and regulators of a sovereign entity which desire to examine the consequences of proposed digital sovereignty requirements and restrictions on organizations and industries.

The audience of this document includes:

a) Organizational leaders (e.g. Chief Information Officer, Chief Data Officer and Chief Compliance Officer), business or technical decision makers and digital platform architects who configure the organization's digital platform to ensure it has the right balance of digital autonomy to support and enable the goals of the organization to be achieved.

b) Policy makers and regulators who wish to understand the impact of digital sovereignty and autonomy matters.

Information technology — Cloud computing and distributed platforms — Framework and concepts for organizational autonomy and digital sovereignty

1 Scope

This document specifies concepts related to the intersection of digital sovereignty, organizational autonomy, and digital platform, and provides a framework enabling organizations to address these concepts.

This document is applicable to all organizations and policy makers involved in organizational autonomy and digital sovereignty in cloud services and distributed platforms.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 22123-1, *Information technology — Cloud computing — Part 1: Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 22123-1 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1 to entry: The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

[SOURCE: ISO/IEC 27000:2018, 3.50]

3.2
digital capability
information technology (3.5) for enabling or supporting a service, product or process of the *organization* (3.1)

[SOURCE: ISO/IEC 38500:2024, 3.10]

3.3
digital service
service offered by one party to another party by means of digital hardware or software technology, or both, including communication over a network

Note 1 to entry: In the context of this document, a service comprises one or more digital capabilities such as a cloud computing, edge computing, or some other distributed computing capability. Such a service will be subject to contract and typically have defined qualities of service, terms, and conditions for use.

Note 2 to entry: Cloud service, edge service, network service, broadcast service, and mobile service are all types of digital service. Not all types are discussed in this document.

[SOURCE: ISO/IEC TS 5928:2023, 3.1.1]

3.4
digital platform
set of correlated and cohesive *digital services* (3.3)

Note 1 to entry: A digital platform as described in this document enables and assists other participant digital services in conducting business with their customers, either by creating and facilitating a multi-sided market for those services, or by enabling the technological creation and operation of those services, or both.

Note 2 to entry: "Distributed platform" is often used as a synonym to emphasize those elements of a digital service, such as edge computing and mobile computing that go beyond the classical datacentres of cloud computing.

[SOURCE: ISO/IEC TS 5928:2023, 3.1.2]

3.5
information technology
IT
resources used to acquire, process, store and disseminate information or data

Note 1 to entry: Resources can include computer or communication equipment, sensors, software, cloud computing and other software-based services

[SOURCE: ISO/IEC 38500:2024, 3.5]

3.6
organizational autonomy
ability of an organization to make decisions independently of external influences

Note 1 to entry: Organizational autonomy is limited by factors such as resources and stakeholder requirements.

4 Organizational autonomy and digital sovereignty

Organizational autonomy and digital sovereignty are important and complex subject areas which have expanded in recent years, as organizations of all types address the challenges inherent to supplying and procuring digital capabilities in an environment of globally available cloud services, rapid technology innovation, and increasing cloud service customer (CSC) agility. Given many cloud services are offered globally, the changing regulatory frameworks in multiple, overlapping and potentially contradictory jurisdictions impact not only cloud service providers (CSPs) but also CSCs.

National sovereignty matters in general have been highlighted by events such as the Covid-19 pandemic, global supply chain issues, security and defence, the movement of people and border control, and other global issues, such as military conflicts and export restrictions.

Sovereignty matters can include:

— safety of citizens;

— conservation of national resources;

— national security;

— prosperity and economic development;

— governance and accountability.

Some of these sovereignty concerns become digital sovereignty concerns for reasons including the following:

— public and private organizations are applying digital platform solutions to address these issues, which elevates the importance and reliance on digital platforms;

— to grow their economy, governments realize they can leverage digital platform and services;

— security, privacy and resiliency are different in the digital world (as opposed to the analogue world);

— the reliance on foreign digital technology suppliers, who can be subject to third-party regulations, adds complexity to solutions;

— some of the underlying digital platforms are supplied by a limited number of companies, including foreign companies;

— governments are keen to encourage local innovation, and fear their local businesses being left behind or overtaken in the market;

— policy interoperability is a prerequisite for cross-border data transfer and is subject to change as national and global priorities change;

— each government and its organizations properly protects its own intellectual property rights (IPR) and takes various measures to do so;

— deriving the maximum value of data requires systems of mutual trust for freely sharing the data across borders.

