TECHNICAL REPORT

ISO/IEC TR 3445

First edition
2022-03

Information technology — Cloud computing — Audit of cloud services

Reference number
ISO/IEC TR 3445:2022(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) 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 or www.iec.ch/members_experts/refdocs).

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 https://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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC 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 and www.iec.ch/national-committees.

Introduction

This document provides an overview of the audit of cloud services. ISO/IEC 22123-1 defines the term cloud auditor while ISO/IEC 17789 describes the cloud computing roles and sub-roles and activities related to the audit of cloud services. ISO/IEC TR 23187 which describes the interactions between cloud service partners (CSNs), cloud service customers (CSCs), and cloud service providers (CSPs) provides some perspectives on the role and responsibilities of a cloud auditor. This is covered in part in Clause 5 as shown in Figure 1.

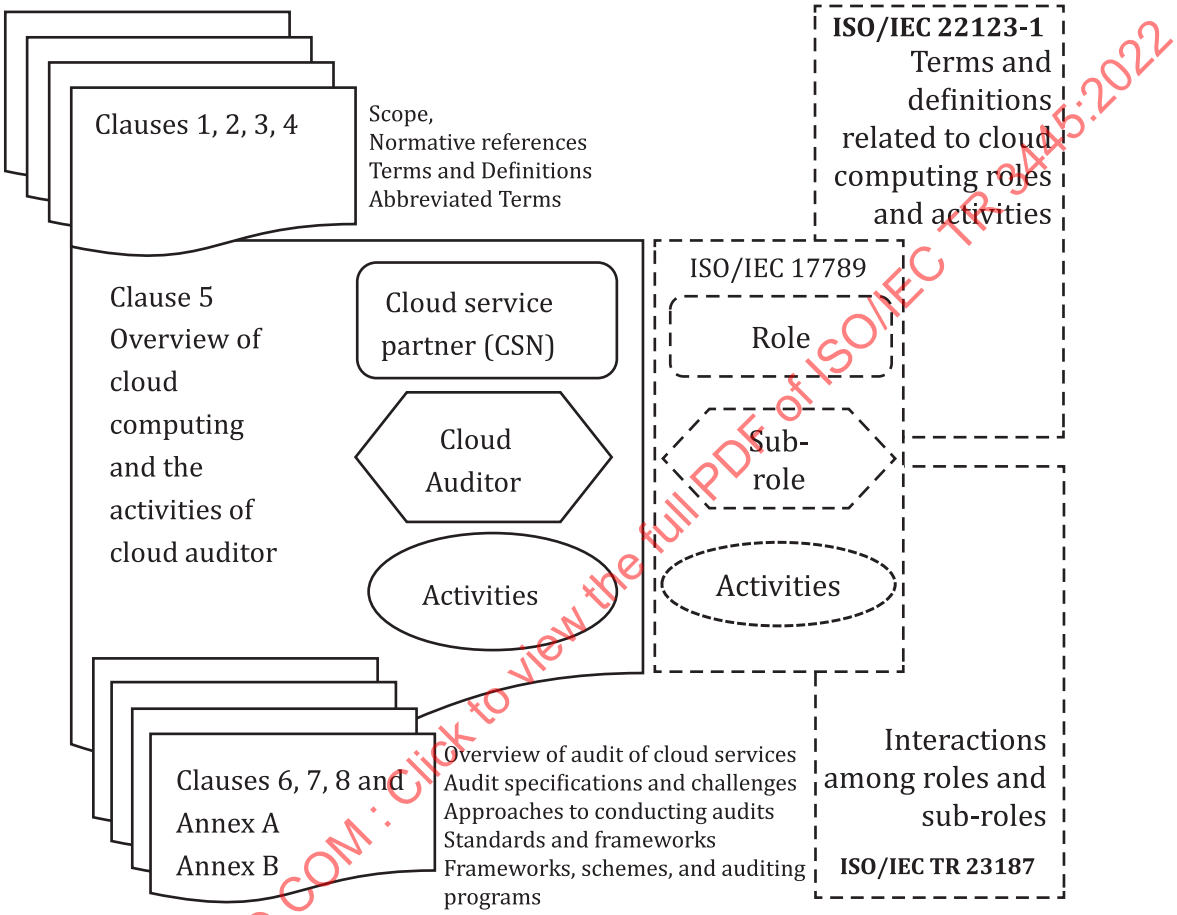

Figure 1 — Structure of the document

The structure of the document is as follows:

Clause 5 includes an overview of cloud computing and its major roles. This clause also covers the role of cloud auditor, its responsibilities, and its relationship with other major cloud computing roles.

Clause 6 provides an overview of cloud service audit including an explanation of the relationship between audit, assessment, compliance, evaluation, assurance and conformity assessment.

Clause 7 builds on the foundation information in Clause 5 to discuss audit specifications and the challenges associated with a cloud audit.

Clause 8 covers approaches to conducting cloud audit.

Annex A provides information on International Standards relating to audit and frameworks for audit schemes, certification and authorization.

Annex B is a compilation of available frameworks and standards which can be used for audit schemes, for certification and for authorization.

Information technology — Cloud computing — Audit of cloud services

1 Scope

This document surveys aspects of the audit of cloud services including:

1) role and responsibilities of parties conducting audit and description of the interactions between the CSC, CSP, and CSN;

2) approaches for conducting audits of cloud services to facilitate confidence in delivering and using cloud services;

3) examples of available frameworks and standards which can be used for audit schemes, for certification, and for authorization.

This document builds upon the cloud auditor role as defined in ISO/IEC 17789 and ISO/IEC 22123.

This document is applicable to all types and sizes of organizations that need to plan and conduct internal or external audits, and that use, provide and support cloud services.

This document is not intended to describe certification or to identify controls that are published elsewhere.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 22123-1:2021, *Information technology — Cloud computing — Part 1: Vocabulary*

3 Terms and definitions

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

ISO and IEC maintain terminology 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 Terms related to the use of audit and assessment

3.1.1
assurance
activity resulting in a statement giving confidence that a product, process or service fulfils specified requirement

[SOURCE: ISO/IEC Guide 2, 15.1]

3.1.2
attestation
issue of a statement, based on a decision, that the fulfilment of specified requirements has been demonstrated

Note 1 to entry: The resulting statement, referred to in the source document as a "statement of conformity", is intended to convey the *assurance* (3.1.1) that the specified requirements have been fulfilled. Such an *assurance* (3.1.1) does not, of itself, provide contractual or other legal guarantees.

Note 2 to entry: First-party attestation and third party attestation are distinguished by the terms declaration, *certification* (3.1.4) and accreditation, but there is no corresponding term applicable to second party attestation.

[SOURCE: ISO/IEC 17000:2020, 7.3]

3.1.3
authorization
privileges that give access to designated activities

[SOURCE: ISO 11442:2006, 3.5]

3.1.4
certification
third party *attestation* (3.1.2) related to an object of *conformity assessment* (3.1.6), with the exception of accreditation

[SOURCE: ISO/IEC 17000:2020, 7.6]

3.1.5
certification audit
audit (3.2.2) carried out by an auditing organization independent of the client and the parties that rely on *certification* (3.1.4), for the purpose of certifying the client's management system

Note 1 to entry: In the definitions which follow, the term "audit" has been used for simplicity to refer to third party certification audit.

Note 2 to entry: Certification audits include initial, surveillance, re-certification audits, and can also include special audits.

Note 3 to entry: Certification audits are typically conducted by audit teams of those bodies providing *certification* (3.1.4) of conformity to the requirements of management system standards.

Note 4 to entry: A *joint audit* (3.2.11) is when two or more auditing organizations cooperate to audit a single client.

Note 5 to entry: A *combined audit* (3.2.9) is when a client is being audited against the requirements of two or more management systems standards together.

Note 6 to entry: An integrated audit is when a client has integrated the application of requirements of two or more management systems standards into a single management system and is being audited against more than one standard.

[SOURCE: ISO/IEC 17021-1:2015, 3.4]

3.1.6
conformity assessment
demonstration that specified requirements are fulfilled

Note 1 to entry: The *process* (3.1.8) of conformity assessment as described in the functional approach in Annex A can have a negative outcome, i.e. demonstrating that the specified requirements are not fulfilled.

Note 2 to entry: Conformity assessment includes activities defined elsewhere in the source document, such as but not limited to testing, inspection, validation, verification, *certification* (3.1.4), and accreditation.

Note 3 to entry: Conformity assessment is explained in Annex A as a series of functions. Activities contributing to any of these functions can be described as conformity assessment activities.

