TECHNICAL REPORT

ISO/IEC TR 22678

First edition
2019-01

Information technology — Cloud computing — Guidance for policy development

Reference number
ISO/IEC TR 22678:2019(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Abbreviated terms **2**

5 Summary of this document **3**

5.1 Purpose of this document 3

5.2 Intended audience 3

5.3 How to use this document 4

6 Understanding cloud computing aspects for policy development **4**

6.1 Introduction 4

6.2 Cloud computing essential characteristics 4

6.2.1 Standard definition of cloud computing 4

6.2.2 Essential characteristics of cloud computing (from ISO/IEC 17788) 4

6.3 Major benefits of cloud computing 5

6.3.1 Benefits for cloud service customers (CSCs) 5

6.3.2 Benefits for society 7

6.4 Implications for policy makers 7

6.4.1 Shared responsibilities 7

6.4.2 Cloud services which are deployed and managed across multiple jurisdictions 8

6.4.3 Economics of managing a global cloud service 8

6.4.4 What global, scalable public cloud computing makes possible 9

6.4.5 Implications of service scale and velocity 9

6.4.6 Implications of continuous development 10

6.4.7 Implications of multi-tenant cloud services 10

6.4.8 Implications of geographical restrictions 10

6.4.9 The need for cloud service data categorisation and classification 11

6.4.10 Interoperability and portability 12

6.4.11 Trust and transparency 13

6.4.12 Exceptional circumstances 14

6.4.13 Compliance, certification, audit 15

6.4.14 Challenges for small and medium sized enterprise (SME) adoption 15

7 Using international standards to assist in developing policies that cover cloud computing **16**

7.1 International standards relevant to cloud computing policy development 16

7.1.1 ISO/IEC 19086 series of standards as applicable to trust and transparency 19

7.1.2 ISO/IEC 19944 as applicable to clarify data concepts 20

7.1.3 ISO/IEC 27552, Privacy information management systems 21

7.2 Other significant standards, specifications, and documents 22

8 Considerations when developing policy **22**

8.1 Considerations for regulatory policy 22

8.1.1 General 22

8.1.2 Multi-tenant issues 23

8.1.3 Avoiding unnecessary barriers to cloud adoption 23

8.1.4 Trust and transparency 24

8.1.5 Interoperability and portability 24

8.1.6 Security and privacy 25

8.2 Considerations for advisory policy 25

8.2.1 General 25

8.2.2 Promotion of cloud technology adoption 26

8.2.3 Terminology and taxonomy 26
8.2.4 Adoption by small and medium enterprises 26
8.2.5 Supplier certifications 26
8.2.6 Network connectivity 26
8.2.7 Interoperability and portability 27
8.3 Considerations for procurement policy 27
8.3.1 General 27
8.3.2 Terminology and taxonomy 27
8.3.3 Cloud service deployment models 28
8.3.4 Supplier certifications 28
8.3.5 Interoperability and portability 28
9 Conclusions **28**
Annex A (informative) **Relationship between key characteristics and implications** **29**
Annex B (informative) **Other relevant standards, specifications, and documents** **30**
Bibliography **32**

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.

Introduction

Cloud computing has become a major industry throughout the world in recent years, and today comprises a global network of large and small datacentres 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 to assist with the development of such policies concerning the deployment and use of cloud computing systems and services.

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 organisations.

This includes material 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.

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 17788, *Information technology — Cloud computing — Overview and vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17788 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
cloud computing
paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand

Note 1 to entry: Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

[SOURCE: ISO/IEC 17788:2014, 3.25]

3.2
jurisdiction
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 authorised regulator. However, in an enterprise or government agency environment, the jurisdiction of a policy might cover a business function, department, agency, or other organisational area of responsibility not tied to geography.

4 Abbreviated terms

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
EN	European Norm
EU	European Union
IaaS	Infrastructure as a Service
ICT	Information and Communications Technology
IEC	International Electro-technical Commission
ISO	International Organisation for Standardisation
IT	Information Technology
ITU	International Telecommunication Union
ITU-T	ITU Telecom sector (responsible for standardisation)
JTC1	Joint Technical Committee 1 (a joint project between the ISO and IEC on standards for ICT)
MLAT	Mutual Legal Assistance Treaty
PaaS	Platform as a Service
PII	Personally Identifiable Information
SaaS	Software as a Service
SC 27	Sub-committee 27 of JTC1, responsible for information security standards
SC 38	Sub-committee 38 of JTC1, responsible for cloud computing standards
SLA	Service Level Agreement
SLO	Service Level Objective

SME Small or Medium sized Enterprise

SQO Service Qualitative Objective

WTO World Trade Organisation

5 Summary of this document

5.1 Purpose of this document

The purpose of this document is to ease the formulation of government and enterprise policies that facilitate the adoption and use of standards-based cloud computing services.

