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

Page

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.

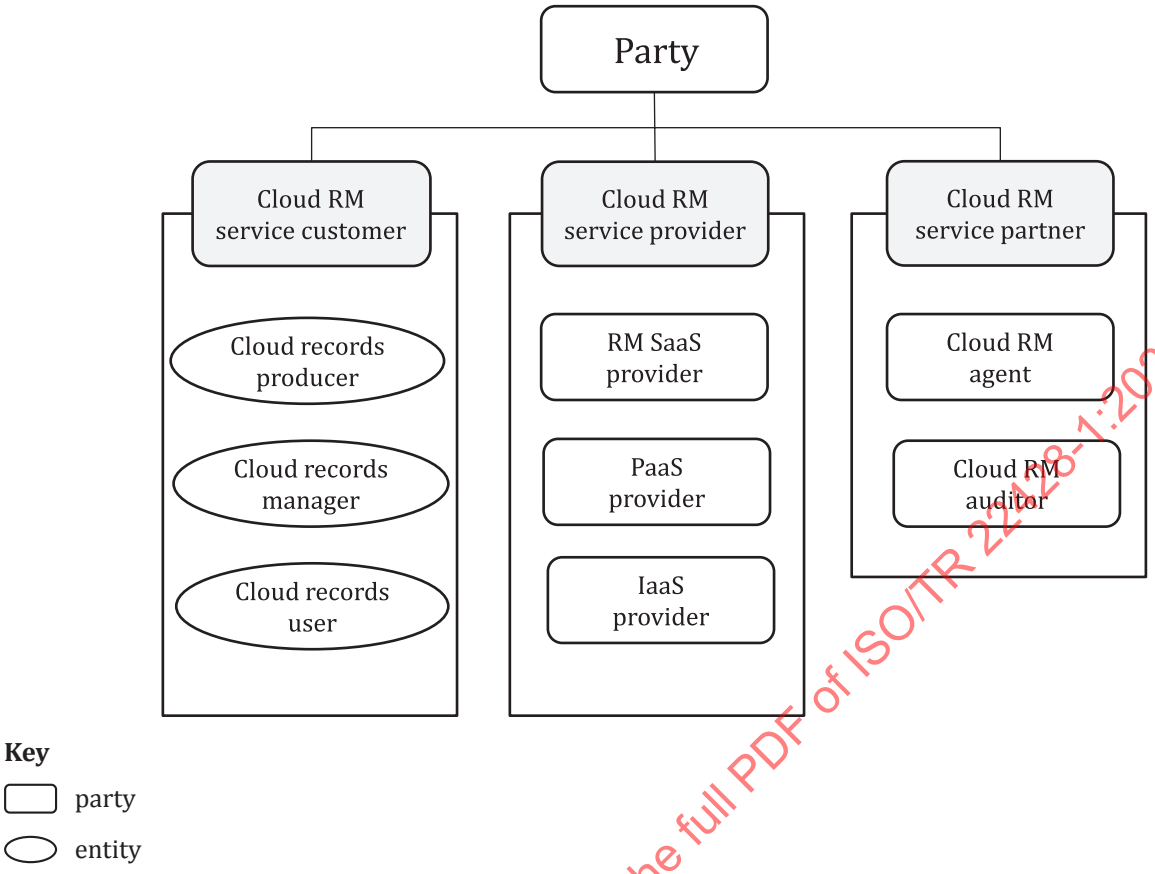

Figure 1 — Cloud records management stakeholder model

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.

The records management SaaS provider is familiar with the data management policies, data processing capabilities, as well as distributed processing, backup, and recovery mechanism of the IaaS and PaaS. The records management SaaS provider implements the records management service considering these factors. The records management SaaS provider clearly states in Terms of Service the limitations of the records management SaaS they are offering due to the constraints of PaaS or IaaS. Records management SaaS providers can contract the cloud SLA with PaaS providers or IaaS providers.

4.3.3 PaaS provider

One of the key roles of a PaaS provider is to provide a platform for developing and running records management SaaS in a secure and reliable manner. SaaS providers can develop SaaS services based on PaaS service, and a customer could use PaaS to develop directly his own applications. SaaS providers enter the cloud SLA contract with PaaS service providers to obtain stable and superior platform services.

4.3.4 IaaS provider

IaaS providers provide hardware such as data storages, servers, and networks in the form of services. For records management, IaaS providers need to provide reliable storage to keep records even if they use storage virtualization. Digital records and their metadata are stored stably and securely in IaaS storage. IaaS providers who are specialized in records management may develop and provide functions for records management, such as long-term preservation or record registration, to customers.

4.4 Cloud records management service partner

4.4.1 Cloud records management agent

A cloud records management agent is an entity that is contracted by a customer to procure a cloud service and manage records stored in the cloud service on behalf of the customer. The cloud records management agent can perform tasks such as selecting the appropriate cloud capability or cloud records management service, and contract with a cloud service provider. The cloud records management agent ought to be familiar with the characteristics of digital records management and cloud services. The cloud records management agent needs the knowledge and experience to perform digital records management services in the cloud environment. The cloud records management agent acts as follows:

— The cloud records management agent, who has delegated records management authority from the customer, stores the customer-generated record in the cloud systems, and manages the stored record on customer's behalf.

— If a cloud records management agent is delegated legal authority from a customer, the cloud records management agent acts as a legal representative for legal disputes arising from issues related to cloud records management.

4.4.2 Cloud records management auditor

A cloud records management auditor may be internal or external to the customer's organization. Their role is to audit the organization's digital records management processes within the cloud records management service environment with specified standards. The cloud records management auditor evaluates whether the cloud service is being provided in accordance with the cloud digital record contract. The cloud records management auditors need especially audit service quality whether they are afforded as specified in the cloud SLA.