Note 4 to entry: The source document does not include a definition of "conformity". "Conformity" does not feature in the definition of "conformity assessment". Nor does the source document address the concept of compliance.

[SOURCE: ISO/IEC 17000:2020, 4.1]

3.1.7
compliance
compliant
meeting or exceeding all applicable requirements of a standard or other published set of requirements

[SOURCE: ISO/TR 19591:2018, 3.60]

3.1.8
process
set of interrelated or interacting activities that use inputs to deliver an intended result

[SOURCE: ISO 19011, 3.24]

3.2 Terms related to cloud service audit

3.2.1
assessment
process of collecting and analyzing outcomes to determine course of actions

3.2.2
audit
systematic, independent and documented *process* (3.1.8) for obtaining *objective evidence* (3.2.12) and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Note 1 to entry: *Internal audits* (3.2.10), sometimes called first-party audits, are conducted by, or on behalf of, the organization itself.

Note 2 to entry: External audits include those generally called second and third party audits. Second party audits are conducted by parties having an interest in the organization, such as customers, or by other individuals on their behalf. third party audits are conducted by independent auditing organizations, such as those providing *certification* (3.1.4)/registration of conformity or governmental agencies.

[SOURCE: ISO 19011:2018, 3.1]

3.2.3
cloud service audit
audit (3.2.2) of the provision and use of one or more cloud services

Note 1 to entry: An audit of a cloud service can include cloud characteristics, cloud deployment, cross cutting aspects and related management and security functions.

3.2.4
audit client
organization or person requesting an *audit* (3.2.2)

Note 1 to entry: In the case of *internal audit* (3.2.10), the audit client can also be the *auditee* (3.2.7) or the individual(s) managing the audit programme. Requests for external audit can come from sources such as regulators, contracting parties or potential or existing clients.

[SOURCE: ISO 19011:2018, 3.12]

3.2.5
audit programme
arrangements for a set of one or more *audits* (3.2.2) planned for a specific time frame and directed towards a specific purpose

[SOURCE: ISO 19011:2018, 3.4]

3.2.6
audit scope
extent and boundaries of an *audit* (3.2.2)

Note 1 to entry: the audit scope generally includes a description of the physical and virtual-locations, functions, organizational units, activities, and processes, as well as the time period covered.

Note 2 to entry: A virtual location is where an organization performs work or provides a service using an on-line environment allowing individuals irrespective of physical locations to execute processes.

[SOURCE: ISO 19011:2018, 3.5]

3.2.7
auditee
organization as a whole or parts thereof being audited

[SOURCE: ISO 19011:2018, 3.13]

3.2.8
auditor
person who conducts an *audit* (3.2.2)

[SOURCE: ISO 9000:2015, 3.13.15]

3.2.9
combined audit
audit (3.2.1) carried out together at a single *auditee* (3.2.7) on two or more management systems

Note 1 to entry: When two or more discipline-specific management systems are integrated into a single management system this is known as an integrated management system.

[SOURCE: ISO 9000:2015, 3.13.2, modified]

3.2.10
internal audit
audit (3.2.2) conducted by, or on behalf of, an organization itself for management review and other internal purposes, and which can form the basis for an organization's self-declaration of conformity

Note 1 to entry: In many cases, particularly in smaller organizations, independence can be demonstrated by the freedom from responsibility for the activity being audited.

[SOURCE: ISO 22300:2021, 3.1.134]

3.2.11
joint audit
audit (3.2.2) carried out at a single *auditee* (3.2.7) by two or more auditing organizations

[SOURCE: ISO 9000:2015, 3.13.3]

3.2.12
objective evidence
data supporting the existence or verity of something

Note 1 to entry: objective evidence can be obtained through observation, measurement, test or by other means.

Note 2 to entry: objective evidence for the purpose of the *audit* (3.2.2) generally consists of records, statements of fact, or other information which are relevant to the audit criteria and verifiable.

[SOURCE: ISO 9000:2015, 3.8.3]

3.2.13
party
natural person or legal person, whether or not incorporated, or a group of either

[SOURCE: ISO/IEC 22123-1:2021, 3.4.1]

4 Abbreviated terms

BCR	binding corporate rules
Cloud SLA	cloud service level agreement
CSA	cloud service agreement
CSC	cloud service customer
CSN	cloud service partner
CSP	cloud service provider
CSU	cloud service user
FISMA	The Federal Information Security Modernization Act of 2014 (FISMA 2014) (US)
GDPR	General Data Protection Regulation (EU GDPR)
HSPD-12	Homeland Security Presidential Directive 12 (US)
ISMS	information security management system
IT	information technology
LGPD	Brazil's Lei Geral de Proteção de Dados
PCIDSS	Payment Card Industry Data Security Standard
PIA	Privacy impact assessment
PIMS	Privacy information management system
SDOC	Suppliers Declaration of Conformity
SLO	cloud service level objective
SQO	cloud service qualitative objective

5 Overview of cloud computing and the activities of a cloud auditor

5.1 Overview of cloud computing

5.1.1 General

Cloud computing, as defined in ISO/IEC 22123-1:2021, 3.2.1, is a 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. The cloud computing paradigm is comprised of cloud computing roles and activities, cloud capabilities types and cloud service categories, cloud deployment models, key characteristics and cross cutting aspects as shown in Figure 2.

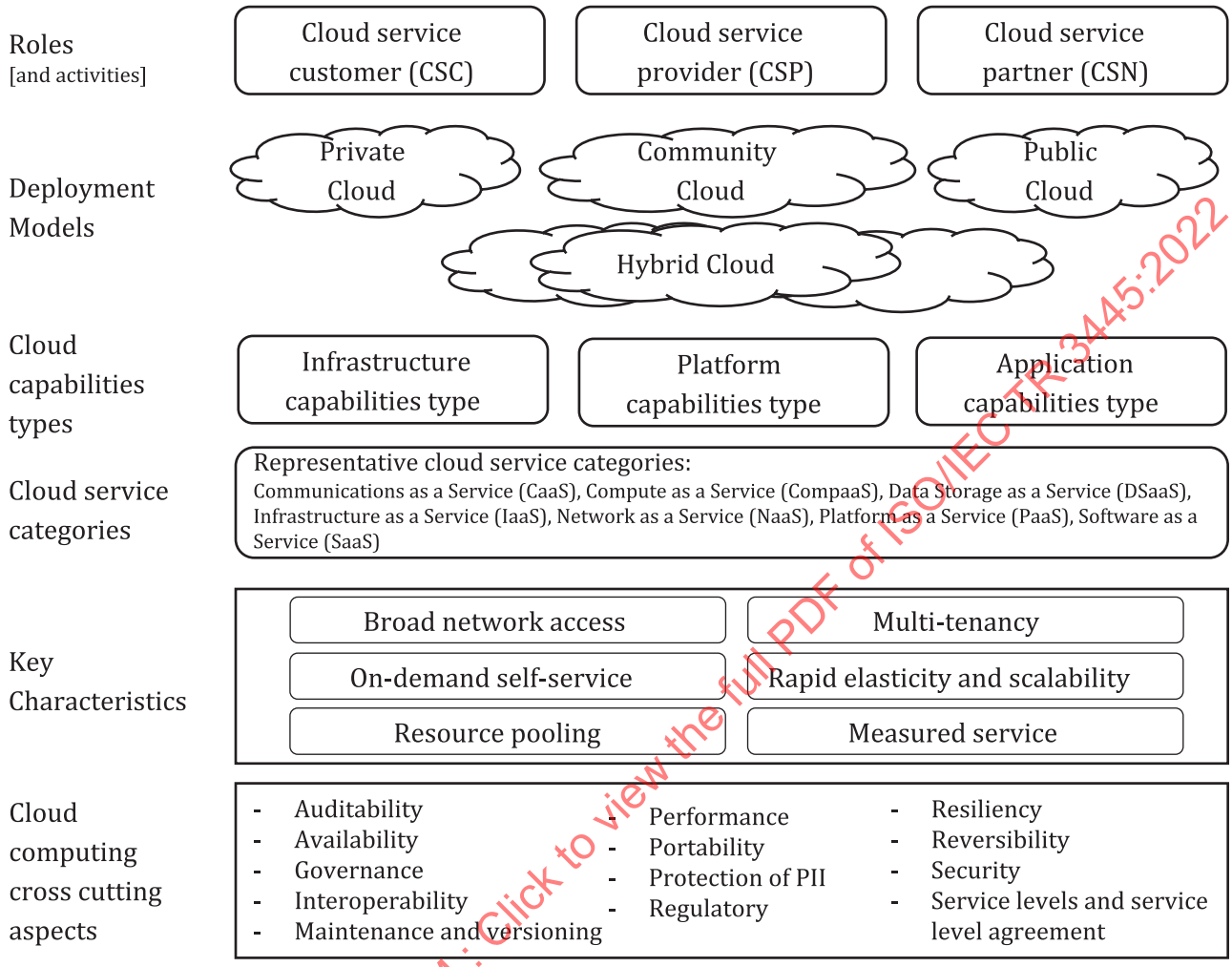

Figure 2 — Overview of cloud computing

5.1.2 Cloud computing roles, sub-roles and activities

In the context of cloud computing and of particular importance to this document is the clarification of the different roles and their activities. ISO/IEC 22123-1 identifies the major roles of cloud computing and ISO/IEC 17789 expands on the roles to include sub-roles activities, and their relationship to the functional components and functional layers of cloud computing.