By following the guidance in this document, developers of policy can:

— leverage international standards in an appropriate fashion when developing policy;

— achieve greater global consistency in applicable laws, regulations and policies;

— reduce costs for CSPs and CSCs;

— increase choice and competition;

— simplify the challenges of deploying and adopting cost effective local, multi-national, or global cloud services.

5.2 Intended audience

— Lawmakers (in both developed and developing countries) at every level;

— Regulators, including Data Protection Authorities (DPAs);

— Those developing enterprise policies including:

  — Cloud service customers (large and small) and prospective customers,

  — Cloud service providers,

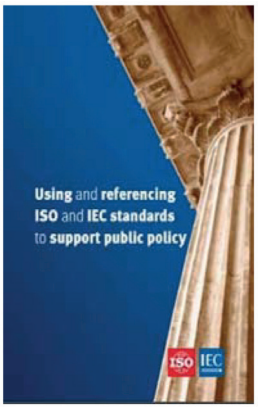
  — Cloud service partners;

— Those developing non-governmental rules and policies about trust and transparency for cloud computing, such as trade bodies and engineering institutions;

— Organisations that provide advice to governments and enterprises on the economic and political implications of technology policies, e.g. the Organisation for Economic Co-operation and Development (OECD).

In particular, this document is intended to assist those in smaller administrations such as local government, developing countries and those lacking in specialist knowledge on these topics.

5.3 How to use this document



This document provides guidance on which specific international standards might be applicable for policies on cloud computing and provides guidance on how they can best be employed. As such this document should be used in accordance with the overall ISO/IEC advice in this area as follows:

"The International Standards developed by the IEC and ISO are voluntary. And while they do not seek to establish, drive or motivate public policy, regulations, or social or political agendas, they can certainly provide valuable support to the implementation of public policy."

This statement comes from the publication "**ISO/IEC: Using and referencing ISO and IEC standards to support public policy**", which is publicly available and can be found at: https://www.iso.org/iso/PUB100358.pdf

Please refer to this ISO/IEC publication for general advice on how international standards can be incorporated in the public policy process and, by extension, in the development of cloud computing procurement policies for both public and private organisations.

6 Understanding cloud computing aspects for policy development

6.1 Introduction

This clause provides an explanation of some key characteristics and implications of cloud computing where an understanding is desirable by those developing public or corporate policy for cloud services. The intent is to present this material in a readable and approachable manner for those who are not full-time cloud computing engineers, while providing references to more technical material which can be considered when appropriate.

6.2 Cloud computing essential characteristics

6.2.1 Standard definition of cloud computing

The definition for cloud computing (3.1) captures several essential characteristics that differ from traditional, local, or hosted computing. These characteristics are further explained in ISO/IEC 17788 and will be described in even greater detail in the forthcoming ISO/IEC 22123[1)].

Effectively, this definition says that cloud computing involves the provision of almost any ICT resource as a service (a *cloud service*) over the network, and that this provision can be done dynamically on-demand at the CSC's request, much like the way utilities, such as telecommunications, are provided. Customers use what they need when they need it, and consumption is billed accordingly. ICT resources can be accessed almost as simply as pressing a switch to turn on a light, and can be released almost as simply as pressing the switch again to turn the light off. The need for the CSC to perform the lengthy processes to acquire, install, configure, secure and operate hardware, software and applications is greatly reduced, if not entirely eliminated.

6.2.2 Essential characteristics of cloud computing (from ISO/IEC 17788)

Cloud computing has a series of essential characteristics, which are summarized in Table 1.

1) Under development. Current stage: 30.60.