Another role of the cloud records management auditor is to conduct an examination and evaluation when the cloud records management service is closed. At the time, the auditor needs to be able to confirm that all records and metadata have been migrated out of a system and that the source records

or "trace" of the record has gone from the service providers system. In addition, the following items are audited regarding cloud services:

— procedures for digital records creation and management;

— procedures for sending and receiving digital records;

— security, availability, stability, performance;

— different types of cloud records management services and billing systems;

— long-term preservation plan;

— backup plan;

— migration plan;

— disaster measures;

— whether access control policies are being used appropriately;

— whether disposal is being undertaken as required;

— whether records are able to be located, retrieved, presented and interpreted;

— whether records are portable and can be managed during transition from one service arrangement to another.

5 Cloud records management environments

5.1 General

Cloud services may have both positive and negative effects on records management due to the intrinsic nature of cloud services. Negative effects (associated with risks and discussed in Clause 7) are mostly caused by the transfer of all or part of the records management control to the cloud service provider. In order to apply cloud services to records management, positive effects of cloud services should be maximized, and the negative effects of cloud services should be minimized. This clause presents considerations for processes, metadata and architecture for cloud-based records management services to minimize the potential negative impacts from adopting cloud services for records management.

5.2 Records management processes in the cloud environment

The cloud service provider provides services supporting to all or part processes for records, from records creation to disposition of records. Customers leverage cloud services to manage records directly, or may entrust whole records management to cloud service providers. Customers and cloud service providers may consider the following in the cloud-based records management process.

— Creating/Capturing records: Customers need to use SaaS to create or capture their own records and preserve them in cloud storages. Records created or captured in SaaS are transferred to the cloud server via the open network, which exposes them to the risk of record integrity or authenticity. Therefore, the data transport protocol is confidential and reliable, and ensures the integrity of the record. Customers also use SaaS to store records in cloud services, which reliably stores the records and metadata for the records in the cloud storage. The link data between a record and its metadata are stored safely and not lost in the cloud storage. Multiple customers share SaaS through a multi-tenancy mechanism. Therefore, SaaS service providers clearly present access control methods and ownership of records and metadata created by each customer. SaaS service providers need to understand the computing resource management policies of PaaS service providers or IaaS service providers and inform customers of SaaS quality level. Role and responsibility associated with record generation, access control and ownership, and the service quality level may be specified in an agreement between a customer and a SaaS service provider.

— Classification and indexing: When a customer requests a classification for records to a cloud service provider, the cloud service provider provides this classification service. If the customer provides records and contextual data, the cloud service provider index the records in the classification with the contextual data. Records once indexed might need to be reclassified at the customer's request, in which case the cloud service provider reclassifies the records with modifying metadata.

— Access control: The cloud service providers need to establish principles for the authority to access, conditions and restrictions regarding the stored records, and provide the customer with search tools for metadata and classification category. Customers can browse only their own records or records that they are allowed to access. Technical measures to prevent illegal copying, leaks, falsification, etc., are taken when allowing browsing by a customer.

— Storing records: In cloud services, records are stored in the form of several copies for easy availability, where management and tracking of each copy is essential. This can cause conflict if they differ from the customer's requirements. Cloud service providers and customers agree on the applicable data management policies. The cloud service has in place a process and storage for the stable preservation of the records and prevent loss of the records due to disaster, system failure, etc. In addition, when a customer requests long-term retention of a record, the cloud service provider has the long-term management policy and long-term stable storages.

— Use and reuse: As long as records are kept in a cloud service, they are useable. Cloud service providers can manage records metadata and metadata for cloud systems to maintain records usability. The records are convertible to alternative formats available at customers desire. In addition, cloud service providers need a plan to ensure continued access and usability of records in the event of a disaster.

— Migration: At the request of a customer, records can be migrated from a cloud service to another or from a cloud service to a customer's server. For the migration of cloud records, an agreement on migration schedules, storage file types, data transfer protocols, security, transfer file types, and integrity verification methods are preceded. After the migration, there is a process for ensuring the integrity of the records and metadata contents and structure. If an error is detected in the process, the cloud service provider informs the customer of the error and clears the error. The records migrated are completely disposed in cloud servers, and the cloud service provider needs to notify the customer of the results of the disposition.

— Disposition: Records stored in a cloud service are disposed of either at the request of the customer or when the retention period specified in the contract expires. Cloud service providers may ask the customer to extend the retention period before the records are automatically disposed at the end of the retention period. The cloud service provider controls disposition processes and destroys records and associated metadata. The cloud service provider has the capabilities to dispose of all distributed copies of records.

— Audit trail: Activities performed by cloud service customers or cloud service providers are recorded in audit trails. Audit trails are protected against unauthorized loss or alteration. They are available upon request for agents who are authorized to do so.

5.3 Metadata in cloud records management services

To ensure the authenticity of records stored in the cloud, the records' metadata need to be reliably managed. In the cloud records management environment, metadata can be classified as: 1) records metadata and 2) system metadata generated by cloud services. The records metadata could be generated by a customer, either through a SaaS application or a customer-owned software. The customer remains responsible for the integrity of the records metadata. The system metadata are needed to manage records and operate in cloud systems.

Most of system metadata are automatically generated in the cloud system, but the cloud service provider may generate them partly by referring to the records metadata. Such metadata can be used as an audit

trail for records management or as evidence to verify the integrity and authenticity of records. The following are the metadata items that could be used for records management by cloud capability type:

— Metadata for SaaS: Tenant ID, User ID, Terms of use, role, and responsibility of the cloud records management service provider, etc.