The major cloud computing roles are:

— Cloud service customer (CSC) is a party which is in a business relationship for the purpose of using cloud services.

— Cloud service provider (CSP) is a party which makes cloud services available.

— Cloud service partner (CSN) is a party which is engaged in support of, or auxiliary to, activities of either the CSP or the CSC, or both.

In performing the role, the party (3.2.13) can take on more than one sub-set of the cloud computing activities of a given role. ISO/IEC TR 23187: provides an overview of and guidance on interactions

between cloud service partners (CSNs), specifically cloud service brokers, cloud service developers and cloud auditors, with CSPs and CSCs.

ISO/IEC 22123-1 and ISO/IEC 17789 do not claim to describe all possible CSN sub-roles. These standards have identified three initial sub-roles of the CSN: the cloud service broker, the cloud service developer, and the cloud auditor. A CSN supports the CSC or CSP or both in delivering or using the cloud services. In the use of cloud computing and in carrying out the activities of each role, an audit client can be a CSC, CSP or CSN. Through the delivery and use of cloud services, interaction and related activities initiated by one party can influence responsive activities from another party or parties.

5.2 Overview of the activities of a cloud auditor

5.2.1 Cloud auditor

Auditors of cloud services and more generally of management systems are required to conduct independent assessments of the CSC's system specific controls for its cloud services. These potentially address stored data, applications, operations, performance, privacy and security of the cloud implementation. Security measures that the CSP implements and operates are also included.

The cloud auditor is further responsible for assessing the CSC's cloud-specific controls. The audit specification criteria vary and can depend on many factors. The audit specifications (see Clause 7) can be set in collaboration with the CSP, by the cloud auditor alone, by standards set independently or possibly as required by law.

Since the cloud auditor's defined audit responsibilities cover both the use and provision of cloud services, the auditor can conduct the audit for the CSP, the CSC or both organizations.

The cloud auditor can perform both internal and external audits.

Figure 3 — An example of CSP and CSC responsibilities

Shared responsibility as illustrated in Figure 3 means the audit criteria specifications vary depending on the cloud deployment model and the cloud services being implemented. It is the responsibility of an auditor to have a comprehensive understanding of these implementation in order to establish clear boundaries and ownership of the security controls that are to be audited. It is important to note that a CSC can use a CSP's third party attestations as evidence that the requirements associated with the CSP have been satisfied.

5.2.2 Responsibilities of a cloud auditor

A cloud auditor's primary responsibility is to conduct audit to the agreed specifications, policies and agreements.

The specifications (see Clause 7) can include standards defined by the CSP, CSC or cloud auditor, standards defined independently, or standards required by law. Certification provided by CSPs and third party suppliers can be evaluated and considered in the result of the audit. The CSP sets the policies for auditing CSP's infrastructures and services.

All agreements are based on the negotiated cloud service agreement (CSA) or cloud service level agreement (cloud SLA).

In addition, ISO/IEC 17789:2014, A.4 states that the cloud auditor's activities focus on the following categories of audits:

— security audit: see 6.3.4.3;

— privacy audit: see 6.3.4.4;

— performance audit: see 6.3.4.5.

Many principles help to make an audit an effective and reliable tool. ISO 19011 discusses principles that provide critical guidance to auditors or cloud auditors in performing their tasks including integrity, fair presentation, professional care, confidentiality, independence, evidence-based approach and risk-based approach. In addition, an understanding of the relationship between transparency, assurance and accountability is a relevant contributor to audit quality.

In addition, the following practises are helpful to ensure an audit is an effective and reliable tool as well as maintain compliance with local laws or regulations:

— Audits can be conducted in a risk-based manner, taking into account concerns regarding the organizational burden for both the outsourcing institution and the cloud service provider, as well as practical, security, and confidentiality concerns regarding access to certain types of business premises or data in multi-tenant environments.

— Audits are subject to the principle of proportionality; they are to be applied in a manner that is appropriate, taking into account, in particular, the institution's size and internal organization and the nature, scope and complexity of its activities.

— Auditors have a professional duty to preserve their objectivity and to avoid conflicts of interest. (Customer audit requirement).

— Auditors are expected to treat all information received as strictly confidential and handle with due care. (Customer audit requirement).

— Auditors usually are compliant with generally accepted international professional standards for auditing and with a code of ethics, one such example is the International Professional Practices Framework (IPPF) issued by the Institute of Internal Auditors of North America (IIA).

5.2.3 Cloud auditor's cloud computing activities

The cloud auditor can conduct the audit for the CSP, CSC, or both. The cloud audit can include both internal (see 6.3.2) and external audits (see 6.3.3). ISO 19011:2018, 5.4.1 discusses the role and responsibilities of the individual(s) managing an audit programme, and ISO 19011:2018, 5.4.2 explains the competence of the individual(s) managing the audit programme.

ISO 19011:2018, 5.2 lays out objectives for an audit programme and the auditor's activities can be aligned with establishing those audit programme objectives. The individual(s) conducting an audit of cloud services can refer to those guidelines.

The auditors in conducting an internal or external audit of a cloud-based IT system have to exercise professional judgement to complete the audit in response to the audit request. In completing the audit for compliance to SOC 2, for example, the auditor in his/her finding can point to pertinent standards previously not being considered or overlooked by the requester. This calls into the recommendation that the auditors need to have appropriate continual development activities to maintain the necessary competency and knowledge in, e.g. information security, data protection and cloud computing system.

5.2.4 Relationship of the cloud auditor to CSPs, CSCs, and other CSNs

The cloud auditor interacts with the CSC and CSP in its auxiliary role. In performing its activities, the cloud auditor inevitably interacts with other CSN sub-roles such as the cloud service developer and cloud service broker. The relationship is closely dependent on the roles involved in the use and provision of cloud services as explained in ISO/IEC TR 23187, Clause 6. For example, a party can play more than one role as a provider of application capabilities type and be using infrastructure capabilities type from a CSP. A clear delineation of roles, relationship and activities is essential in establishing the audit scope and objectives. Depending on the objectives of the audit result, the cloud auditor is to work with CSCs, CSPs or audit clients (organizations requesting audits), and align its audit specifications (see Clause 7) appropriately to standards and laws (see 7.5).

ISO/IEC TR 23187 presents several illustrative scenarios of a cloud computing environment whereby cloud auditor identifies the activities performed in relation to the use or provision of the cloud service as part of planning the audit objectives. ISO/IEC 17789 and ISO/IEC 22123-1 explicitly assign the responsibility for providing cloud services to the CSP. Cloud services are being offered in many incongruent forms and sizes. The "provider" of the cloud service can be offering capabilities such as data storage and computing power or access to an application. The activities of a CSP can include data handling, processing data, processing for storage directly or through outsourcing services and managing the cloud service for users or for a CSP. The cloud auditors establish a good understanding of the context, the delivery of the cloud services, and the roles, responsibilities and relationship among the roles.

The cloud auditor can work independently or as a member of an auditing team. It is possible for an organization to assemble an internal assessment and audit. This audit team will be responsible to the organization's audit processes, activities, functions or locations and, as appropriate, authority for decision-making. In this capacity, the individual auditor is most likely responding to and working with senior management and critical stakeholders within the organization.

6 Overview of the audit of cloud services

6.1 General

A cloud service audit is defined in this document as an audit of the provision and use of cloud services, and it is described in 8.4.1.2 in ISO/IEC 17789:2014 to assess a system specific controls against a specified set of audit criteria to ensure that they have been satisfied. A cloud service audit is not independent from auditing of an organization's system and it is helpful to consider as integral part of the entire system.