Table 1 — Cloud computing essential characteristics

Characteristic	As seen in cloud computing
Broad network access	The cloud service can be accessed from an arbitrary location by a wide variety of device types including PCs and mobile devices of all kinds, connected in many ways, usually by the Internet but sometimes by private networks, such as a corporate internal network.
Measured service	Customers' use of the cloud service is measured, and they might be charged based on what they really use, much as electricity supply is often billed based on measured energy consumption. Reduced usage can therefore mean reduced cost.
Multi-tenancy	Multi-tenancy means the resources supplied by a cloud service are shared by multiple CSCs. Each tenant's use of the resources is isolated and inaccessible from all other tenants — so that CSCs are assured that their data and their use of applications cannot be seen by any other CSCs. This is comparable to the expectation that details in a bank account are not visible to other customers of the bank. Note that a single customer can sometimes have multiple, different tenancies with a given cloud service, e.g. where the activities of different departments in an organisation need to be kept isolated from each other. Note also that while a private cloud by definition has only a single CSC, that single customer might still choose to employ multiple tenants of their own for isolation purposes.
On-demand self-service	Generally, cloud services allow the customer to sign up, pay for, and make use of the service without needing to interact with a human customer service representative. Customers are generally also able to manage their service, or cancel it, again without requiring human intervention. There might be exceptional circumstances where interaction with a human operator is required, but these will be abnormal cases, not regular business practice.
Rapid elasticity and scalability	Cloud services are able to allocate resources dynamically to a particular workload as needed. This is sometimes described as scaling up (increasing the size of a single resource), or scaling out (allocating additional similar resources). The intent is that customers can expand and contract their use of the cloud service as dynamically as possible, often to cope with planned or unexpected increases or decreases in workload. For example, if a website hosted on a cloud service suddenly attracts a huge amount of interest, the website owner can order (and pay for) more computing power and bandwidth so their site isn't overloaded. Once the peak is past, the resources can be released and the cost reduced. Another important aspect of cloud service scalability is that the resources available can appear effectively unlimited to the customer. This is in contrast with traditional datacentres, where the number of servers, the amount of data storage capacity, the network bandwidth all typically have limits that can only be changed by installing more equipment.
Resource pooling	Cloud computing gains efficiency by sharing various resources between multiple tenants and workloads. As an example, in traditional computing, ten customers might be hosted on ten separate servers, even if each of them was only using half of each server's capacity. In a cloud computing environment, those ten customers could be automatically provisioned onto just five servers

To explore the inter-relationship between these six essential characteristics and the various implications of cloud computing identified in this document, see Annex A.

6.3 Major benefits of cloud computing

6.3.1 Benefits for cloud service customers (CSCs)

The benefits enjoyed by CSCs are summarized in Table 2.

Table 2 — Customer benefits of cloud computing

Benefit to customer	As seen in cloud computing
Low capital investment	A customer wishing to develop or run a new application no longer needs to provision their own IT equipment, nor the buildings and infrastructure needed to house and support it, and potentially does not need to acquire, install and operate much or all of the software stack for the application. The customer is able to pay a relatively small amount (i.e. no need to buy server equipment) while developing and/or deploying the new application, then gradually build up the amount of cloud server resources they use as the usage of the application and revenue stream increases.
Cost-effectiveness of cloud scale	CSPs are able to purchase at scale, meaning that servers and other resources are much cheaper when bought in huge quantities. These cost savings can be passed on to the individual customers. Also, the cost per server of running very large datacentres, in terms of manpower, energy and other costs, is much lower than in hundreds of small installations.
Use as needed	Cloud services allow customers to start small, then ramp up and down very quickly as needed. The customer can reduce their bills during “quiet” periods for their business, and increase capacity in readiness (or in response to) peak loads such as for seasonal shopping or unexpected popularity.
Competition	Cloud service prices are very competitive due to the dynamics of the market. Each new project has a choice of which CSP to use, and new start-ups continue to challenge the big operators with special features and innovations.
Security	At one time, security was seen as a concern with moving to use cloud services, but today it is seen as a significant strength. Security is no longer considered as a significant hurdle in adoption of cloud computing. There are several reasons for this. Firstly, reputable CSPs often have security teams working around the clock and around the world to keep their systems secure, up to date with security patches, and ahead of any emerging threats that can be identified. They are very quick to respond to incidents. Even large commercial enterprises and smaller governments will struggle to recruit and pay for an equivalent level of 24×7 security expertise on their own staffs. Secondly, one of the biggest threats to computer security is the “insider” attack, where someone with administrative or physical access is involved in the breach, perhaps a corrupt or disgruntled employee, but who would not have the same kind of access to an external cloud service. (See ITU-T X.1601).
Availability and Reliability	Many CSPs operate multiple datacentres in separate locations and this offers customers the opportunity for improved availability of their applications and data. Applications can be run in multiple datacentres, and data can be replicated between those datacentres, avoiding any single point of failure. If one datacentre is taken offline by some natural disaster or major failure, CSC access to applications and data can be switched instantly to another datacentre.
Advanced capabilities	It is increasingly the case that CSPs are making advanced capabilities available as off-the-shelf cloud services. Examples include AI systems, advanced Analytics, and Big Data services. Some of these services are pre-trained on vast datasets. CSCs might struggle to implement these advanced capabilities in-house, due to limited access to the skilled people and resources. It is often far more cost-effective to integrate these advanced cloud services into new applications built by the CSC.
Choice of cloud service deployment models	Cloud computing allows a CSC to choose the most appropriate deployment model to meet their requirements, including public, private, community and hybrid cloud service deployment models (see ISO/IEC 17788). For a private cloud deployment model, the CSP will be part of the CSC’s own organisation.
Easier compliance	Most public cloud CSPs obtain a variety of certifications for their cloud services. By taking advantage of these cloud services, a large part of the burden of obtaining certifications and ensuring compliance can be lifted from the CSCs. Also, CSPs often provide advice, guidance and support for their CSCs who are seeking to have their use of the cloud service comply with such things as privacy and data protection regulations in their jurisdiction.