— Metadata for PaaS: Name and version of execution platform, name and version of the service development platform, API version, name of the application used for continuous integration and continuous development, etc.

— Metadata for IaaS: OS name and version, storage type, container type; Network type, number of record copies; file system name, type and version of hypervisor, etc.

The records metadata are available at any time at the customer's request. However, system metadata may be proprietary to the cloud service provider and may not have to be provided to customers. This could be an issue in situations where there is no prior agreement on ownership of the system between the customer and the cloud service provider. The cloud service provider makes this clear at the time of contracting the obligations to provide metadata and its ownership, depending on the type of metadata. Figure 1 shows the relationship between records metadata and system metadata generated in cloud services.

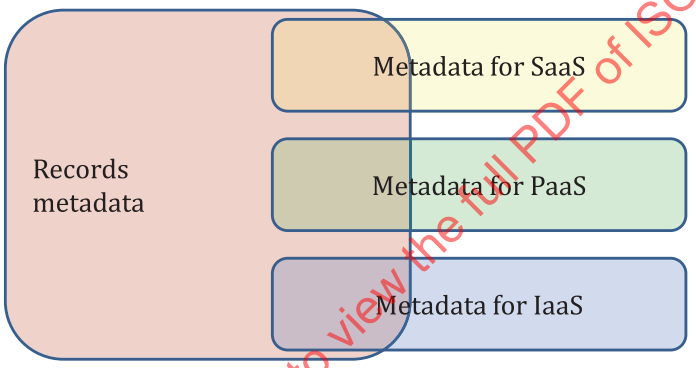

Figure 2 — Records metadata on cloud services

5.4 Cloud reference architecture for managing authoritative records

Cloud services are classified into IaaS, PaaS, and SaaS depending on the capabilities of the computing resources they provide. IaaS are services that provide flexible computing infrastructures to a number of customers by virtualized physical server (CPU, Memory, Operating System [OS], storage, and network). PaaS provide on demand the underlying functions and capabilities needed for the development and deployment of SaaS. PaaS are likely to be generic, and not specific to the records management function. SaaS are applications in the form of service.

The IaaS is sustainable enough and prepare for any form of incident for the reliable and secure storage of records. The IaaS for records management also provides functions related to preservation and disposition of stored records as well as backup and recovery services. The SaaS for records management has the functions necessary to acquire, preserve, search, and browse records.

Cloud computing essentially has a service-oriented architecture, which means that cloud records management services are delivered on a modular basis of self-contained business activities with specified outcomes, and whose detailed workings are opaque to the cloud service customer. It would be helpful to have a reference standard for cloud records management services that organization scan refer to when performing records management through cloud services. This document provides a cloud-based records management service reference model to the services of the trust-based third-party records management repository standard defined in ISO 17068. This reference model is called Service

Oriented Records Management Architecture (SORMA), a term formed by combining SOA and records management. The following are descriptions of the service hierarchy that SORMA includes.

— SORMA SaaS service is composed of services that constitute the digital records management application used by customers, and includes services such as acquisition, registration, classification, conversion, preservation, and disposition.

— SORMA PaaS is a service that provides capabilities necessary to implement and run a records management SaaS such as an application development platform, application management and execution, and IaaS control and interface.

— SORMA IaaS service is a layer that provides storage, network, and computing services.

MoReq 2010 describes SOA-based modules for records management. MoReq 2010 presents service modules required for general records management, which have granularity of class-level so that they can be easily referenced in implementation. SORMA presents records management service units of each cloud capability type.

SaaS may be developed on a local server or IaaS, but mostly SaaS are developed on PaaS because PaaS maximize the performance of SaaS. Recently, there are many cases where it seems that the PaaS are excluded from the cloud architecture because most IaaS providers often provide PaaS services together. However, the PaaS functionality has not disappeared, and the PaaS functionality is more internalized in IaaS. In this respect, Figure 2 below shows the structure of SaaS service depending on the PaaS and based on the IaaS, within the SORMA architecture.