While governments can potentially build their own customized technology solutions, this can create new security and sovereignty concerns. Many of these issues can, for example, be addressed through public-private partnerships, meaning that governments rely increasingly on private businesses and non-profit organizations to help address these issues and increase their prosperity while maintaining an appropriate degree of independence.

When it comes to the digital capabilities of organizations, the same concerns of independence and freedom of an action or choice also apply to organizations – including private, public and not-for-profit. To address these concerns, organizations can take into account the degree of independence (which is called “autonomy” in this document to distinguish it from national sovereignty) necessary to achieve their goals.

This document addresses sovereignty matters that:

a) are imposed by governments;

b) affect organizations (including private, public and non-for-profit organizations); and

c) impact the digital platforms that organizations use to support and enable their goals.

This is shown as the intersection in Figure 1.

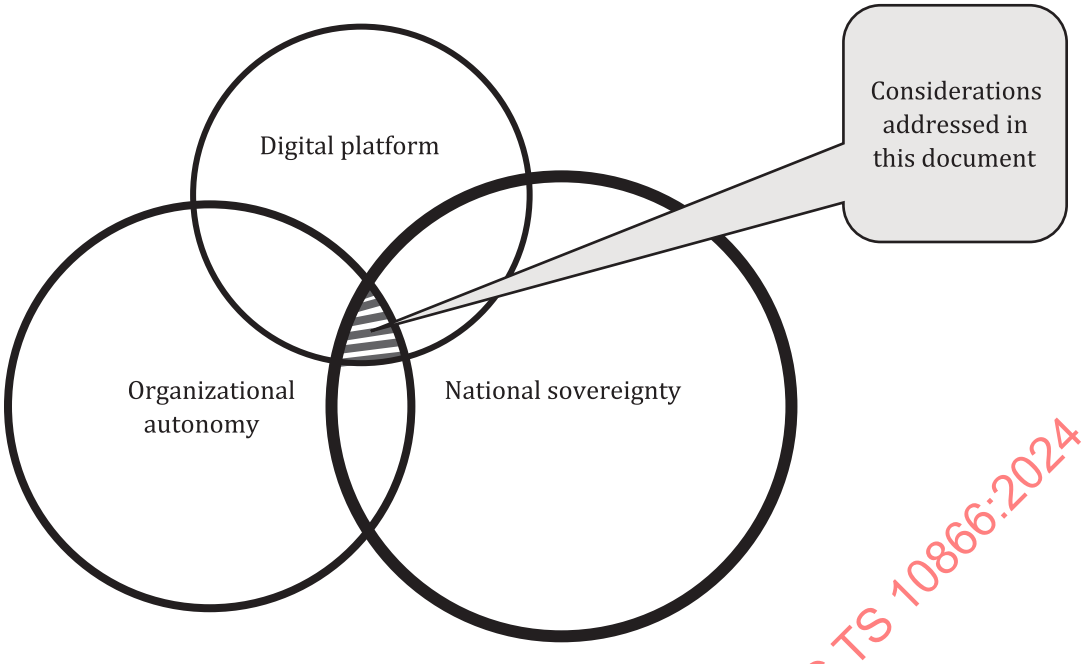


Figure 1 — Digital sovereignty matters addressed by organizations

5 Framework

5.1 Purpose

The purpose of this framework is to enable organizations to identify and evaluate organizational autonomy and digital sovereignty matters faced by organizations and balance the applicable digital capabilities to achieve their objectives.

The framework helps organizations choose or create appropriate digital services, configure their digital platform, and balance the requirements and restrictions of digital sovereignty with their own need for organizational autonomy. Applying this framework can also help organizations to refine their objectives and considerations when configuring or fine tuning the digital capabilities at their disposal to achieve this balance.

