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/IEC 2019



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2019

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
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

© ISO/IEC 2019 – All rights reserved

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**

 © ISO/IEC 2019 – 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 2019 – 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 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.

© ISO/IEC 2019 – 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 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]

© ISO/IEC 2019 – All rights reserved

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

© ISO/IEC 2019 – All rights reserved