TECHNICAL REPORT

ISO/TR 22428-1

First edition
2020-09

Managing records in cloud computing environments —

Part 1: Issues and concerns

Gestion des documents d'activité dans les environnements d'informatique en nuage —

Partie 1: Enjeux et préoccupations

Reference number
ISO/TR 22428-1:2020(E)

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

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out by ISO technical committees. Each member body interested in a subject has the right to be represented on the relevant technical committee if such committee has been established. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electro-technical Commission (IEC) on all matters related to electro-technical standardization.

The procedures used to develop the present document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the various approval criteria needed for different types of ISO documents 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 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 listed in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is given for the purpose of information for users' convenience 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 on 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 Technical Committee ISO/TC 46, *Information and documentation*, Subcommittee SC 11, *Archives/records management*.

A list of all parts in the ISO 22428 series can be found on the ISO website.

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

A cloud service refers to capabilities offered via cloud computing where users can borrow, to use flexibly, physical or virtual resources which include software and platform, as well as computing infrastructure, such as data storage and computing servers. The cloud service offers benefits, such as dynamic scalability, enhanced organizational agility, resilience and cost reduction, enabling improved organizational competitiveness and efficiency. Cloud services are emerging as an essential aspect of information technology due to location-independent resource sharing, availability via the Internet and mobile devices, and the ability to deliver on-demand services and lower costs.

Currently, the explosive growth of digital content through mobile platforms and the Internet of things is driving organizations to move their computing systems and information assets to the cloud. As a result, a number of companies and government organizations have shifted their business systems to cloud services, and many other organizations are planning to adopt cloud services. In the near future, it is expected that most data will be processed and stored in cloud services.

Cloud services might prove to be an alternative for organizations that are reluctant to invest in establishing their own computer systems for digital records management. Cloud services can provide the software, hardware, and platform needed to implement a system for records at an affordable price. It is often not easy for an organization to implement a system for records that meets all the criteria set out in ISO 15489-1. If there is a cloud service that satisfies all the criteria set out in ISO 15489-1 and which is provided at a low price, organizations have good reasons to consider using the cloud service.

However, organizations can be reluctant to adopt cloud services for their records management due to unknown risks, safety and privacy concerns, and an absence of convincing use cases. While the advantages of cloud services are well-advertised, awareness of the risks and issues that should be taken into account in a records management context is often lacking.

Cloud services are based on the concept of borrowing computing resources provided by third parties. The functions, processes or architectures inside the cloud are not disclosed externally. Even if a customer agrees with a cloud service provider about their requirements, it is difficult to know in advance whether their requirements can be met. In particular, it can be very difficult for general-purpose cloud services to fully satisfy the requirements of the records management process. There are various types of cloud services according, each of which offers different capabilities. In order to apply a cloud service to the records management task, the customer could select a cloud service that is suitable for the characteristics of the records management. The customer also to understands the general characteristics of cloud services. Otherwise, there is a possibility that desired records management outcomes will not be able to be delivered after adopting a cloud service.

In addition, in the case of large cloud services, cloud systems can be distributed around the world transcending national borders. Users from various countries or regional communities can share a cloud service belonging to a particular country. These characteristics of the cloud can cause various conflicts and issues because the jurisdictional structure and social environment of the country where the cloud service provider belongs is different from those of the cloud users. As a result, cloud users can be faced with unexpected risks associated with immature legal and social agreements for cloud technology.

Therefore, when records managers introduce cloud services to records management, they should consider the legal and social aspects as well as the technical aspects in advance in order to prepare for potential risks. Records managers can provide cloud service providers with prerequisites for managing risks, specified in contracts to reduce the probability of risks coming to fruition. This document aims to provide guidelines for persons and organizations who are intend to adopt cloud services for records management.

Managing records in cloud computing environments —

Part 1: Issues and concerns

1 Scope

This document presents a model for cloud records management and outlines the risks and issues that are considered by records managers before adopting cloud services for records management. The model for cloud records management includes a stakeholder model, processes, metadata, architecture, and use cases. Risks and issues are classified into those originating from cloud services internally and those originating from cloud services externally. Internal risks are associated with cloud services, systems and stakeholders. External risks and issues can occur in the social and legal context in which cloud services operate.

The target audience of this document includes:

- records, information, knowledge, and governance professionals;
- cloud service architects;
- archivists using cloud services for managing records;
- developers of cloud-deployed records management software;
- ICT staff; and
- providers of cloud-based records management services.