The adoption of cloud computing requires important changes to many CSC business processes. The CSPs have varied business specific needs. The selection of cloud deployment models, cloud services, and CSPs includes certain complexities since the CSCs select solutions to integrate and interoperate with their infrastructure that are all built and run differently. The concerns as well as benefits of using cloud services, provisioning capabilities and resources, and responsibilities for CSCs and CSPs covered in Clauses 6 and 7 are elements to be considered in the design and implementation of an audit. This can contribute to the strategies and plans for the journey to implement cloud computing.

ISO/IEC 27017 provides guidelines for information security controls applicable to the provision and use of cloud services. It includes implementation guidance for relevant controls specified in ISO/IEC 27002 and additional controls with implementation guidance that specifically relate to cloud services. The criteria specifications vary and are dependent on several factors. A CSC or an external third party auditor contracted by the CSC can conduct an external audit, i.e. a second party audit on a CSP. It is important to note that a CSC can use a CSP's third party attestations as evidence that the requirements associated with the CSP have been satisfied.

6.2 Objectives of an audit of cloud service

6.2.1 General

Cloud computing enables network access to physical or virtual resources and transforms traditional business information technology (IT) services. It offers benefits associated with the key characteristics (see Figure 2) and the use of cloud services also requires diligence and care in planning and strategies. The evidence obtained from audits (3.2.2) and cloud service audits (3.2.3) can help to provide clarity and understanding to the use of cloud services and in planning for their future developments.

A cloud service audit (3.2.3) offers a practical value to the CSCs or audit client, and it is applicable to all types and sizes of organizations. CSUs are persons who expect to trust that the cloud service products are deemed secure to use or deploy cloud service; and have confidence that the CSP(s) will have the appropriate security processes in place to maintain their security posture. In order to build trust, cloud service audits (3.2.3) have an important purpose of cloud computing.

The CSCs in some circumstances, can seek assurance in determining the adoption of suitable cloud service strategy to meet their business specific needs (6.2.4 and 7.4) and selecting the best solution with a CSP or CSPs. There are a few contributors to the challenges: In the cloud computing environment, the management responsibilities are shared between CSCs and CSPs. It is not a simple task for one party to monitor and manage one's environment and it is added complexity in sharing responsibilities without clear visibility of the other environment. CSCs and CSPs have separate and different configurations, governance practises and policies for addressing each environment.

An audit or a cloud audit is a good start for assessing the organization's system compatibility for adoption of the use of cloud computing. It can provide evaluation and comparison of the service offerings before acquisition, determination of potential planning for expanding use of cloud services or for preparation for cyber insurance and auditing the system for continued use of cloud services.

6.2.2 Audit objectives

An audit (3.2.2) focuses on obtaining objective evidence (3.2.12) and evaluating it objectively to determine the extent to which the audit criteria are fulfilled. The types of audit performed include security, privacy impact and performance. A cloud service audit (3.2.3) typically includes some of all of the following as evidence (depending on who the cloud auditor is responsible to not everything in this typical list will apply):

— fundamentals and impact of cloud computing;

  An objective of a cloud audit is to determine the impact of cloud computing on the organization's systems and its boundaries. This includes:

  — different types of cloud computing architectures and service delivery models;

    Cloud architecture bring together the necessary components and capabilities to connected to allow applications to run on e.g. cloud capabilities types (see Figure 2). As every organization and every CSP has their own unique environment that result in different types of cloud computing. architectures and service delivery models are unique in every organization. Assessment is to navigate challenges (7.14) and security threats to adopting a cloud computing architecture.

  — different cloud services;

    When an organization is using more than one cloud service which are potentially provided by different CSPs, the complexity of assessment increases. The audit of any CSP is subject to negotiation and visibility is further challenged (see 7.9).

— provider management and its role in maintaining service;

The assessment seeks to have a good understanding of the service model and applicable metrics, the difference between the organization and the cloud service, and the perimeter of the technology boundary. This is considered as third- and fourth-party risks.

— security risk assessment of the system associated with the use of cloud services (see 7.3, 7.4 on challenges];

When using a cloud service from a CSP who is using services delivered from another CSP, for example, the assessment does not consider only the benefits of using cloud service but that security risks can be compromised. ISO/IEC TR 23187, Clause 10 illustrates some exemplary scenarios that are only representative of a fraction of offerings available. One objective of a cloud services audit is to assess the security risk of systems associated with the use of the cloud services. This can include on-premises systems, management systems, and others.

— different connected services and devices;

One objective of a cloud service audit is to assess how these services and devices connected to the system; security and privacy management; data protection, transfer and use; device security and integrity plan; access control.

— governance, policies and processes;

One objective of a cloud services audit is to include applicable and required principles, policies and frameworks by which an organization is directed and controlled. It also includes the establishment of strategy and policy for the use of IT, and organizational control of the use of IT. The processes by which an organization obtains assurance that the risks to its information, and thereby the operational capabilities and integrity of the organization, are effectively identified and managed (also see challenges 7.5, 7.6 and 7.14). In view of a cloud service audit (3.2.3), cloud governance and cloud security can include:

— identifying and maintaining security controls;

— balancing the responsibilities for security shared between CSC and CSP;

— deploying a set of core cloud security controls with an understanding of CSC's responsibilities;

— meeting regulatory requirements to protect sensitive data in the cloud computing environment;

— regulatory compliance and legal procedure (also see 7.6, 7.7, 7.14 on challenges];

One objective of a cloud service audit includes reviewing the use of cloud computing is subjected to compliance to applicable and required laws and regulations. This is applicable to using and providing services in the cloud computing environment.

— operations, performance and security;

One objective of a cloud services audit is to assess the operations, performance and security of the cloud service are instrumental to the business continuity and impact components and resources of the service, e.g. service resilience, scalability and disaster recovery. Audit can include, for example, an assessment of a disaster recovery plan.

— examines whether a specified set of audit criteria are met (see Clause 7);

Per ISO 19011, the audit criteria can include individually or in combination the following:

— requirements defined in one or more management system standards;

— policies and requirements specified by relevant interested parties;

— statutory and regulatory requirements;

- one or more management system processes defined by the organization or other parties;
- management system plan(s) relating to the provision of specific outputs of a management system (e.g. quality plan, project plan);

— exception on external certifications;

Dependent on the business operation, one objective of a cloud services audit is to uncover one or more audit exceptions or deviations. These can include external certifications that correction to the controls included for coordination and implementation as they can potentially expose risk to the auditee's customer data and intellectual property.

6.2.3 Audit boundaries

The extent and boundaries of the audit, and the audit scope generally includes a description of the physical and virtual locations, functions, organizational units, activities and processes, as well as the time period covered. In a cloud computing environment, security and compliance are a shared responsibility between the CSP and the CSC as shown in Figure 3. The audit scope accounts for this consideration and align with an organization's overall audit programme and objectives.

The CSP is responsible for protecting and securing the infrastructure, including the hardware, software, network and facilities that the CSP utilizes to operate their cloud services, whereas the CSC and CSN are responsible for security measures related to the security of their content and applications that operate on the CSP's. Just as the responsibility to operate the IT environment is shared between the CSP and its customers, so is the management, operation, and verification of IT controls (i.e. inherited, shared and customer specific controls).

The system boundaries of the shared responsibility model shift depending on the deployment model that the CSC implements and operates as shown as examples in Figure 3 and will affect the scope of the environment in the cloud computing environment defined to be audited. The figure presents the platform and application capabilities types in which the CSCs have reduced responsibilities and use less resources, but they also have less control of the environment hosting their sensitive data. Special attention to contractual agreements and on-going due diligence is included to ensure that the CSPs maintained and met the required security measures throughout the duration of the agreement.

Understandably an audit of different cloud deployment models is inevitably different as the environment and CSA are unique to the CSCs and CSPs. ISO/IEC TR 23187, Clause 10 illustrates six examples of different delivery of cloud services involving various roles and activities that are not the anticipated relationship between users or CSCs with CSPs. It is possible that these examples - reselling of cloud services, cloud service exchange, management of cloud services, cloud data management service and shared cloud service, do not have an CSA or cloud SLA directly between CSP and CSC. The audit client and auditor are to follow diligent evaluation of the cloud computing environment and the audit objectives.

6.2.4 Relationship of an audit and the organization

Figure 4 illustrates how the appropriateness and regularity of audit and assessment can benefit an organization's strategic planning, risk management and business mission. There is an inter-related fundamental relationship between establishing a comprehensive understanding of the organization's IS and its risk management, the organization's strategy, business mission, and audit – see Figure 4. A good inventory and analysis of the organization's system can contribute to building the organization's strategy and business mission, and to establish the audit scope, objectives, regularities, and specifications. An audit can involve testing, validating, and verifying each control within the organization's service is operating effectively and service description is accurate. The assessment of the audit can be used to update the organization's understanding, to help in strategizing the use of cloud services, and to design an internal or external audit. Auditors can benefit from the review of monitoring efforts while audit findings can validate the organization's monitoring efforts. The organization's assessment efforts can help to evaluate the application of appropriate technical and non-technical controls (e.g. legal) in compliance to various countries and geolocation laws and regulations.