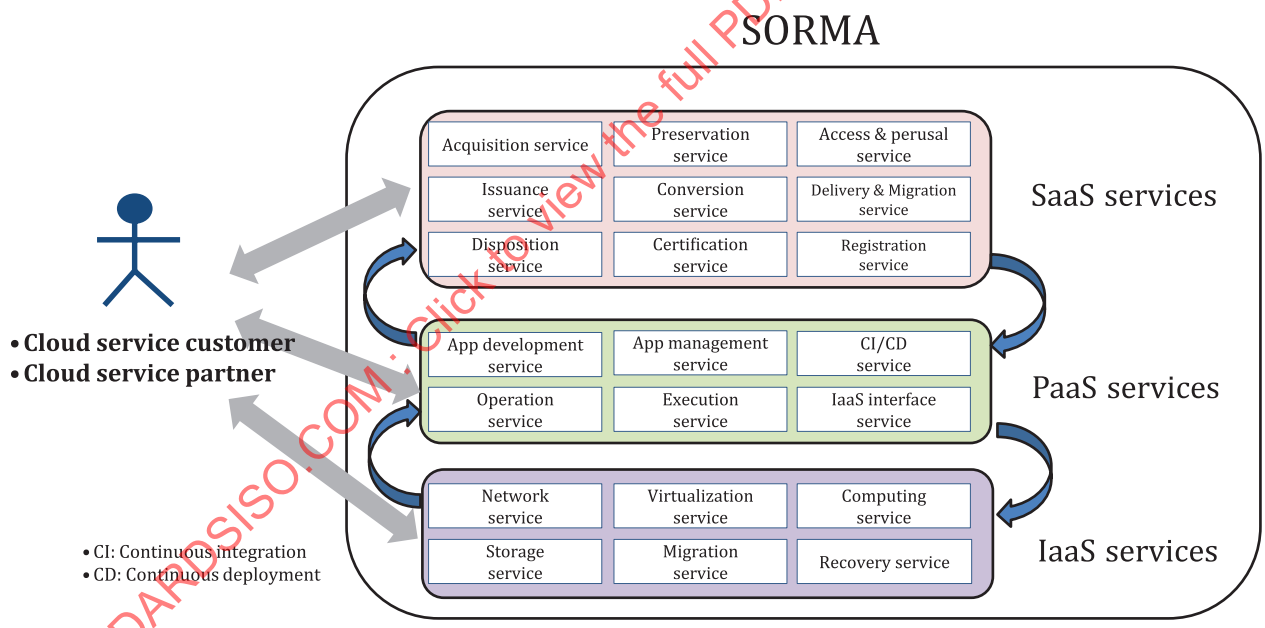

Figure 3 — Reference architecture for records management in the Cloud

6 Use cases in cloud records management

6.1 General

Customers may borrow partly or totally the cloud capabilities according to their requirements, or develop their own records system using cloud services. Therefore, there are various use cases for records management on cloud services. This clause presents the risks and issues related to cloud-based records management use cases.

6.2 SaaS shared by customers

This use case happens when the cloud records managers in an organization use SaaS for records management task. The records management SaaS are provided in the form of web-based software, and the service interface and configuration could be partially adjusted according to the customer's requirement.

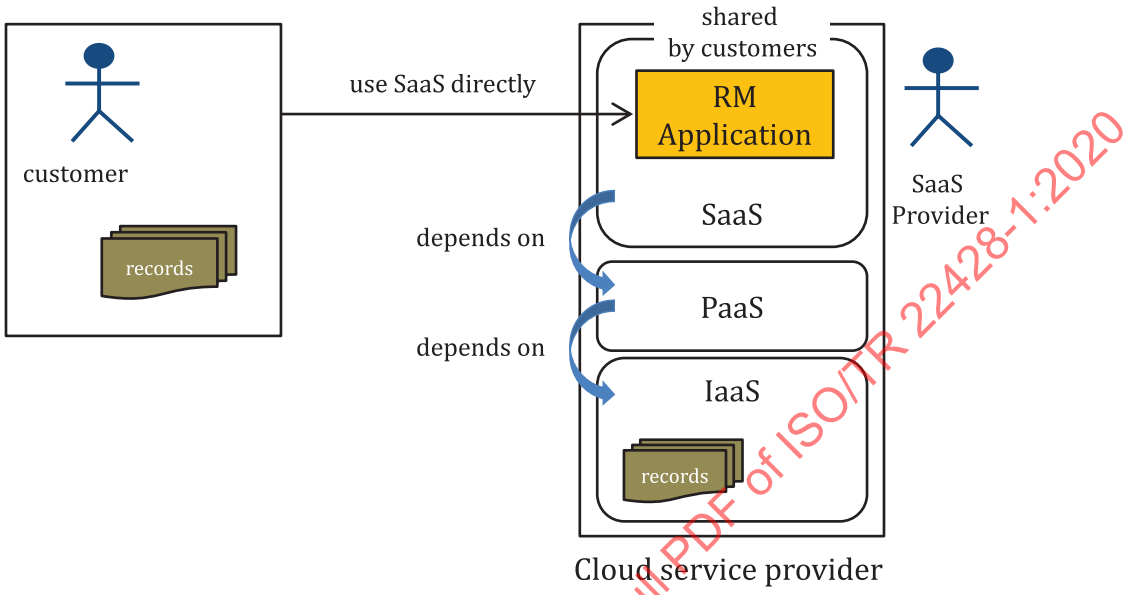

Figure 4 — Records management SaaS shared by customers

Customers pay for SaaS usage in accordance with the billing scheme established by the SaaS service provider. As SaaS are managed by the service provider, the records manager only needs to focus on records management and monitor the quality of service.

Customers can sometimes require customization to SaaS, but it can be very difficult for service providers to accommodate such requests adequately. Even though SaaS have multi-tenancy features, in most cases they offer only minimal customization of the user interface. Thus, the customers have a difficulty to configure optimal records management options that meet the needs of the organization or the business situation.

Customers who require long-term retention periods for their records concern the business continuity of SaaS service provider. Therefore, the customers may consider exit arrangements and migration plans, and the potential costs and resource if necessary.

Customers need to review whether SaaS has been implemented on reliable PaaS or IaaS. Customers may also consider whether the SaaS service provider will take overall responsibility as a service representative, when a failure occurs in PaaS or IaaS, as well as SaaS.

SaaS is based on a multi-tenancy mechanism where multiple customers can share a single application service. Multi-tenancy mechanisms may inadvertently expose information from other customers. For example, the data entry function of the web interface recommends automatically data input previously. The statistics package in SaaS can easily show the word that users search the most or input/output data category information. Therefore, when implementing the multi-tenancy feature of SaaS, special care is taken to ensure the privacy of each customer.

6.3 SaaS developed by customers

In this use case, customers develop their own records management application as a service using PaaS. The developed records management application is used as if it were an exclusive application of a customer. This approach occurs in the following situations:

— there is no SaaS that can meet the customer's specific requirements;

— existing records management SaaS cannot accommodate a huge number of records management transactions;

— the customer does not want to share records management applications.