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 30300, *Information and documentation — Management system for records — Core concepts and vocabulary*

ISO 13008, *Information and documentation — Digital records conversion and migration process*

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 30300, ISO 13008, 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 http://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

[SOURCE: ISO/IEC 17788:2014, 3.2.5]

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

3.2
cloud capability type
classification of the functionality provided by a cloud service to the cloud service customer, based on the nature of resources used

[SOURCE: ISO/IEC 17788:2014, 3.2.4]

3.3
cloud deployment model
ways in which *cloud computing* (3.1) can be organized based on the control and sharing of physical or virtual resources

[SOURCE: ISO/IEC 17788:2014, 3.2.7]

3.4
cloud records
digital records created, preserved or managed by a cloud service

3.5
cloud records management
records management entrusted to cloud service

3.6
cloud records management service customer
party that is in a business relationship with the records management service provider for the purpose of using cloud records management services

3.7
cloud records management service partner
party that is engaged in support of, or as auxiliary to, activities of either the *cloud records management service provider* (3.8) or the *cloud records management service customer* (3.6), or both

3.8
cloud records management service provider
party that makes *cloud records management* (3.5)services available

3.9
cloud service
one or more capabilities offered via *cloud computing* (3.1) invoked using a defined interface

[SOURCE: ISO/IEC 17788:2014, 3.2.8]

3.10
cloud service customer
party which is in a business relationship for the purpose of using *cloud services* (3.9)

[SOURCE: ISO/IEC 17788:2014, 3.2.11]

3.11
cloud SLA
cloud service level agreement
part of the cloud service agreement that includes cloud service level objectives and cloud service qualitative objectives for the covered cloud service(s)

[SOURCE: ISO/IEC 19086-1:2016, 3.4]

3.12
cloud service provider
party which makes *cloud services* (3.9) available

[SOURCE: ISO/IEC 17788:2014, 3.2.15]

3.13
IaaS
Infrastructure as a Service
cloud service category in which the *cloud capabilities type* (3.2) provided to the cloud service customer is of the infrastructure capabilities type

[SOURCE: ISO/IEC 17788:2014, 3.2.24]

3.14
multi-tenancy
allocation of physical or virtual resources such that multiple *tenants* (3.21) and their computations and data are isolated from and inaccessible to one another

[SOURCE: ISO/IEC 17788:2014, 3.2.27]

3.15
PaaS
Platform as a Service
cloud service category in which the *cloud capabilities type* (3.2) provided to the cloud service customer is of the platform capabilities type

[SOURCE: ISO/IEC 17788:2014, 3.2.30]

3.16
private cloud
cloud deployment model (3.3) where *cloud services* (3.9) are used exclusively by a single *cloud service customer* (3.10) and resources are controlled by that cloud service customer

[SOURCE: ISO/IEC 17788:2014, 3.2.32]

3.17
public cloud
cloud deployment model (3.3) where *cloud services* (3.9) are potentially available to any *cloud service customer* (3.10) and resources are controlled by the *cloud service provider* (3.12)

[SOURCE: ISO/IEC 17788:2014, 3.2.33]

3.18
SaaS
Software as a Service
cloud service category in which the *cloud capabilities type* (3.2) provided to the cloud service customer is of the application capabilities type

[SOURCE: ISO/IEC 17788:2014, 3.2.36]

3.19
SOA
Service Oriented Architecture
architectural style that supports service orientation and is a paradigm for building business solutions using IT

[SOURCE: ISO/IEC 18384-1:2016, 2.48; ISO/IEC TR 30102:2012]

3.20
SORMA
Service Oriented Records Management Architecture
reference architecture model for records management based on cloud services, which includes service components for supporting records management in the form of *SOA* (3.19)

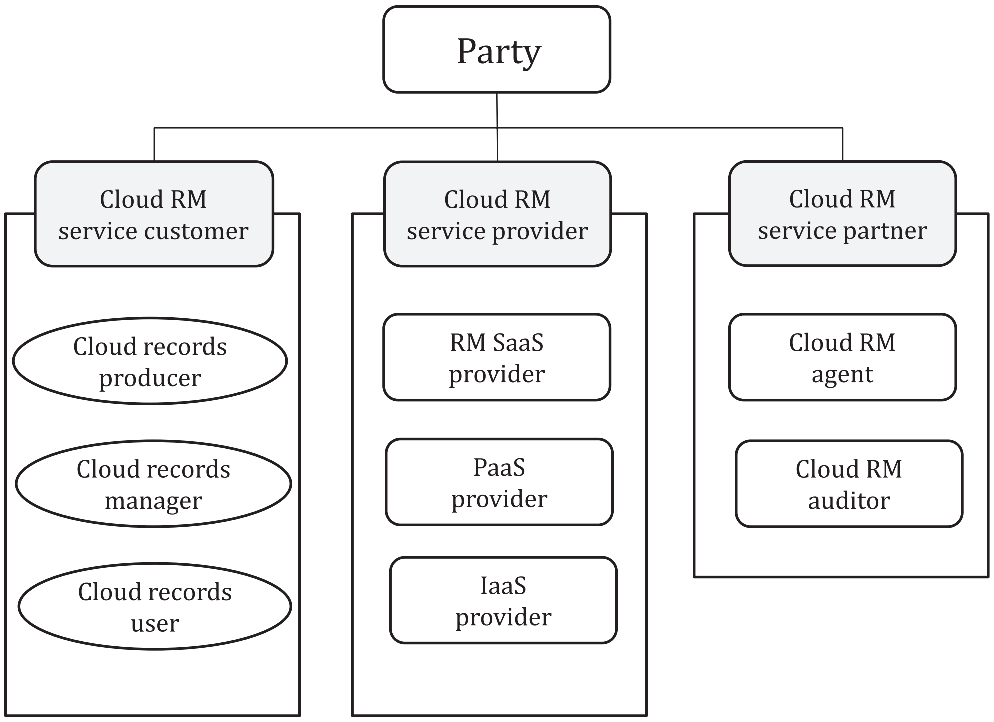
3.21
tenant
one or more cloud service users sharing access to a set of physical and virtual resources