Figure 4 — Relationship and purpose of audit to an organization

Organizations, when considering adding cloud computing into their IT strategies, first begin with understanding cloud computing before transitioning to the cloud or expanding cloud services. An audit report can provide prudent analytical information to the planning and implementation process. A sound cloud strategy does not narrowly focus on IT but involves many major functions of an organization (e.g. business, legal, finance, operations, procurement and human resources). This is not to be confused with a cloud implementation or migration plan. Business cloud strategy is asymmetrical, dependent on company size. For example, one very large organization can have more than 10 000 virtual machines on-premises and managed multiple private data centres. The cloud computing environment introduces moving parts across on-premises or cloud-based services and creating a complex web of infrastructure when interconnected.

Cloud computing offers many benefits and has transformed the way businesses approach the consumption and delivery of IT services. But everything in Figure 2 and the potential to work with emerging technologies cannot be easily turned on with a flip of a switch. Organizations are to establish effective risk assessment and management processes before migrating its information technology operations to a cloud operating environment. Initiating an audit can provide pertinent information to establish a systematic and vigilant strategic plan. An assessment can include the following areas:

— define the business case for adopting the use of cloud computing;

— identify organization requirements and regulations;

— compare internal requirements with cloud service specifications;

— define metrics and security parameters (see 7.11, 7.12);

— understand the differences (challenges) between legacy system (see 7.3.2) and cloud computing system;

— understand the structure of the cloud services and the hosting of cloud services;

— develop a high-level objectives and control objectives;

— define functional domains and organizational priorities;

— decoupling and separating an organization's business service from the infrastructure used to run it (i.e. virtualization);

— consider flexibility to use CSPs that provide reliable and scalable user application, development environments and infrastructure, and most importantly, meet the organization's risk profile;

— data sovereignty and accessibility to business customers, stakeholders and users, and the ability for rapid deployment of new user application;

— cost allocation and resources subscription.

6.3 Types of cloud audit

6.3.1 Overview

From the perspective of ISO 19011, the definition for "audit" (see 3.2.2) supports the description of the three types of audits in Table 1:

Table 1 — Different types of audits

First party audit	Second party audit	Third party audit
Internal audit (3.2.10)	External audit	External audit
Organization's internal assessment	External provider audit	Certification and/or accreditation audit
Organization's outsourced party audit	Other external interested party audit	Statutory, regulatory and similar audit

IT system audit is generally classified into three categories as illustrated in Table 1. But the cloud computing system audits in this document are categorized into two categories, internal audit (First party audit) and external audit (Second party audit). It is helpful for auditing entities to understand this difference. In consideration of the exposition of cloud services and an organization's risk posture, the organization considers the frequency or regularity of conducting an audit and assessment to ensure the efficiency of controls and to satisfy its governance and laws.

6.3.2 Internal audit

Internal audits (3.2.10), also known as first party audits (see 3.2.2 note 1) can be conducted by an employee of the organization, a person hired by the organization or jointly with an outsourced consulting organization. The person conducting an internal audit is acting on behalf of the organization and not as a customer or certification body. An internal audit can include identifying risks to be mitigated to optimize the benefits of any outsourcing relationship, and to position the organization to assess and manage risk as the cloud services evolve, especially for third party compliance.

An internal audit is generally meant to provide assurance by assessing and reporting on the effectiveness of the governance, risk management, and control processes and is designed to help the organization achieve strategic, operational, financial, and compliance objectives. An internal audit of the provision and use of cloud services will also focus on the organization's enterprise operation and security requirements with the use of cloud computing. It is focused not only on whether the company processes meet the requirements of a standard, but on all rules the company has set for itself. The design of the audit, which depends on the audit objectives and the information that the organization is seeking, can be much more comprehensive and thorough than other audits. The audit proactively identifies risks to be mitigated to optimize the benefits of the cloud services.

Internal audits are often associated as first party audits (see 3.2.2 note 1). A CSP can conduct an internal audit of its cloud service products and make the report available in response to the request of its customers.

Generally, as best practise of an ISMS, organizations assess potential risks when making changes to their structures. This is especially true with the adoption, continued use and in anticipation of expanded use of cloud computing. By having a clear understanding of the key risks to the organization, the organizations can make strategical plans to manage those risks. Internal audit provides fundamental information to assist an organization to determine adequate preparation in reducing risk and a mean for evaluating migration process.

In preparing the business case for adopting a cloud strategy, organizations' internal audit can assess the following:

— Regulatory compliance: assess the CSPs' approach to meeting the regulatory requirements with which the organization has to comply (see 7.5, 7.6).

— Data location and ownership: assess whether the location of CSPs data storage and processing meets the required jurisdictional conditions (7.6.2).

— Business viability and recovery: assess the confidence of getting the organization's data if and when the CSPs lose their business, and the impact to recovery capabilities.

— Colocation and data segregation: assess the physical location of data storage and assurance of data server and separation of the organization's data (7.6.2).

— Systems and data: assess the sensitivity and adaptability of the organization's data considered for possible use in the cloud environment.

— Organization's risks and controls: assess CSPs that best align with the organization's controls and evaluate how best to address any gaps.

— Roles and responsibilities: determine the roles and responsibilities of both the organization and CSPs in ensuring the use of the cloud services.

— Assessment of application: determine the suitability of legacy or non-cloud systems viability for cloud migration and applicability for use with cloud services.

— Assessment of applications for migration: non-cloud to private cloud, non-cloud to public cloud, private cloud to public cloud and private cloud to public cloud.

— Privileged user access: assess CSPs control and assurance of access to the organization data (e.g. 7.11, 7.14).

6.3.3 External audit

6.3.3.1 General

External audits are also known as second party audits and third party audits. A second party audit is conducted by a person who has an interest in the organization, such as a customer, partner, or its agent. It can be conducted on-site or off-site by reviewing documents submitted by the organization being audited, e.g. ISO/IEC 27001. A third party audit can be conducted by an independent auditing body, such as an agency or government agency that provides certification and registration for conformance.

An organization conducts an audit of another organization, e.g. a CSP, to ensure that the CSP meets the requirements specified in the CSA. The requirements potentially include similar areas as internal audit - assessing and reporting on the effectiveness of governance, risk management, and control processes that have been designed to help the organization achieve strategic, operational, financial, and compliance objectives.

The audit client has the option to request for an external audit of its CSP even when the CSP is certified by a third party audit. In seeking an external audit, the organization is looking to have a better understanding of the CSP's capability to meet the organization's needs and to determine the contractual elements.

6.3.3.2 Assessment of parties related to the organization

The CSC considers the assessment of any third parties associated to the organization that access and process the organization's data to ensure compliance to the CSC's or user's security requirements, policies and governance. It is a continuing challenge for many organizations to manage third party audits and aggregate data for a single unified audit profile. The CSC can specify the controls that the

CSPs can demonstrate compliance within an audit report or assessment of third party connected to the CSP. The complexity increases for auditing across multiple CSPs and monitoring changes for multiple cloud services provided by multiple CSPs.

The organization includes a process and governance for monitoring its third party users who have access to the organization's data and systems. This assessment to demonstrate the organization's process to manage its third party users as well as outsourced vendors. The assessment includes details, controls, risks, contracts, privacy notices and certificates from the third party users.

6.3.4 Exemplary tests and audits

6.3.4.1 Overview

Exemplary tests and audits including scans are subject to negotiation and agreement, and yet many direct testing and access to the CSP's physical infrastructure are usually non-negotiable. CSPs can choose to disallow CSCs to perform such activities or CSPs can limit the range and types of activities to remote vulnerability scans and comprehensive walk-in on-site visits. Therefore, it is very important for CSCs to test the effectiveness of the governance framework and policy. The use of cloud services will continue to evolve and change with time and testing of the effectiveness of governance will continue. Conformance testing will be conducted to validate the procedures overtime. Alternatively, there are various best practise scenarios, e.g. CSCs can design a security breach as tests.

6.3.4.2 Exemplary tests

For the use of cloud computing, CSCs and CSUs have to rely more on assessment and not actual testing. A potential CSC can use the description of the CSP's proposed service offerings and attempt to integrate and test some of the services. Depending on the size of the potential CSC and the use of cloud services in certain regulated industries, exemplary tests or tests can be arranged that can include a deeper level of peering needs. For example, 1) automatic method to test availability of delivered functions (see 8.5); 2) codes can be built, tested and integrated regularly to ensure that applications are always in a working state; and 3) penetration testing after code is deployed especially for the use of the application capabilities type.

