DRAFT International Standard

ISO/IEC DIS 22678

Information technology — Cloud computing — Guidance for policy development

ICS: 35.210

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

Secretariat: **ANSI**

Voting begins on:
2026-06-18

Voting terminates on:
2026-09-10

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 22678:2026(en)

© ISO/IEC 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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 ..... **vi**
Introduction ..... **vii**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviated terms **3**
5 Summary of this document **4**
5.1 Purpose of this document 4
5.2 Intended audience 4
5.3 How to use this document 5
6 Understanding cloud computing aspects for policy development **5**
6.1 Introduction 5
6.2 Cloud computing essential characteristics 5
6.2.1 Standard definition of cloud computing 5
6.2.2 Essential characteristics of cloud computing (from ISO/IEC 22123-2:2023) 6
6.3 Major benefits of cloud computing 7
6.3.1 Benefits for cloud service customers (CSCs) 7
6.3.2 Benefits for society 8
6.4 Implications for policy makers 9
6.4.1 Shared responsibilities 9
6.4.2 Cloud services crossing multiple jurisdictions 10
6.4.3 Economics of a CSP operating a large cloud service 11
6.4.4 What global, scalable public cloud computing makes possible 12
6.4.5 Implications of cloud service scale and velocity 12
6.4.6 Implications of continuous development 13
6.4.7 Implications of multi-tenant cloud services 13
6.4.8 Implications of geographical restrictions 13
6.5 The meaning of “platform” in cloud computing 14
6.5.1 Ambiguity of "digital platform" 14
6.5.2 Digital economic platform 15
6.5.3 Digital technology platform 15
6.6 Cloud service data categorization and classification 15
6.7 Interoperability and portability 16
6.7.1 General terminology 16
6.7.2 Interoperability in a cloud computing environment 16
6.7.3 Portability in a cloud computing environment 17
6.8 Switching in a cloud computing environment 17
6.8.1 General 17
6.8.2 Technical challenges 18
6.8.3 How often do CSCs switch to a different CSP? 18
6.8.4 Obstacles to switching 19
6.8.5 Competing CSP architectures 20
6.8.6 Challenges when writing policy on switching 20
6.9 CSC Digital assets 21
6.9.1 General 21
6.9.2 Basic digital assets 22
6.9.3 Virtualized digital assets 22
6.9.4 Compound assets 23
6.9.5 Metadata assets 23
6.9.6 Derived data from or about service use 23
6.9.7 Data linking assets 25
6.9.8 Digital assets unsuitable for portability 25
6.10 Trust and transparency 25

© ISO/IEC 2026 – All rights reserved

6.10.1 General ... 25
6.10.2 Trust in cloud services ... 26
6.10.3 Trust in the legal environment ... 26
6.10.4 Trust in the technologies and standards ... 27
6.10.5 Trust in the data ... 27
6.10.6 Trusted Intermediaries ... 27
6.11 Service continuity in exceptional circumstances ... 28
6.12 Conformance, certification, audit ... 28
6.13 Challenges for small and medium-sized enterprise (SME) adoption ... 29
6.13.1 General ... 29
6.13.2 Non-IT small and medium-sized enterprises ... 29
6.13.3 IT-oriented small and medium-sized enterprises ... 29
6.13.4 Impact of policies on small and medium enterprises (SMEs) ... 30
6.14 Digital sovereignty and autonomy ... 30
6.15 Dataspaces ... 31
6.15.1 General ... 31
6.15.2 How a dataspace works ... 31
6.15.3 Automation in dataspaces ... 32
6.15.4 Dataspace governance ... 32
6.15.5 Dataspaces and cloud computing ... 32
6.16 Multi-cloud ... 32
6.16.1 General ... 32
6.16.2 Different services from different CSPs ... 32
6.16.3 In-parallel use ... 33
6.16.4 Hidden cloud services ... 33
6.16.5 False multi-cloud deployments ... 33

7 Using ISO/IEC standards to assist in developing policies that cover cloud computing ... 34
7.1 ISO/IEC standards relevant to cloud computing policy development ... 34
7.1.1 General ... 34
7.1.2 ISO/IEC 19086 series of standards as applicable to trust and transparency ... 38
7.1.3 ISO/IEC 19944 as applicable to clarify data concepts ... 40
7.1.4 ISO/IEC 27701 - Privacy information management system (PIMS) ... 41
7.2 Other significant standards, specifications, and documents ... 42