6.3.2 Benefits for society

The benefits for the wider society that can flow from cloud computing are summarized in Table 3.

Table 3 — Benefits to society from cloud computing

Benefit to society	As seen in cloud computing
Energy efficiency	Large purpose-built datacentres can be far more energy efficient than many smaller ones. They can also be in places where power is more readily available at a lower cost, or where the power used is based on renewable energy. Some datacentres are even designed to operate on free-air cooling, which greatly reduces the energy requirement. In addition, CSPs are able to optimise their customer's workloads and data on to the minimum needed number of servers[a].
Robustness and Resilience	Connections to cloud services are robustly protected, and far less vulnerable to virus or other malware attacks. They are also often strong enough to withstand determined distributed denial of service (DDoS) attacks from hackers and botnets. Cloud service providers often offer geographic diversity, such that cloud services can continue even in the event of a major natural disaster disabling one of their datacentres. Further, because these systems generally use software to provide resilience across multiple physical machines, they do not require every computer to run reliably. For a large cloud service datacentre, there is no need to carefully tend every server. Rather, workloads can be moved without impact to the customer. The service remains resilient even if the individual servers are not. The failed equipment can then be reconditioned and reused or recycled as appropriate. The resilience of cloud services benefits society, because CSCs no longer depend on their own resources and skills to keep business processes running.
Lawful access	While customer privacy is important, society also needs to protect itself from bad actors. When data is stored in cloud services, rather than on local computers, there are additional measures to obtain properly authorised legal access to it for criminal investigations, anti-terrorism, and other government purposes. However, this is not a panacea, and both legal and engineering challenges remain. For example, a situation where data is stored in (and/or managed from) another jurisdiction might involve legal complications for investigators, such as requiring the use of a Mutual Legal Assistance Treaty (MLAT) to obtain the cooperation of appropriate authorities in the other jurisdiction. A related area is e-discovery during legal proceedings, for which international standards such as the ISO/IEC 27050 series of standards could be helpful.

[a] A small business moving to the cloud could reduce its energy consumption and carbon emissions by more than 90 %, by running its business applications in the cloud instead of running those same applications on its own infrastructure.

Source: Bibliography [39]

6.4 Implications for policy makers

6.4.1 Shared responsibilities

Due to the nature of cloud computing, where the CSC and the CSU have considerable control over the use of the cloud service, there are *shared responsibilities* to maintain the security, privacy, confidentiality, and integrity of the service. For example, CSCs remain responsible for following best practices in their use of the cloud service, such as in handling passwords or other credentials, in giving appropriate permissions to specific users, in the type of data they put into the cloud service, and in labelling content so that it can be treated correctly by the cloud service. Such practices determine the overall security, privacy, confidentiality and integrity of the service, but are beyond the control of the CSP alone.

The use of industry-defined codes of practice to guide both the CSP *and* the CSC in the operation and use of cloud services is widely held to be a valuable approach.