6.3.4.3 Security audit

A security audit can include cloud security, system security, endpoint security, vulnerability assessment, penetration testing, security risk assessment and information security management. For cloud audit, attention is directed to:

— Different data classification, or authorization level:

Cloud consumption model: where the cloud service resides, cloud service model/combination, ownership, new implementation or expansion building interoperability, workload provision, and data sensitivity.

— Visibility and governance:

In a cloud computing environment, many security controls can be beyond an organization's IT perimeter, and visibility to those controls and dataflow further increases the complexities. CSPs can limit direct access and audit of their systems. The CSPs can agree to provide assurance, e.g. audit and certification reports. Basing on an assessment or audit of the system on available information from CSC and CSP, there are areas that cannot completely be accessible to CSCs. A well-crafted and considered governance and process can help to elevate some visibility gaps. For assessment and audit of cloud services, visibility increases in complexity when considering the use of multifarious infrastructures, cloud services, deployment models and CSPs as shown in Figure 2 and Figure 3.

ISO/IEC TS 27008 describes the principles of auditing information security controls with reference to ISO/IEC 27002, which are general information security control measures, and ISO/IEC 27017, which are cloud service-specific information security control measures.

6.3.4.4 Privacy audit

Privacy as the focus of cybersecurity is safeguards of data, but privacy is most concerned with data of the individual and rights of the individual. In auditing an event, privacy risks look at data processing as it is the focus in ISO/IEC 27018 (see 6.3.4.4, ISO/IEC 27018:2019 PII Processors and public cloud) on protection of personally identifiable information (PII) in public clouds carried out by PII processors using cloud services.

For a privacy audit, the focus begins with the organization's privacy data architecture and data classification. The organization establishes an understanding on data as an asset (data subject, specific pieces of information such as personal data), data relationships and flows, and the business context in which the data is used across the organization. This includes the purpose in processing, legal basis, third party's involvement and access.

— Data classification considerations include:

  — how the organization is tracking sensitive data;

  — organization's data protection impact assessment;

  — jurisdiction;

  — mapping of recipients of data;

  — how service providers are being designated contractually and processing of data especially personal information;

  — contractors access and processing of data.

Privacy audit is to provide an audit trail and reporting as part of the management workflow that also covers security, e.g. authenticate users, validate identity, process for verification and detailing responsibilities to individuals.

A cloud auditor assesses the protection of personally identifiable information aspects of a cloud service and the CSP's operations against data protection regulations of the appropriate jurisdictions, following the guidelines issued by the data protection authorities and relevant standards. If the CSP is certified with a certain privacy framework, reliance on a report is optional. Privacy impact assessment (PIA) is subject to regulations and/or legislation that the CSC and CSP are operating the use of the cloud service. PIA report can include documentation about measures taken for risk treatment, for example, measures arising from the use of the information security management system (ISMS) in ISO/IEC 27001.

Designing and implementing the appropriate privacy audit is conditioned in part to required laws, regulations, and government requirements, but it is possible for global organizations to establish a holistic and globally harmonized approach to meet compliance to regulations and limit the use of sensitive information.

6.3.4.5 Performance audit

A performance audit is designed to assesses the CSP's ability to meet the performance targets for the cloud services as stipulated in the cloud SLA.

This audit can be included as part of either security or privacy audit.

6.3.4.6 Financial audit

A financial audit is designed to assess the CSC's cost management of its consumption and optimization of resources as they correspond to the performance targets for the cloud services as stipulated in the cloud SLA.

6.3.5 Relationship between audit and assessment for cloud computing

An audit (3.2.2) is a formal, systematic, independent, and documented process, as opposed to an assessment (3.2.1) that simply provides a process to collect information and analyze outcomes to determine course of action that benefits the organization. Generally, organizations have information gathered on their own systems and can include governance, policies, privacy, description of roles and responsibilities, and resources. This information allows the organization to lay out a foundation before setting out requirements and context that support the business mission and functions. This information gathered will allow the organizations to determine if a formal audit is needed. The auditor cannot audit or assess without the applicable information of the perimeter. Depending on an organization's needs and size, the information can be an assessment or audit conducted either internally or by an external party. For practicality and transparency, the information used is to be collaborated and engaged with stakeholders from all departments to ensure distinct processes are not unfairly overlooked vertically and horizontally.

Although the process of producing an assessment can involve an audit, its purpose is to provide a measurement rather than to express an opinion, i.e. determination about the fairness of statements or quality of performance. An assessment can be conducted as of a point in time, not necessarily over a period. Generally, an assessment aims to get a snapshot of the current status and provide a measuring stick to an ideal or a projected state whereas an audit targets compliance.

An assessment can be conducted by an organization's internal team or contracted third party to do an internal check. It is regularly conducted in advance of and in preparation for an audit, and it can be extended to a detailed audit. In this approach, an assessment seeks to look at how things can be, and then comparing how things essentially are with this benchmark. With a pre-emptive assessment, the organization has time and scope to remedy any issues, vulnerabilities, or gaps. The information for an assessment is usually collected in a few different ways, including surveys, interviews, comparison with external standards or frameworks, statistics, or reviews of records and reports showing historical information. An assessment can be useful to establish meeting the requirements for a sub-group of customers of an organization, e.g. government sector. Depending on the objectives, an assessment or an audit can be conducted annually and is particularly useful, if not also necessary, to be considered when determining major changes such as implementing or adding cloud services, to the system of an organization.

6.3.6 Relationships among audit processes and reports

6.3.6.1 General

Table 2 illustrates the relationship between audit, assessment, compliance, attestation, assurance, certification and authorization. All these processes serve different purposes and involve assessment, audit or both.

Table 2 — Relationships among audit process and reports

	Description of the process
AUDIT ASSESSMENT	**Audit** (3.2.2) – An audit is a "systematic, independent and documented process (3.1.8) for obtaining objective evidence (3.2.12) and evaluating it objectively to determine the extent to which the audit criteria are fulfilled". The evidence is evaluated impartially to determine whether it satisfies the criteria that is set for the audit. An audit provides findings and conclusion as supported by audit evidence that was formulated when defining and formalized audit programme. In comparison, **assessment** is simply a process of collecting and analyzing outcomes as opposed to the formal systematic and documented process to obtaining evidence and producing findings and conclusion.
Audit Assessment	An audit can follow the simple process of assessment depending on the audit objectives and scope. An organization or audit client requesting for an assessment in preparation for adopting cloud services can request an audit or an assessment.

Table 2 *(continued)*

	Description of the process
Attestation	**Attestation** (3.1.2) – An attestation is an issue of a statement, based on a decision, that the fulfilment of specified requirements has been demonstrated. The audit can be performed to establish, e.g. security compliance, and an evaluation of the objective evidence obtained from the audit can be used to support a decision to issue of a statement of attestation. The attestation is met with an issuance of a statement that fulfilment of specified requirements has been demonstrated based on a decision following review. For example, when the CSPs will not allow CSCs or their representatives or an auditor to perform on-site audits of their facilities or services, the CSP alternatively substantiate an attestation or assessment report from an independent third party. This statement can be evaluated and considered in the result of the audit.
Assurance	**Assurance** (3.1.1) – An assurance is the "activity resulting in a statement of confidence that a product, process or service fulfils specified requirements." An audit programme arranges one or more audits for a specific time frame. An assessment (3.2.1) of the audit findings and conclusion provide evidence that justifies the reasonability of the assurance. The statement in turn is intended to convey the assurance that the specified requirements have been fulfilled.
Compliance	**Compliance** (3.1.7) – A compliance is "meeting or exceeding all applicable requirements of a standard or other published set of requirements". A compliant audit or assessment is to establish the applicable requirements have been met. The audit reports evaluate the validity of compliance based on, e.g. a defined baseline standard and not essentially relevant to ensure that specified requirements meet the level of assurance. A blended approach includes compliance and assurance would include compliance with policy and the ability to provide assurance of a true assessment to the level of understanding of risks.
Certification	**Certification** (3.1.4) – A certification is a "third party attestation (3.1.2) related to an object of conformity assessment (3.1.6), with the exception of accreditation". Certification specifically focuses on third party attestation related to products, processes, or persons and is used to convey assurance that specified requirements have been demonstrated. As presented in 6.3.8, conformity assessment includes certification. The audit is carried out by an organization independent of the customer. Certification audit includes initial, surveillance, re-certification audits, and special audits. ISO/IEC 17021-1 also addresses joint, combined and integrated audits. A joint audit (3.2.11) is when two or more auditing organizations cooperate to audit a single customer. A combined audit (3.2.9) is when a customer is being audited against the requirements of two or more management systems standards, and an integrated audit is where a customer has integrated the application of requirements of two or more management systems standards into a single management system and is being audited against more than one standard. Annex A includes a general exemplary list of certification, authorization and programs. ISO/IEC 27006 is primarily intended to support the accreditation of certification bodies providing an information security management system (ISMS) certification. By extending from the requirements contained within ISO/IEC 17021-1, it specifies requirements and provides guidance for bodies providing audit and certification of an ISMS. The document is good reference source since an ISMS helps protect all forms of information, whether digital, paper-based or in a cloud system. A certification audit (3.1.5) carried out by an organization that is independent of the audit client and the parties to put the necessary assurance seal and set the stage for attestation (3.1.2) and authorization (3.1.3).