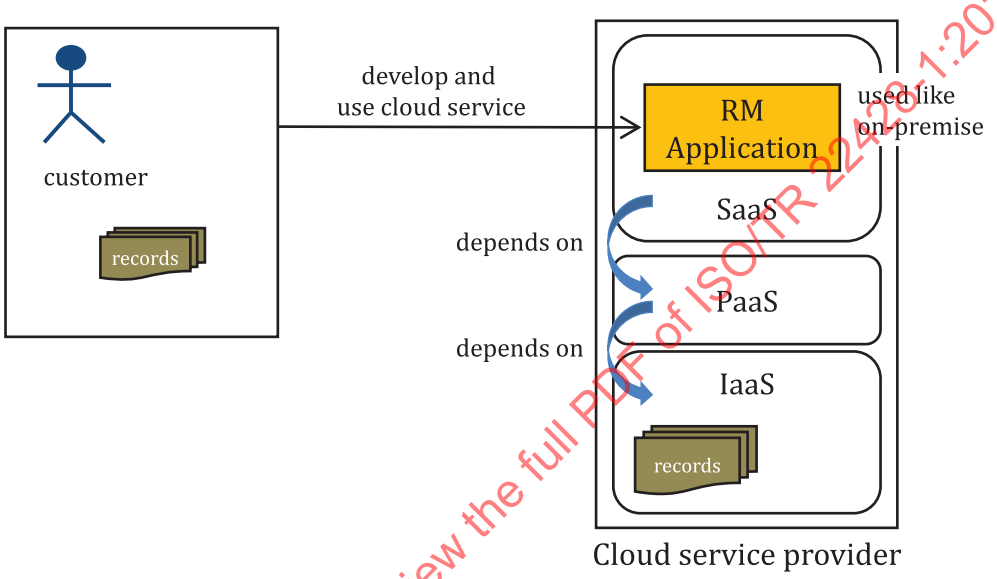

Figure 5 — SaaS application developed by a customer

In this use case, the customer develops a records management application that meet specific requirements. The records management application developed in this use case reflects the customer's records policy and the technical and economic situation. Since the records management application developed in this use case is not shared among customers, it is advantageous in terms of security and privacy.

However, this approach is possible when the customer has the cost and ability to develop a cloud-based records system. Although the use of PaaS reduces the costs of the development environment, the development process will require additional costs for cloud software professionals.

6.4 Records management based on IaaS

In this use case, customers develop records management application using IaaS storage service. The IaaS provide customers with hardware information or APIs necessary for hardware utilization. The customer's records management application implements a management process, and the records retention is implemented in IaaS as shown in Figure 6.

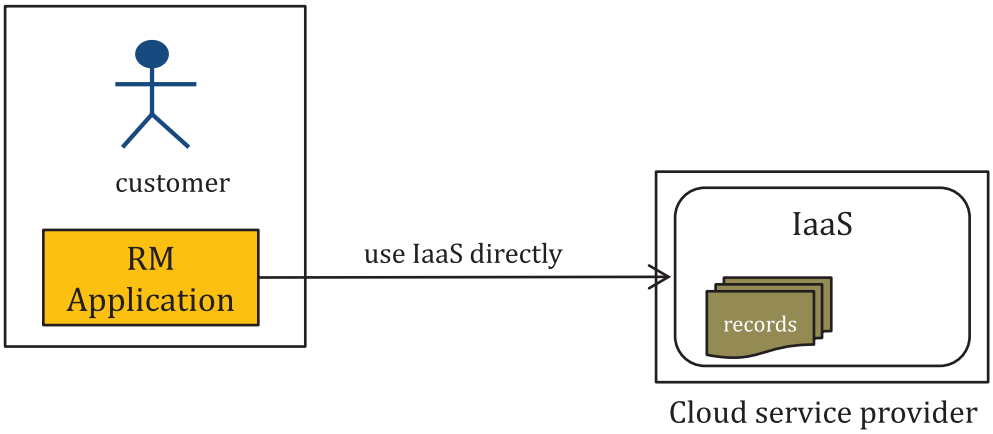

Figure 6 — IaaS used directly by a customer

The primary advantage of this approach is that customers can use the storage for records inexpensively. It is also easier for customers to progressively migrate their records system into a cloud service over time.

In this use case, the records management application interfaces directly with the IaaS provision in order to access storage; this requires control and management of the IaaS resources in detail, which may be very tricky. The IaaS service provider's backup methodology, backup cycle, retention and deletion policies are correctly aligned with those required by the records management application.

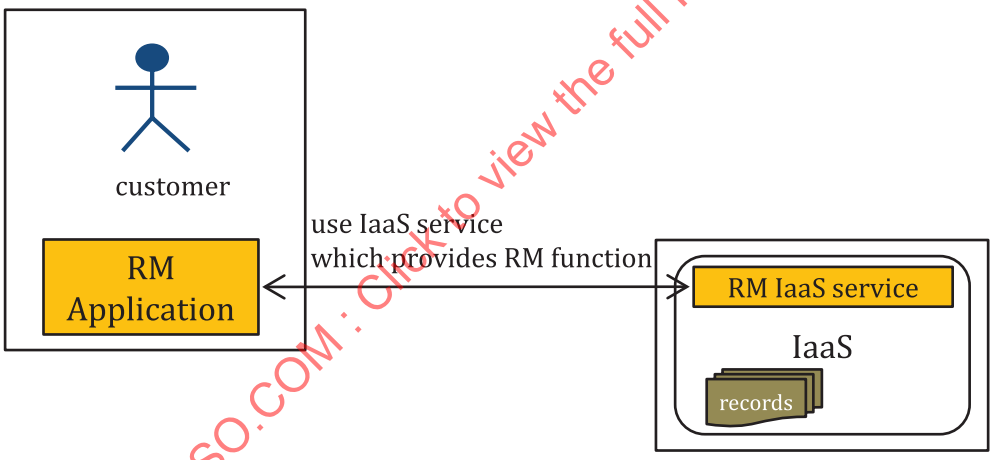

Figure 7 — IaaS with records management functionalities

Some IaaS are designed specifically for records management and include features to support long-term records preservation and records disposition, making it easier to implement records systems as shown in Figure 7. However, these features often incur a higher license fee that non-specialized IaaS services.