Most organizations operate in multiple jurisdictions, since even a single location is often subject to both local and federal administrations. Many organizations are cross-border, with customers, suppliers, or facilities across multiple geographic or political boundaries.

Digital sovereignty requirements in any of these jurisdictions can influence the objectives of the organization as well as the configuration of its digital platform. For example, some jurisdictions require data residency, which can require different digital capabilities than in other jurisdictions. That can impact not only the organization's overall digital platform but also its overall objectives and therefore its organizational autonomy.

Understanding these digital sovereignty requirements and restrictions while striking an appropriate balance with organizational autonomy is a key outcome of using the framework in this document.

5.2 Organizational objectives and digital capabilities

Figure 2 shows the high-level approach of the framework. To utilize this framework, the organization clarifies its objectives and the digital capabilities it requires to support and achieve these objectives. The organization also ensures a balance between these objectives and the digital sovereignty requirements it will encounter.

The framework utilizes an iterative approach, with the following steps as shown in Figure 2:

a) Determine organizational objectives and assess associated risks.

   1) In this step, the organization outlines its objectives, while considering the associated risks for achieving those objectives. Initially, this step will be organizationally focused (or a "business outcome"), include an understanding of the organization's risk appetite and have only a minor focus on the information technology needed to achieve the objectives.

   2) The first iteration of this step may be performed without insight into the digital capabilities required to achieve these objectives, but later iterations will benefit from such insight.

b) Identify the digital assets and capabilities required to achieve objectives.

   1) At this step, the broad organizational objectives are understood – but what digital capabilities are needed to either support those objectives, or to enable them? For example, some organizational objectives will only be capable of being achieved through the application of digital capabilities.

   2) Clarifying those supporting and enabling digital capabilities that are critical to the organization's objectives is the goal of this step. Initially, these capabilities can be at a fairly high level, e.g. digitally design the required manufacturing process. As the steps in the framework are iterated through, a more fine-grained description of the capability is helpful, e.g. map digital design plans to 3D printing machines located in manufacturing facilities in Eastern Europe.

c) For each digital capability, determine the desired degree of organizational autonomy.

   1) In this step, each of the digital capabilities should be examined in more detail to clarify its criticality and uniqueness to the organization and its objectives.

   2) This examination helps the organization to understand the importance of its autonomy for this capability, and the potential impact of the autonomy on external factors such as digital sovereignty. The required autonomy of some digital capabilities can be determined by the purpose of the organization, e.g. high precision manufacturing of electric motors can require a high degree of autonomy for an electric motor company, but possibly less autonomy for a haulage company..

   3) This step also involves a more detailed examination of potential digital sovereignty requirements on the digital capabilities in each jurisdiction.

   4) See 5.3 for more detail.