Table 2 *(continued)*

	Description of the process
Authorization	**Authorization** (3.1.3) – An authorization is "privileges that give access to designated activities". An assessment can be performed so as to issue an authorization. The authorization is focused, e.g. privileges, access control, authentication, etc. and the process to grant privileges to designated activities and generally can be coupled with a certification process in the use of cloud services, e.g. US FedRAMP – see Table 3.

6.3.6.2 Example scenarios of audit processes for cloud computing

Table 3 — Example scenarios on audit processes from the prospective of CSCs and CSPs

Process	Example scenarios	What does the process as applied to the example mean for		Assessment	Audit
		CSC	CSP		
Audit AUDIT	Prepare a cloud computing migration plan	— begin with an internal assessment to build an audit plan to determine the design and operational effectiveness of identified perimeter — establish audit scope, governance and policies — set up audit plan and communicate it to all stakeholders and management	— CSP provides to the auditor the data / information relating to the identified perimeter — CSP can use industry recognized legislations, frameworks and standards to comply with fundamental cloud security principles and requirements	√	√
NOTE Extreme right columns suggest whether an assessment, audit or both are used – see 6.3.5.					

Table 3 *(continued)*

Process	Example scenarios	What does the process as applied to the example mean for		Assessment	Audit
		CSC	CSP		
Assessment Assessment	Organizations considering cloud services or defining a cloud strategy – the organizations are to determine whether it is a simple assessment or a formal audit	— assessment of the system includes e.g. an inventory of applications, risk analysis, governance, policies, organization's risk appetite, etc — leverage mapping to standards, frameworks, CSPs publicly available security controls to assess CSPs overall security controls, e.g. determine what and where data is processed, and who has access to which data — assess the overall level of security offered by CSPs — assess and determine workload for use in the cloud computing environment	Assessment of CSP: — risk and security management, product catalogue in mapping to organization's capabilities — demonstrate compliance to fundamental cloud security principles and requirements — contribute information on self-assessment platform e.g. CSA STAR Self-assessment	√	√
Attestation Attestation	Attestation of compliance with federal, national and local statutes as well as industry best practises	— attain attestation on security controls as a basis for implementation that will be required by an auditor to validate the controls — attestation plays a part as the certification for products by third party — attestations are used to meet industry requirements to ensure compliance with federal, national and local statutes as well as industry best practises. Note that attestations simply attest that the tool exists and do not affirm their operational viability	— provide the CSC with the applicable attestation reports on the security controls associated with the cloud services — the attestation reports, which can be performed by an independent third party	√	
NOTE Extreme right columns suggest whether an assessment, audit or both are used – see 6.3.5.					

Table 3 *(continued)*

Process	Example scenarios	What does the process as applied to the example mean for		Assessment	Audit
		CSC	CSP		
Assurance Assurance	Measuring and assuring CSPs' ability to securely deliver cloud services	— contracted a third party to evaluate and validate e.g. SLA, negotiate new contract, etc. with either CSP or CSN — assurance involved the process of analysing and verifying that can be used in the assessment of audit records or selected assurance level, e.g. SOC 2, ISO, etc.	— include validating the CSP's output of a self-assessment of e.g. risk management — provide assurance on risks associated with managing and protecting the data in the cloud on behalf of CSCs and their users	√	
Compliance Compliance	Meeting compliance for required laws, regulations, and government requirements (see 7.5)	— review CSP's compliance reports that are relevant to the business functions of the organization; — leverage the mapping with industry accepted security standards, regulations, and controls frameworks	— compliance reports are prepared by a third party and are made available to CSCs — a variety of different types of compliance that can be required by industry, CSCs, etc. to meet a certain type of certification or framework.	√	√
Certification Certification	Meeting certification e.g. ISO/IEC 27001, SOC 2 [SOC 2 - SOC for Service Organizations: Trust Services Criteria - The SOC 2 is a report based on the Auditing Standards Board of the American Institute of Certified Public Accountants' (AICPA) existing Trust Services Criteria (TSC)].	— select and prepare the applicable controls for audit as some requires audit that carries over six months and is conducted by outside/third party auditors. This includes what data necessary for certification — verify the certificate is valid, and if necessary, verify that the provider maintains the required compliance	— provide the required certification by a third party that is valid within the applicable period	√	√
Authorization Authorization	Authorized cloud services, e.g. US Federal Risk and Authorization Management Program (FedRAMP)	— organizations review the authorization prior to considering the CSP's offering and services	— CSP is to provide evidence of implementing and documenting specified security control to an independent third party auditor to receive and maintain the authorization	√	
NOTE Extreme right columns suggest whether an assessment, audit or both are used – see 6.3.5.					

6.3.7 Conformity Assessment – Objectives and expectations

ISO/IEC 17000 provides terms and definitions applicable to conformity assessment. Conformity assessment (3.1.6) is the "demonstration that specified requirements are fulfilled". Conformity assessment procedures provide a means of assuring that the products, services, or systems produced or operated have the required characteristics, and that these characteristics are consistent from product to product, service to service, or system to system. Conformity assessment includes sampling and testing, inspection, supplier's declaration of conformity, certification, and management system assessment and registration. It also includes accreditation of the competence of those activities by a third party and recognition (usually by a government agency) of an accreditation program's capability. The collection of all activities that are repeatedly applied to a specified group of products, processes, services, systems, persons or bodies is referred to as a 'conformity assessment scheme 'or 'scheme' (e.g. NIST SP 2000-01).

Conformity assessment is the demonstration that specified requirements are fulfilled. Determination on how the requirements are met is made through testing, inspection, and audit, and it can be performed by the manufacturer, the purchaser or a third party. Attestation made by a manufacturer is a Suppliers Declaration of Conformity (SDOC). A third party attestation is a certification. The output is that requirements have been met but not that a product or system is secure.

Conformity assessment decisions are often based on a sample at a point in time, and surveillance activities help ensure ongoing conformity. They can include pre-market activities, such as quality checks at manufacturing plants, and post-market activities, such as sample testing and complaint resolution. Conformity assessment in the cybersecurity space is challenging, where products are being updated continuously.

Standards for Conformity Assessment are published by the ISO Committee on Conformity Assessment (CASCO) in cooperation with the IEC. They involve testing, inspection, SDOC, certification, and accreditation.

6.4 Cloud audit and trust

Cloud computing is not the typical IT infrastructure located within an users' security boundary. A cloud computing environment can be a commercial network-based computing model with resources provides from geolocation in faraway server. Every organization's computing environment and their use of cloud services are uniquely different from other organizations. The CSP manages and virtualizes physical resources and can either be providing services directly or indirectly to CSCs or CSUs.

The audit programme objectives described in ISO 19011 emphasize that the audit conducted be consistent with the audit client's strategic direction and support their management system policy and objectives. The purpose of an audit is to provide the audit client with the auditor's opinion of the specific perimeter or service, or product as presented and for which the audit programme objectives are created. The auditor's opinion enhances the degree of confidence that intended users can place in the defined specific purpose. The viability of the audit provides reasonable confidence that the audit objectives can be achieved.

The challenges described in 7.14 cover specific aspects of using cloud services whereas trust (/ confidence) is directed toward the audit as a whole. An audit of cloud services aims to meet the audit client's expectations in a demonstrable, verifiable and potentially measurable way. The audit objectives aligning to the audit plan can clearly be apparent or capable of being logically proved. The audit is dependent on as well as limited by the requester's thorough understanding and provision of information, and readily availability of information from other related parties. For example, in ISO/IEC/TR 23187 and Subclause 7.14.2, CSPs collaborate with third parties in providing critical functions that are not always transparent or known to the CSP's customers. The audit perimeter and the audit stated objectives are not necessarily covering the organization's entire system and or necessarily include a variety of specific services. It can be challenging to establish trust that the audit as a whole is verifiable and measurable.