[SOURCE: ISO/IEC 17788:2014, 3.2.37]

4 Stakeholder model

4.1 General

The cloud stakeholder model in this document is borrowed from the service model provided by ISO/IEC 17788, and extends it to the records management domain. A cloud records management service customer is a party that enters a business relationship with a cloud records management service provider for the purpose of using cloud records management services. A cloud records management service provider is a party that makes cloud records management services available. A cloud records management service partner is a party that is engaged in support of, or as auxiliary to, activities of either the cloud records management service provider or the cloud records management service customer, or both.



Key

▭ party

⬭ entity

Figure 1 — Cloud records management stakeholder model

4.2 Cloud records management service customer

4.2.1 General

Cloud records management service customers use cloud services to produce, transmit, maintain, and dispose of digital records and metadata. Customers strive to negotiate records management policies and procedures with cloud service providers on prior to entering the service contract. Customers can have cloud SLA contracts with cloud service providers to ensure confidence in the quality of records management.

Customers can be divided into several entities (individuals, teams, organizations) based on their records management role internally as follows:

— cloud records producer;

— cloud records manager;

— cloud records user.

4.2.2 Cloud records producer

Cloud records producers use cloud records management services to produce reliable records. This means that the cloud records producer ensures the authenticity, integrity, and reliability of the records by means of a cloud service. Cloud records producers inspect the records they write and verify that the records are stored in the cloud service without compromising their attributes.

When creating a record, cloud records producers are able to generate metadata that includes business context and verify that the metadata are generated without distortion. Cloud records producers is responsible for verifying that metadata are registered and preserved at a cloud service.

4.2.3 Cloud records manager

Cloud records managers have the responsibility of managing the records of their organization using cloud records management services. The cloud records manager leverages cloud services to perform administrative tasks such as registration and preservation of records, migration and conversion, search/query requests, verification of records integrity, and user authentication. The cloud records manager is expected to be familiar with the data management policies of the cloud service provider before using the cloud service, and consult with the cloud service provider if necessary.

The cloud records manager is responsible for reviewing the cloud service, ensuring that all requirements that arise from business and stakeholder expectations and the organization's regulatory environment can be met. The cloud records manager is responsible for inspecting the cloud service to see whether there are any constraints or problems in the functionalities by which records are created, registered, preserved, retrieved, browsed, and destructed.

When constraints are required for records management in the cloud, cloud records managers can establish records management policies and procedures for those constraints, and may make specific demands from cloud service providers as needed. For example, a cloud records manager may require a private cloud service provider to store records in a separate repository. The cloud records manager may ask the cloud service provider for access control policy on the records.

The cloud records manager manages access to records by setting the access level of each cloud records and specifying the access rights of cloud records users. The access rights of cloud records users are specified depending on their role, seniority, security clearance, location, etc.

The cloud records manager periodically monitors the registration and classification of records, their preservation status, and security mechanisms. Cloud records managers can maintain records stability and security quality beyond a certain level through the cloud SLA contract with a cloud service provider. In addition, the cloud records manager establishes a disaster recovery plan in advance with the cloud service provider in order to resolve any potential problem related to records within the cloud service.

4.2.4 Cloud records user

A cloud records user is an entity (such as an individual, team, or organization) that searches, accesses, or browses records through cloud services. Cloud records users are authenticated to cloud service providers before they use records. Cloud records users' authorization to access to cloud records is managed by the cloud records manager.

4.3 Cloud records management service provider

4.3.1 General

Cloud service providers are classified as IaaS providers, PaaS providers, and SaaS providers, depending on the capabilities they provide, and have the roles and responsibilities necessary to perform secure and reliable digital records management.

4.3.2 Records management SaaS provider

A records management SaaS provider is a party that provides application services for records management. Records management SaaS includes all functions required for records management. The records management SaaS provider makes public SaaS service quality that he can afford. Based on the quality of service, cloud customers contract cloud SLA with the cloud service provider, by which the provider is legally bound to keep the quality level specified in the cloud SLA.