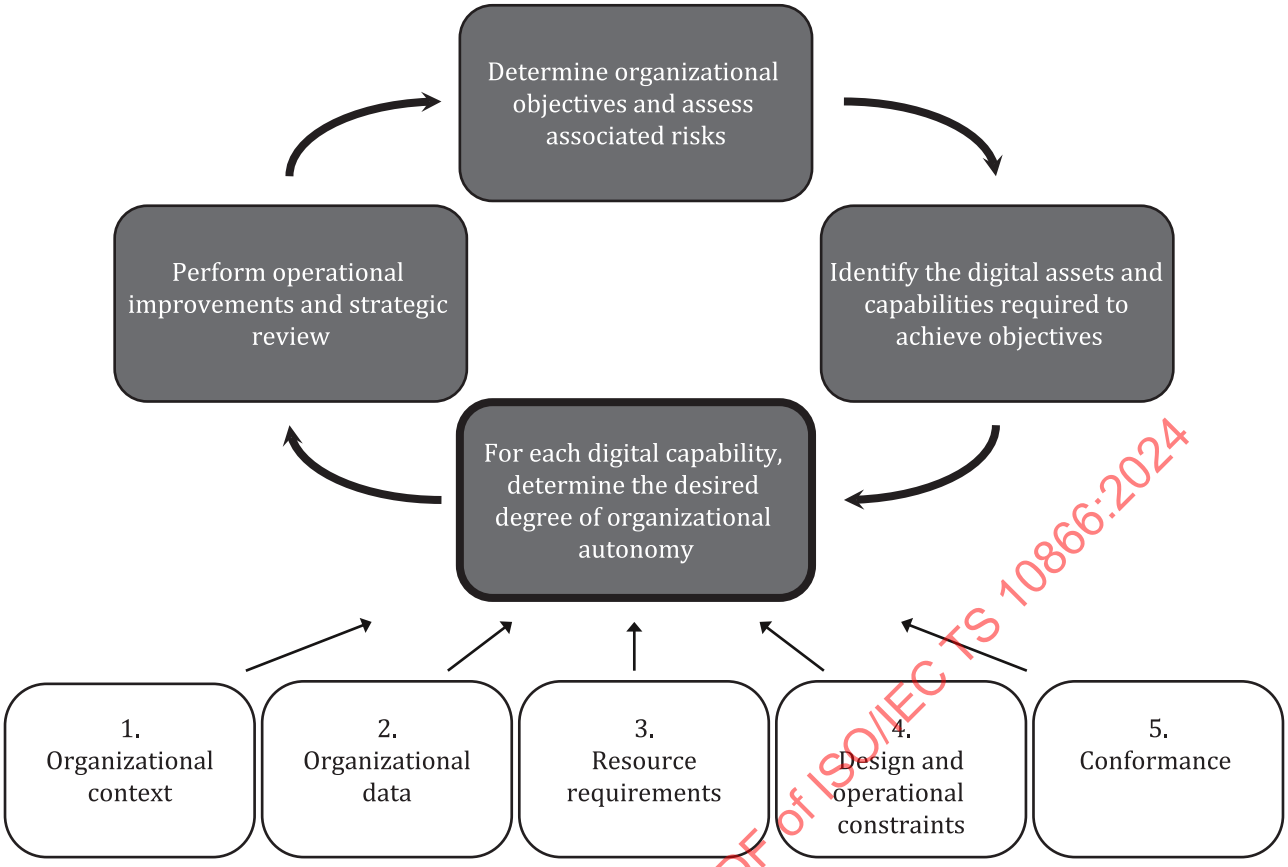
d) Perform operational improvements and strategic review

   1) In this final step, the organization learns about the digital capabilities that are needed to achieve the objectives. These learnings can come from more iterations of this framework through planning as well as actual implementation of the digital capabilities.

   2) The organization's processes and capabilities change, along with its context, including customers, stakeholders, and the digital sovereignty requirements applicable to the customers, suppliers and facilities.

   3) Owing to the changes cited in 2), the organization should review both its operations (how can they be made more efficient and with less risk) and its strategic plans (do the objectives of the organization need to be adjusted).

   4) The results of these reviews are then input to step 1 and the next iteration of the framework begins.



NOTE In this figure, the iterative activities of the framework are represented by black boxes. Aspects of digital capabilities to be considered are represented by white boxes.

Figure 2 — Organizational objectives, digital capabilities and inputs for evaluation

5.3 Determining the desired degree of organizational autonomy

For each digital capability required by the organization to meet its objectives, the organization takes many factors into account to appropriately balance the requirements and restrictions of digital sovereignty and the organization's own need for organizational autonomy.