8 Considerations when developing policy ... 42
8.1 The purpose of "considerations" in this document ... 42
8.2 General considerations for all types of policy ... 43
8.3 Considerations for regulatory policy ... 44
8.3.1 Context ... 44
8.3.2 Multi-tenant issues ... 44
8.3.3 Avoiding unnecessary barriers to cloud adoption ... 44
8.3.4 Measurement and logging ... 45
8.3.5 Trust and transparency ... 45
8.3.6 Interoperability and portability ... 46
8.3.7 Cloud service provider switching ... 47
8.3.8 Digital assets ... 47
8.3.9 Security and privacy ... 47
8.3.10 Dataspaces ... 48
8.4 Considerations for advisory policy ... 48
8.4.1 Context ... 48
8.4.2 Promotion of cloud technology adoption ... 48
8.4.3 Terminology and taxonomy ... 49
8.4.4 Adoption by small and medium enterprises ... 49
8.4.5 Supplier certifications ... 49
8.4.6 Network connectivity ... 49
8.4.7 Interoperability, portability, and switching ... 50
8.4.8 Multi-cloud ... 50
8.5 Considerations for procurement policy ... 51
8.5.1 General ... 51

© ISO/IEC 2026 – All rights reserved

8.5.2 Terminology and taxonomy 51
8.5.3 Cloud service deployment models 51
8.5.4 Supplier certifications 51
8.5.5 Interoperability, portability, and switching 52
Annex A (informative) **Relationship between key characteristics and implications** **53**
Annex B (informative) **Other relevant standards, specifications, and documents** **54**
Bibliography **56**

© ISO/IEC 2026 – All rights reserved

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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

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.

This document was prepared by Joint Technical Committee ISO/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.

© ISO/IEC 2026 – All rights reserved

Introduction

Cloud computing has become a major industry throughout the world in recent years, and today comprises a global network of large and small data centres and telecommunications networks, operated by many different cloud service providers, offering vast numbers of different cloud services to their customers. These cloud services range from simple email and productivity applications, through replacements for traditional on-premises software, up to advanced services that cannot be constructed in any other way, such as social networks, big data processing, machine learning, and cognitive services.

Cloud computing offers many benefits to cloud service customers, to governments, and to society.

As with all commercial services, governments and enterprises are adopting policies to ensure that customer and governmental interests are protected.

This document provides information and guidance to assist with the development of policies concerning the deployment and use of cloud computing systems and services. This document is intended for use by lawmakers, regulators and customer management as well as cloud computing providers and partners.

This document is intended for use by lawmakers, regulators, cloud service procurement teams and customer management as well as cloud computing providers and partners.

© ISO/IEC 2026 – All rights reserved

Information technology — Cloud computing — Guidance for policy development

1 Scope

This document provides guidance on the use of international standards as a tool in the development of those policies that govern or regulate cloud service providers (CSPs) and cloud services, and those policies and practices that govern the use of cloud services in organizations.

This includes content that explains cloud computing concepts and the role of cloud computing international standards in formulating policies and practices.

The document makes references to various international standards. Where possible, these standards are ISO/IEC standards. Where a suitable ISO/IEC standard is not available, references are made to documents published by other WTO-registered standards bodies[1)].

As explained in the WTO Agreement on Technical Barriers to Trade (TBT), standards play a vital role in supporting technical regulations and conformity assessment, however this document does not cover matters of trade.

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 22123-1:2023, *Information technology — Cloud computing — Part 1: Vocabulary*

ISO/IEC 22123-2:2023, *Information technology — Cloud computing — Part 2: Concepts*

ISO/IEC 22123-3:2023, *Information technology — Cloud computing — Part 3: Reference architecture*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 22123-1:2023 and the following apply.

ISO and IEC maintain terminological 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
jurisdiction
⟨cloud computing⟩ geographical or corporate area over which a cloud computing policy extends

Note 1 to entry: In a government policy context this will generally be the geographical area over which the body enacting the policy has legal authority either as government or as authorized regulator.