6.5 Multiple IaaS used by customers

In this use case, one customer's system for records uses two or more IaaS services to ensure the stable storage and availability of records as shown in Figure 8. The primary advantage of this approach is that customers ensure the continuity of their records, even if one of IaaS providers ceases business. The disadvantage is that significant technical effort is required to maintain consistency between the versions stored in each IaaS. Furthermore, the cost of this approach is inevitably higher than that of using a single IaaS service.

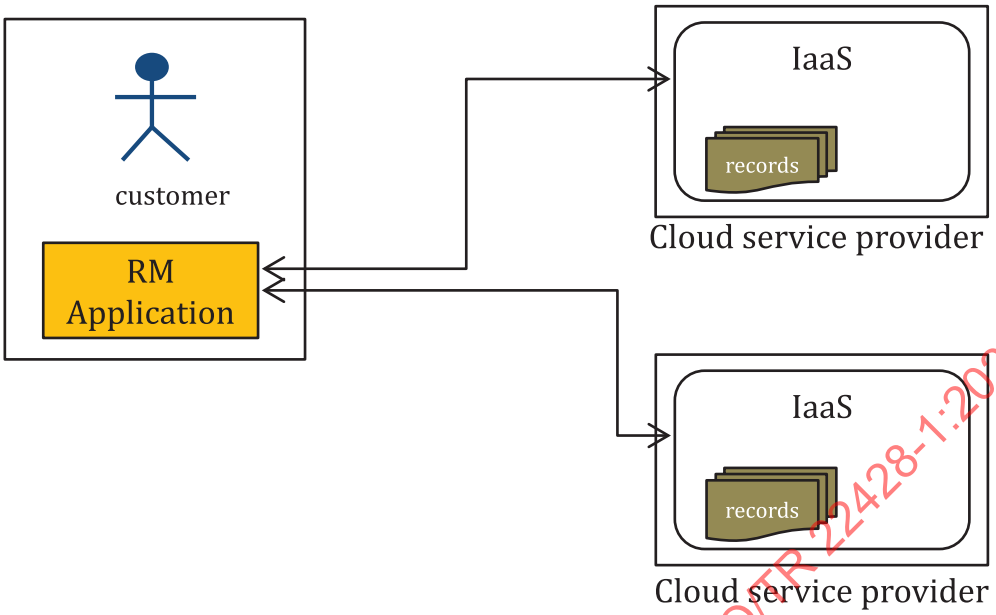

Figure 8 — Multiple IaaS used

6.6 Records management agent

If customers are not able to use cloud services, they may outsource their digital records management tasks to a third-party RM agent rather than to a cloud service provider. The records management agent is an expert on the area of digital records keeping and cloud services. The records management agent acts as an intermediary between the cloud service provider and the customer as shown in Figure 9. Typically, the records management agent contracts cloud SLA agreement with the cloud service provider on behalf of the customer. This approach allows customers who have difficulty in use cloud services to use them for records management. However, the cost of engaging a records management agent is added to the normal costs of cloud services.

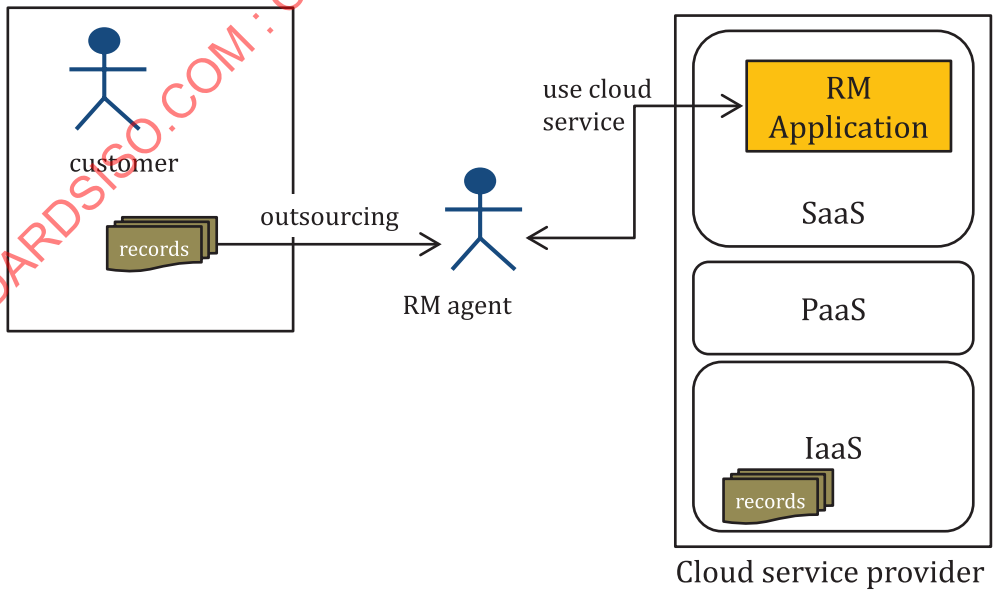

Figure 9 — Records management agent using SaaS

Records management agents may develop their own records management applications in order to provide cloud records management services to customers as shown in Figure 10. This usually occurs

where the customer's records management requirements are not normal and so generic cloud records management services cannot meet the requirements, or where the RM agent has a business model that requires the use of its own software. In this use case, records management agents can develop records management applications using cloud services and perform records management tasks commissioned by customers.