Figure 2 also shows a way to achieve this balance by considering various factors including:

a) organizational context (e.g. competition, governance, policies, environmental and societal impacts);

b) classification and categorization of the data that this digital capability processes;

c) resource requirements such as time to market, funding, skills and technical infrastructure;

d) design and operational goals including degree of control, latency, or responsiveness

e) conformance to organizational policies (which can include the compliance issues of the multiple, overlapping and potentially contradictory jurisdictions in which the organization operates or plans to operate, as well as internally defined values and culture);

Organizations can consider the following common aspects when determining their desired degree of autonomy:

— data access, processing, and storage controls;

— data location requirements and restrictions;

- data flow boundary requirements and restrictions;
- access by extraterritorial authorities;
- control over the organization's digital identities and attribute-based access controls;
- sovereignty of operation e.g. whether cloud services and workloads will continue to run and be available even if a government has applied sanctions on another government or an organization ;
- cost and requirements for service switching from one provider to another (to mitigate vendor lock-in);
- data portability, portability of digital assets/artefacts including data to lower cost of switching;
- degree of interoperability required in order to develop multi-vendor solutions;
- open-source software;
- data portability requirements and transparency, e.g. use of cloud native technologies to provide for workload portability or interoperability requirements;
- encryption requirements e.g. key management;
- architectural issues and related certifications related to sovereignty;
- network requirements e.g. whether extraterritorial fibre requires additional redundancy;
- degree to which the organization requires cybersecurity protection, the technical choices involved, such as encryption issues and key management;
- the extent of data security required, in motion, at rest and during compute;
- the degree to which the organization requires data centre redundancy to address national security concerns;
- the degree to which foreign government access to data is expected to be curated;
- the degree to which trusted data sharing or confidential computing is required;
- the degree of transparency regarding data access and compliance with sovereign-imposed data obligations and restrictions required by the organization. The elements of transparency approach include the following:
  - What data are collected: To what degree the organization expects its digital service providers to describe the most important types of data they will collect, such as data relating to health, sexuality, and location.
  - How data are used: To what degree the organization expects its digital service providers to describe the most significant uses of data..
  - Sharing data: To what degree the organization expects its digital service providers to inform it when they share customer data with third parties, and what policies they apply. For example, companies should tell customers clearly how and why they disclose customer data to governments, and the extent to which the law allows them to disclose that. They should also tell customers if they will share customer data with third parties such as data brokers or advertisers or make it available for sale.
  - Business models: To what degree the organization expects its digital service providers to disclose how they profit and how that affects their use of customer data.

The list above is neither exhaustive nor prescriptive. Each organization can draw its own conclusions regarding which aspects are applicable and should be reviewed in the framework.

6 Application of the framework

6.1 General

Digital sovereignty requirements are described uniquely by each government and often evolve over time. Similarly, each organization determines how to achieve its own autonomy goals within the requirements and restrictions of each applicable jurisdiction.

This framework is flexible so that organizations can apply it in ways which are specific to the organizational context and the digital capabilities required to achieve its goals. For example, an organization can have some capabilities which are very specific to certain customer use cases, while other capabilities are more general across a range of the organization's activities.

Regardless, the organization will likely note that certain patterns emerge. An advantage of this framework is that it allows the organization to discern these patterns and make special note of the capabilities which are more unusual or more critical to the success of the organization's objectives.

Some examples specified in 6.2 to 6.6 clarify this approach. Conformance and compliance across multiple jurisdictions can involve a complex matrix of requirements and restrictions, so these examples are greatly abbreviated compared to how such an organization would use the framework in actual practice.

6.2 Example: Critical infrastructure under threat

6.2.1 General

This example analyses an organization which provides critical infrastructure in a threatened region. Infrastructure identified as critical always requires additional oversight, and this is even more so in times of conflict.

The organization wants to provide business continuity in case of attack, but there are some additional digital sovereignty concerns beyond typical business continuity planning. These special organizational goals should be considered when identifying the digital assets and the digital capabilities to feed into the framework.

This organization receives requirements to ensure their digital solution supports the applicable goals of continuing to communicate with citizens, and protecting sensitive and confidential data from use by attackers. In addition, this goal can require a data denial capability.

This is not a comprehensive list of sovereign requirements for the organization, but it is enough to begin using the framework.

For each of the goals, the organization shall identify the digital capabilities needed to achieve the goal. Some capabilities can apply to multiple goals, but this is not always the case.

An application of the framework produces the results in 6.2.2 to 6.2.6.

6.2.2 Organizational context

The context in which the organization operates includes the following aspects:

— whether the organization has been classified as critical infrastructure by an applicable government;

— the expected impacts of an invasion or attack;

— any existing conditions regarding data residency and redundancy;

— the availability of resources.