1) The WTO ISO Standards Information Gateway (http://tbtcode.iso.org) is the official portal listing all standardising bodies that have accepted the Code of Good Practice. This is the authoritative source for up-to-date information on which bodies are "recognised" for TBT purposes. The Code is open to any standardising body within a WTO Member's territory, and acceptance is voluntary but strongly encouraged by the WTO.

© ISO/IEC 2026 – All rights reserved

In an enterprise or government agency environment, the jurisdiction of a policy can cover a business function, department, agency, or other organisational area of responsibility not tied to geography.

Note 2 to entry: The use of <cloud computing> indicates that this term is being defined only for the cloud computing context, and should not be confused with the many other uses of "jurisdiction" in other contexts, especially for regulations and other policies.

3.2
observed derived data
subset of cloud service derived data containing factual records of interactions that the CSC has had with a cloud service

Note 1 to entry: Examples of observed derived data are access logs, call logs, change records, and audit records.

[SOURCE: ISO/IEC DIS 19941-1 [1]]

3.3
inferred derived data
subset of cloud service derived data created by the CSP through analysis of the cloud service and its usage

Note 1 to entry: Inferred derived data is often a subjective and approximate estimate rather than an objectively calculated derivative.

Note 2 to entry: Inferred derived data is often (though not exclusively) used to estimate CSC attributes, interests, and potential behaviours.

Note 3 to entry: Examples of using inferred derived data include product recommendations.

[SOURCE: ISO/IEC DIS 19941-1 [1]]

3.4
dataspace
data space
environment enabling trusted data sharing between participating parties, based on an agreed governance framework, along with an agreed set of policies, semantic models, standardized protocols, processes, and facilitating services

[SOURCE: ISO/IEC DIS 20151 [2]]

3.5
trusted cloud service
cloud service that satisfies a set of requirements such as transparency for governance, management and security so that a cloud service customer (CSC) can be confident in using the cloud service

Note 1 to entry: The set of requirements will vary depending on the involved cloud service customer, the nature of the cloud service and the governing *jurisdiction* (3.1).

Note 2 to entry: The set of requirements could also be related to additional cross-cutting aspects such as performance, resiliency, reversibility, SLAs, etc.

Note 3 to entry: Transparency means that the cloud service provider (CSP) should commit to the CSC that they have appropriate and clear control and reporting mechanisms for governance, management and security, such as SLA commitments, online announcements, data handling policies, etc.

[SOURCE: ITU-T Y.3501:2016 [3]]

3.6
CSC digital asset
class of data objects that includes CSC data and a subset of cloud service derived data essential for the effective use of the cloud service

Note 1 to entry: Examples of cloud service derived data that are part of CSC digital asset are configuration settings, security, and access and control rights management. Such cloud service derived data are sometimes referred to as CSC metadata.

© ISO/IEC 2026 – All rights reserved

Note 2 to entry: Examples of cloud service derived data that are not part of CSC digital asset are those covered by the intellectual property rights of others, or that constitute a trade secret of another party, or that can compromise the security and integrity of the cloud service.

Note 3 to entry: CSPs and CSNs also have their own digital assets.

Note 4 to entry: CSC digital assets are in digital form, limited to that for which the CSC has control and is independent from its contractual relationship with the CSP.

[SOURCE: ISO/IEC DIS 19941-1 [1]]

4 Abbreviated terms

API	application programming interface
ATAG	authoring tool accessibility guidelines
BSI	British Standards Institution
CCRA	cloud computing reference architecture
CSA	cloud service agreement
CSC	cloud service customer
CSN	cloud service partner
CSP	cloud service provider
CSU	cloud service user
DDoS	distributed denial of service (attack)
DPA	data protection authority
EU	European Union
GDPR	General Data Protection Regulation (EU and UK)
IaaS	infrastructure as a service
ICT	information and communications technology
IEC	International Electro-technical Commission
IETF	Internet engineering task force
IoT	internet of things
ISMS	information security management system
ISO	International Organization for Standardization
IT	information technology
ITU	International Telecommunication Union
ITU-D	ITU Development sector (assisting developing nations)
ITU-T	ITU Telecom sector (responsible for standardization)
JTC 1	Joint Technical Committee 1 (a joint project between the ISO and IEC on standards for ICT)

© ISO/IEC 2026 – All rights reserved