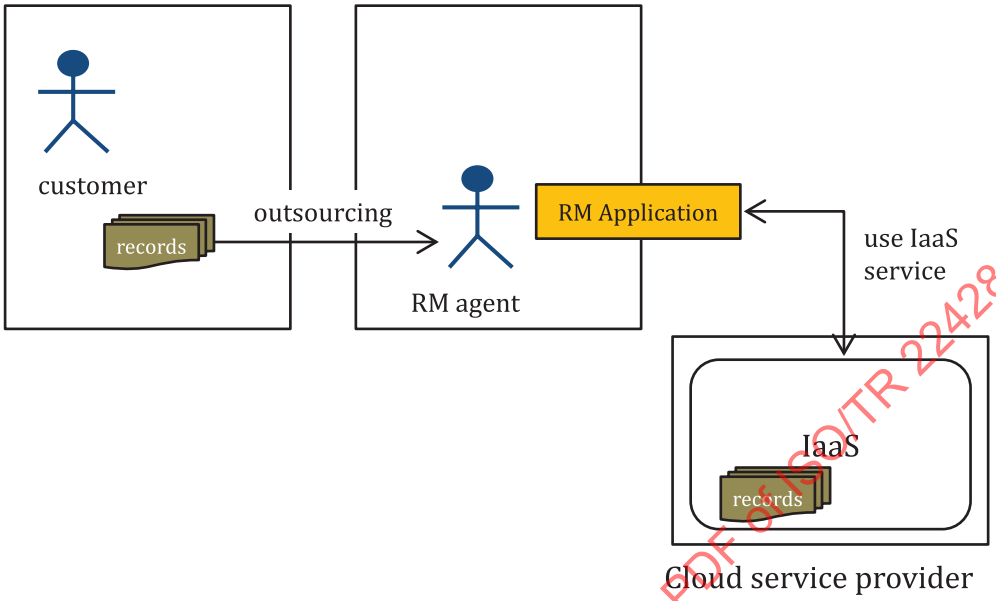

Figure 10 — Records management agent using IaaS

7 Risks in cloud records system

7.1 General

As shown in Clause 6, cloud-based records management is performed using various cloud capabilities through an open network, which could lead to unexpected risks in records management. These risks are divided into risks arising from the inherent nature of cloud services, risks resulting from the cloud system, and risks caused by stakeholders. Customers need to be aware of these risks in advance and ensure that the cloud service provider can take measures against these risks. This clause presents risks in type and suggests briefly check points to prepare.

7.2 Cloud service risks

Records management using cloud services presents several potential risks due to the SOA nature of cloud computing. The table below lists the typical attributes of cloud computing and summarizes the associated risks.

Table 1 — Potential risks for records management associated with cloud services

Cloud service attributes	Description	Potential risks for RM
Service-oriented	All computing resources are provided in the form of services by cloud service providers.	The cloud service providers unilaterally determine the policy of computing resource management. Conflicts may arise if the policy of the cloud service provider is inconsistent with the customer's records management policy.
Flexible	Servers, networks, and storage can be arranged by virtualization to enable customers to respond more aggressively to changing business situations.	The integrity of a record requires stable storage for as long as the record is required to be maintained. The configuration of virtual servers used in cloud computing changes frequently in order to provide elasticity of service provision on demand. These frequent changes may result in unintended consequences such as unexpected alterations to configuration of record stores, metadata or security controls
Provisional	The ability to procure the resources needed for cloud computing with rapidity and agility.	In cloud computing, the resources needed by tenants are procured as needed and released when no longer required. This causes problems related to the stability of records systems, due to the unexpected growth or unplanned configuration of new services or storage resources.
Open	With the exception of the private cloud, cloud services are accessible to the public.	In public cloud services, customers share software and hardware. This potentially increases the likelihood of privacy breaches or other security leaks due to error or intent, but this risk is substantially mitigated by the additional security resources contributed by cloud providers, which in most cases result in security provisions which are significantly enhanced compared to the network security put in place by most small/medium organisations
Opacity	The internal workings of the cloud service are hidden from the customer.	The cloud records management software may not perform as expected by customers. If there is a problem with the cloud service, there is nothing the customer can do about it.
Commoditisation	The customer cannot normally customise records management tools provided on a SaaS basis.	The cloud service provider simply delivers the service "as-is" on the same basis to all customers of a given classification and functionalities.
Lock-in	The customer's business software is dependent on the cloud service totally, making it impossible to move to another cloud.	Records migration between cloud services is both difficult and expensive; the cloud service provider's contractual terms may also increase costs of exit.

Cloud service technology is changing rapidly, and at present, there are many standards and products. There is always the possibility that business continuity could be affected by changes in cloud technology, changes in cloud service providers, or changes in standards. In other words, cloud services are liable to constant change. Provisioning, which quickly arranges computing resources according to the customers' demand in the cloud service, is one of the most important advantages of the cloud service. However, provisioning could make stable and long-term digital record keeping difficult, and may compromise the reliability of records.

Customers can carefully review the following points at the stage of contracting with the cloud service provider to minimize the damage caused by the risks in cloud services.

— In the event of a service issue, are the responsibilities of the cloud records management service provider clearly defined?

— How does the cloud service provider ensure tenant privacy and data confidentiality despite SaaS service sharing?

— How does the cloud service provider ensure virtual or physical independence such that records and related metadata can be stored reliably and unhindered by storage or network changes due to virtualization or provisioning?