6.2.3 Data categorization, classification and usage

The data managed by the organization includes:

— public data which shall be kept publicly visible;

— private and high-impact data such as health records and account data, which shall remain both accessible and confidential;

— sensitive or top-secret data which has additional security and access controls.

6.2.4 Required resources

The resources required by the organization include:

— time and expertise for design cycles to define and prototype a reference architecture;

— staff trained to invoke the emergency capabilities.

6.2.5 Design and operational considerations

The operational constraints of the organization include:

— a data governance programme, including reference architecture for emergency protocols and capabilities;

— onsite staff authorized to invoke the emergency protocols and capabilities.

6.2.6 Conformance

The organization conforms to:

— organizational policy, ethics and culture;

— appropriate settings applied based on data classification.

NOTE Additional legal requirements can apply, such as changing government requirements and restrictions while under attack or invasion (e.g. a wartime response can require cross-border data transfer, even if the default is to limit or restrict such transfers).

6.3 Example: Critical data are recoverable

6.3.1 General

This example analyses an organization which provides critical infrastructure in a threatened region. The organization in this example is similar to the organization in 6.2, but it is focused on a single sovereign requirement of ensuring that the most critical data for continuity is protected and recoverable. This can require the capability for data redundancy. An application of the framework produces the results in 6.3.2 through 6.3.6.

6.3.2 Organizational context

The context in which the organization operates includes the following aspects:

— whether the organization has been classified as critical infrastructure by an applicable government;

— existing conditions regarding data location and its redundancy;

— the degree of data redundancy required to protect against loss e.g. the use of multiple cloud storage regions and multiple cloud service providers;

— the type of data (transactional, static, structured or unstructured, size, streaming, etc.);

— existing contingency plans for data recovery.

6.3.3 Data categorization, classification and usage

The data managed by the organization includes:

— public data that is kept publicly visible;

— private and high-impact data such as health records, which are kept accessible but remain confidential;

— sensitive, top-secret data which has additional security implications and access controls.

6.3.4 Required resources

The resources required by the organization include:

— time and expertise for design cycles to define and prototype a reference architecture;

— network capacity – bandwidth and latency;

— storage capacity;

— cross-border network topology and associated threat exposure to the terrestrial and submerged infrastructure.

6.3.5 Design and operational considerations

The operational constraints of the organization include:

— a data governance programme, including reference architecture for emergency protocols and capabilities;

— onsite staff authorized to invoke the emergency protocols and capabilities;

— assurance that applications can consume the data from redundant locations.

6.3.6 Conformance

The organization conforms to:

— organizational policy, ethics and culture;

— appropriate settings applied based on data classification.

NOTE Additional legal requirements can apply, such as changing government requirements and restrictions while under attack or invasion (e.g. a wartime response can require cross-border data transfer, even if the default is to limit or restrict such transfers).

6.4 Example: Account management of a global digital platform

6.4.1 General

In this example, an organization operates a global online platform. It wants to provide the same consistent services using a common architecture (i.e. multi-cloud, edge and Internet of Things) in multiple locations, including those in different jurisdictions, such as in different regions. There are many types of services platforms like this including streaming services, fintech, edtech and smart city services to citizens. This example focuses on streaming services.

In this example, the most important digital capabilities are for membership and account management. The organization has a goal to acquire members globally and manage their online accounts while strongly protecting personal data in multiple and potentially conflicting jurisdictions.

Sovereignty concerns arise not only because the data of citizens must be protected, but also because some content can violate local cultural norms or regulations and be restricted for some or all users.

6.4.2 Organizational context

The context in which the organization operates includes the following aspects:

— how regulated infrastructure is defined and any requirements or restrictions about its use;

— users who can be citizens in one geographic region, yet sign up while in another region, and perhaps even access the service when they are in yet another region.

