FINAL DRAFT
Technical Specification

ISO/IEC DTS 10866

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

ISO/IEC JTC **1**/SC **38**

Secretariat: **ANSI**

Voting begins on:
2024-07-02

Voting terminates on:
2024-08-27

Reference number
ISO/IEC DTS 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:

1. 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.
2. 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

4.1 Overview

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.

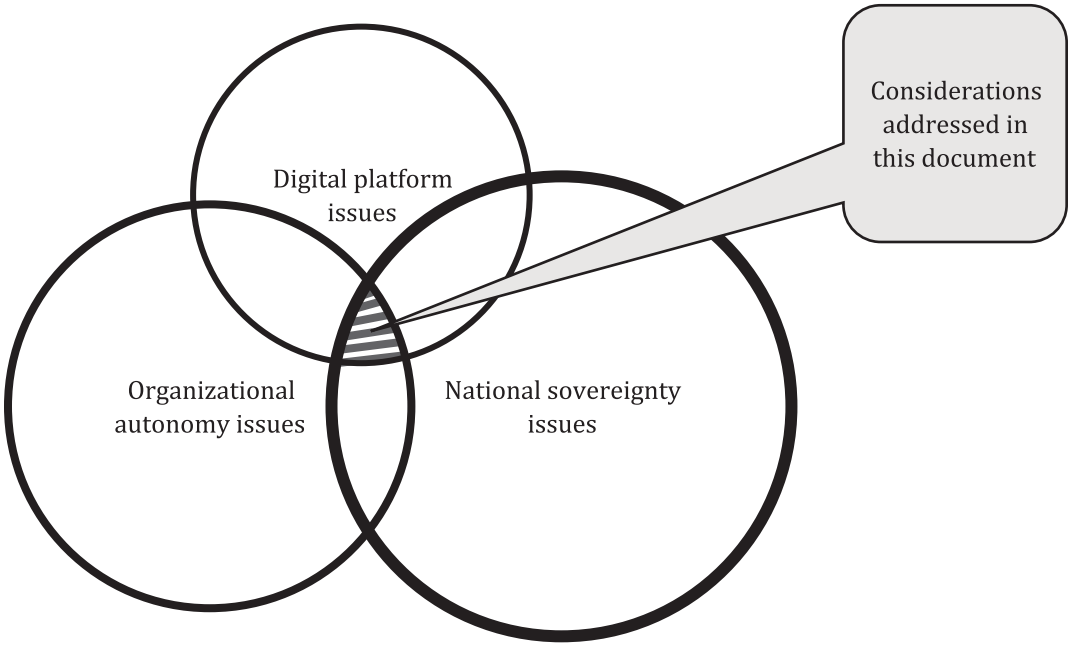

Figure 1 — Digital sovereignty matters addressed by organizations

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.