— Does the cloud service provider have a policy for ensuring consistency in copies of records?

— How does the cloud service provider guarantee complete disposal of all copies and versions of a record at the time of disposition?

— Does the cloud service provider have a service governance?

— Is there a way to prevent the cloud service provider from unlawfully or inappropriately deleting or destroying records without the customer's approval?

— Can the cloud service provider return records in any case at the request of a customer under a contract? Can the cloud service provider also return records in the format requested by the customer?

— Can records be returned to customers even if the cloud service provider goes out of business?

7.3 Cloud system risks

Cloud computing is based on three basic mechanisms for delivering services reliably and inexpensively to customers: multi-tenancy, hardware virtualization, and file distribution. Multi-tenancy is a mechanism by which multiple customers share an application or platform. Hardware virtualization is a mechanism that virtualizes hardware resources so that they can be flexibly used as needed. Typical examples include server virtualization, storage virtualization, and network virtualization. File distribution is a mechanism for distributing copies of a file across multiple servers or storage systems to improve file availability and easy recovery. This clause presents the risks arising from these three primary cloud mechanisms and security risks.

In public cloud service, a customer's records and other data are logically segregated from those of other customers, but they share the same hardware and software. This multi-tenancy mechanism potentially increases the likelihood of privacy breaches or other security leaks due to error or intent, but this risk is substantially mitigated by the additional security resources contributed by cloud providers, which in most cases result in security provisions that are significantly enhanced compared to the network security put in place by most small/medium organisations. There may also be some potential for information leakage where the service provider is required to provide performance or system metadata to a customer or regulator in relation to the operation of their service, but this high-level performance and activity data are unlikely to prove sensitive for most organisations.

The integrity of a record requires stable storage for as long as the record is required to be maintained. The configuration of virtualized servers and storage used in cloud computing changes frequently in order to provide elasticity of service provision on demand. These frequent changes may result in unintended consequences such as unexpected alterations to configuration of record stores, metadata or security controls. The flexibility that allows users to massively increase their processing power or storage makes it easy to misconfigure such expansions so that records management policies and workflows are not properly applied to entire areas of the organization's virtual network or storage. Properly managing the virtual resources of cloud computing can be a significant overhead.

The file distribution mechanism can make it difficult to maintain consistency and ensure the disposal of stored records that are distributed randomly. Copies of records that are stored on different systems may have the same content, but different system metadata. The cloud system is able to manage these copies as the same record. When changes to records are made (such as conversion), the cloud system makes the same changes to the copies of the records and then also reflect the changes in system metadata. Consistent management of the system metadata for the copy of the cloud record ensures the authenticity of the record, even if there are copies of the record in the cloud. Upon request by the

customer to destroy the record, the cloud service provider destroys the record and its associated copies. However, if the cloud service provider has his own file disposition policy, complete disposition of records may be difficult. If there is a request to migrate records in the same cloud service or to another cloud service, the cloud service provider checks the records metadata, determines the records to be migrated, and then performs the transfer. All copies of the records that remained on the cloud server prior to migration need to be completely destroyed.

The cloud computing paradigm delivers services via the Internet. As with all networked IT services, including those hosted on an organization's own premises, cloud services are potentially at risk from malicious thing such as viruses, hacking, or denial of service attacks. Most cloud service providers have security expertise and more security resources than their customers, and the risk posed to the records of the customer organization from such things may even be reduced by transferring them to a cloud records management service.

7.4 Cloud stakeholder risks

As with any IT network, the actions of all employees of both the customer and the cloud service provider may lead to risks to the records stored in cloud services. Unauthorised or unqualified users may accidentally or deliberately access, modify, copy, or erase records, and those with hostile intent might be able to enact fraud or theft, or insert malicious software.

Before purchasing cloud records management services, the potential customers need to ensure themselves that the cloud service provider has put in place adequate authentication processes to ensure that access to records is only granted to a legitimate user. These processes include a method for the customer to issue authenticated identities to their authorized users (e.g. login and password), and a method to restrict user rights by both record classification and by user security level. All actions undertaken by any user need to be recorded in appropriate audit trails.

It is potentially possible for an authorized user of a cloud computing system to make radical changes to its configuration with relative ease; for example, some cloud services allow the commissioning of hundreds of virtual servers with a few short instructions. Such changes may have a significant negative impact on the integrity of the system for cloud record and its records if unplanned or not carried out correctly. The customer need to ensure that users authorized to make such changes are properly trained, and control and monitoring options are available to detect and prevent hostile action against their cloud computing resources. The customer may also finds out assurances about the security and monitoring capabilities of a cloud service provider.

Cloud systems can change and control configuration information almost autonomously in many unusual situations. In exceptional circumstances however, a cloud service provider might terminate the cloud service that they offer. Occasionally, a user may intentionally or accidentally request an operation beyond the system's automatic control range. In this case, the user's faulty request may act as a major threat to the entire cloud system. Viruses, Ransomware or DDoS attacks, and security attacks can also pose a threat to cloud systems. In view of these risks, cloud service providers need to monitor the entire system in real time and be able to react quickly when problems arise.

The cloud service provider toned to ensure business continuity of the cloud services it provides. In exceptional circumstances, however, the cloud service provider may suddenly terminate the cloud service. In this case, it is possible to migrate the records kept in the cloud service to the customer or other cloud service without undermining the record's quality and integrity according to predefined procedures.

8 Social and legal issues of cloud services

8.1 General

As society becomes more data-centric, cloud services are coming to be seen as the core IT infrastructure, and organizations and governments are adopting cloud services more and more. However, a legal standard appropriate to regulate cloud computing is not fully in place in most jurisdictions, and uniform