6.4.3 Data categorization, classification and usage

The data managed by the organization includes:

— public data kept publicly visible;

— personal data subject to multiple data protection laws;

— private and high-impact data such as viewing records, and account metadata kept accessible but remaining confidential;

— temporarily restricted data which has additional security and access controls;

— account data and metadata that can be processed or stored in a different jurisdiction than where it was created and where a customer resides.

6.4.4 Required resources

The resources required by the organization include:

— time and expertise for design cycles to define and prototype a reference architecture;

— identity federation;

— network capacity and availability.

6.4.5 Design and operational considerations

The operational constraints of the organization include:

— identity federation to ensure privacy compliance in multiple regions;

— licensed content only delivered to specific regions (where being viewed by a user or where a user account was created);

— ability to determine where consumption is occurring;

— network latency.

6.4.6 Conformance

The organization conforms to:

— organizational policy, ethics and culture.

NOTE Additional legal requirements can apply, such as government requirements and restrictions related to digital safety and content, including age restrictions.

6.5 Example: Global streaming platform content delivery

6.5.1 General

This is another example of a global streaming platform. In this case, the most important digital capability is for video streaming over local networks.

Sovereignty concerns arise not only because of differing cultural norms and different intellectual property protections for streaming content creators, but also because streaming can be occurring on limited local network resources.

6.5.2 Organizational context

The context in which the organization operates includes the following aspects:

— how regulated infrastructure is defined and determined;

— rapid production of content or time to market;

— variable licensing structures globally;

— different political sensitivity towards some content in various jurisdictions;

— support for mandated public service requirements (e.g. news, emergency broadcasting);

— any relevant national network neutrality considerations.

6.5.3 Data categorization, classification and usage

The data managed by the organization includes:

— public data kept publicly visible;

— personal data subject to multiple data protection laws;

— private and high-impact data such as viewing records, and account metadata kept accessible but remaining confidential;

— temporarily restricted data which has additional security and access controls;

— account data and metadata can be processed or stored in a different jurisdiction than where it was created and where a customer resides;

— embargoed data which has additional security and access controls;

— temporarily restricted data which must never be inappropriately disclosed.

6.5.4 Required resources

The resources required by the organization include:

— time and expertise for design cycles to define and prototype a reference architecture;

— local caching network(s) considerations;

— monitoring, deployment, maintenance;

— local network capacity and availability.

6.5.5 Design and operational considerations

The operational constraints of the organization include:

— content distribution networks (CDNs) requiring monitoring, deployment, and maintenance;

— collaboration with local Internet service providers (ISPs) for takedowns etc.;

— ability to determine where consumption is occurring;

— ability to manage bandwidth usage to meet local requirements and restrictions.

6.5.6 Conformance

The organization conforms to:

— content licensing permissions;

— organizational policy, ethics and culture;

— permitted bandwidth constraints;

— content used in video streaming which can be subject to protection under Intellectual Property Rights (IPR), including copyright.

NOTE Additional legal requirements can apply, such as government requirements and restrictions related to digital safety and content, including age restrictions.

6.6 Example: Trusted data sharing within a food services supply chain

6.6.1 General

This example involves a prepared food manufacturer that is required to disclose the provenance of all the ingredients involved in the manufacture of their food products. Sovereignty concerns arise because the transparency derived from this requirement benefits farmers and suppliers, consumers and anyone attempting to measure the societal impact of their food, all of whom are valuable to governments.

The organization being examined in the example is the prepared food manufacturer. The high-level architecture for their data sharing resembles a dataspace. For the purposes of this example, a dataspace is a cloud computing arrangement with:

— a shared trust model, vocabulary, and semantics;

— data contract negotiation and discoverability.

Although the goals of the food manufacturer were imposed to comply with local law, they also benefit the manufacturer even under typical business conditions. These benefits include:

— sharing data between organizations to achieve a shared business goal;

  — e.g. goals of efficiency and resilience of the supply chain or value chain;

  — e.g. organizations such as regulators and researchers;

  — data can be shared via exchange or via in situ processing;

— respecting the rights and obligations associated with the data;

— protecting trade secrets of both the food manufacturer and its suppliers;

— reducing governance and compliance costs;