7 Audit specifications and challenges

7.1 Overview

The audit specifications build on the consideration of the components discussed in Clause 5 and Clause 6. Stakeholders such as the audit client, auditee, and auditor will set the perimeter of the audit – how, why, where, and environment. Subclause 8.3, Figure 8 illustrates an exemplary process for auditing – identify, assess, plan, initiate, test and monitor – in which setting audit specifications can be incorporated in the planning. The planning is to determine the focus and boundary of the audit. There are many considerations that will be presented in Clause 7.

The audit specifications can be set by the CSP, by the cloud auditor, be determined by independent third party standards or be required by law. All involved parties have to have an agreed scope and set of processes, measurements, standards, and metrics for the audit.

7.2 Establishing audit scope

The extent and boundaries of an audit, and the audit scope generally includes a description of the physical and virtual-locations, functions, organizational units, activities and processes, as well as the time period covered. The scope of the audit is critical information in the audit programme that an organization set up for a specific time frame. The audit scope for each audit can be aligned with the organization's overall audit programme and objectives.

7.3 Audit risk assessment

7.3.1 General

The audit client and organization have to have a reasonable understanding of security controls and cloud computing environment in order to define the boundary for the audit and its objectives. The cloud service audit (3.2.3) typically examines a set of controls covering a variety of topics. The set of topics and the set of controls vary depending on the audit criteria. For the purpose of categorizing security controls and understanding the responsibilities, Figure 3 illustrates the responsibilities of the CSP and CSC relating to the use of cloud computing. For cloud computing, examples of control topics include:

— cloud capabilities types;

— virtualization;

— data management and storage;

— access Control, least privilege access;

— supporting infrastructure;

— governance and policies;

— encryption;

— network security.

As part of an overall cloud strategy, it is necessary to include risk management practises to support decisions in adoption of cloud computing. Assessing risk is incorporated with assessing the system compatibility for adoption of the use of cloud computing. When formulating a cloud computing strategy, organizations can begin to make calculated decisions about what they will and will not accept in order to mitigate risks associated with the adoption of cloud computing and align with the organization's risk acceptance, governance, regulatory requirements and the business mission.

7.3.2 Risk assessment of cloud computing systems and legacy or non-cloud computing system

An audit or assessment is to provide evidence that aligns with the auditee's prescribed objectives are met. This can involve in understanding the integration of the auditee's on-premises system that includes a legacy system. The legacy systems can be an older, if not outdated system or application. It can be due to lack of support or that it is no longer support the needs of a business or an organization. The legacy systems are generally not created for the use in the cloud computing environment and as a consequence cannot be easily lifted and dropped into the cloud computing environment. There are challenges for the legacy systems to meet the compliance associated in the adoption and use of the cloud service. A strategy can be carefully crafted to determine how best to migrate the legacy systems securely to the cloud computing environment.

In another word, a legacy system can be part of a non-cloud computing system. A non-cloud system can be a system housed internally that can include applications installed within in-house servers and mainframes and IT infrastructure behind its firewall. This system allows the organization to maintain the control to meet certain compliance while security remains challenging when incorporating in a cloud computing environment. A non-cloud computing system built for use within an internal IT infrastructure faces the similar challenges described above for the legacy one.

7.4 Security controls assessment

Standards that provide information relating to security controls assessment include ISO/IEC 27002, ISO/IEC 27007, ISO/IEC TS 27008, ISO/IEC 27017, and ISO 19011. ISO/IEC 27017 gives guidelines for information security controls applicable to the provision and use of cloud services and includes additional controls with implementation guidance specifically relate to cloud services and additional implementation guidance for relevant controls specified in ISO/IEC 27002. ISO/IEC 27007 provides guidance on managing an information security management system (ISMS) audit programme, on conducting audits, and on the competence of ISMS auditors, in addition to the guidance contained in ISO 19011. ISO/IEC TS 27008:2019, Annex C provides guidance on audit procedures for ISO/IEC 27017 technical controls.

The auditor assesses security controls of both the CSC and the CSP. The CSC or the audit client cannot assume to inherit the CSP's security controls. The following are some key considerations:

a) The CSP's security authorization package can include a list of controls that are expected to be implemented by the CSC. CSCs are to review this list, consider the context in which they are using the cloud services and prepare a list of security controls that are the full or partial responsibility of the CSC. Cloud auditor reviews the CSC's responsibility matrix to validate it against the CSP's security authorization package and focus on the audit of the controls that are identified as the CSC's responsibility.

b) Auditors pay special attention to the "configurations" of the CSC's cloud services and audit these configurations for security. These configurations are associated with the options that CSPs offer to configure security to meet the needs of the CSCs. However, in order to activate these options, the CSC can configure the system appropriately. They can be managed by the CSC in accordance with the configuration management family of controls.

c) Auditors pay special attention to the techniques used for user authentication and the assurance level of the digital identities. Every user of a cloud system is a "remote" user authenticating over a shared medium, for example, the use of multi-factor authentication mechanisms leveraging digital identity credentials with assurance commensurate with the criticality of the cloud application.

d) Auditors pay special attention to the handling and storage of PII or other sensitive data in cloud services. Depending on governance and jurisdiction, the management of data is in commensurate with the risk of exposure of data. For example, for highly sensitive data, it is recommended that the encryption keys are not to be managed by the CSP who is also providing the storage service.

e) Auditors review how the CSC's contingency plan is affected by or is integrated with the use of cloud computing giving consideration to organizational policies and regulatory requirements.

An incident response plan including basic processes and understanding escalation procedures, is particularly crucial for the CSC when a cloud computing system is involved.

7.5 Required laws, regulations, and government requirements

Compliance is not simply meeting the requirements, but when compliance is applied correctly, it is instrumental to the long-term success of any organization.

The organization's leadership determines how to sustain the culture and behavior of compliance, and adopt an effective, organization-wide compliance management system to meet the organization 's obligations, and the needs and expectations of its stakeholders. ISO 37031 presents a compliance management system that is based on the continual improvement principle.

Audits can also be required to verify compliance with general regulations especially when processing PII is involved, for example:

— privacy [e.g. GDPR, HIPAA, LGPD, CPRA (California Privacy Rights Act)];

  data transfer and data protection [GDPR – Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs)]

— industry specific regulations [e.g. financial services and banking regulations – AICPA (American Institute of Certified Public Accountants), and Payment Card Industry Data Security Standard (PCI DSS)];

— sectors [e.g. health information (US Health Insurance Portability and Accountability Act of 1996) ("HIPAA")];

— governments (e.g. GDPR, LPPD, HSPD-12[1)], FISMA[2)], LGPD);

— regulatory [e.g. Payment Card Industry Data Security Standard, HIPAA, EU (European Union) Data Protection directive, pharmaceutical].

Many CSPs are under continuous audit for security compliance including, for example, the Payment Card Industry (PCI) or ISO/IEC 27001:2013. CSC benefits by inheriting the compliance of their cloud services but are still responsible for their configurations and utilization of the cloud services. CSPs have statements of applicability and downloadable audit reports. In general, auditors can map the CSPs prior attestations to the cloud services that the CSC are being audited against. Although it is the duty of the CSC to implement security best practices, CSPs build in security controls to protect their platforms. This is because the CSPs maintain large-scale data centers and are under continuous audit. Physical access to the CSPs' data centers is not necessary at the CSC level as the CSCs can leverage the physical security attestations from their CSPs.

In meeting the demand and expectations of the consumers and marketplace, technology and changing landscape evolve separately in different spaces and directions demand updates to regulations. For example, the US Health Insurance Portability and Accountability Act (HIPAA) applicable to just the patient information flowing through the healthcare system and not generally to personal health data. New technologies and a greater awareness of public health after a pandemic can also fundamentally change conception of health privacy, making it less about keeping information private than controlling how it is used. There is a critical necessity to understand how an organization uses its data and the technology interfaces between many components such as devices, networks and ecosystems, and to apply the appropriate controls not only to satisfy the existing laws and regulations but also to assess and analyse the information for better understanding of potential risks.

1) Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors

2) The Federal Information Security Modernization Act of 2014 (FISMA 2014) updates the Federal Government's cybersecurity practices

7.6 Policies

7.6.1 General

Each organization establishes various policies to support, for example, its organizational goals, trans-border data flows, data protection, privacy, risk management, incident response, identity, access management, and its use of cloud service(s), i.e. cloud policy. An audit can involve assessing monitoring and testing the effectiveness of the policies.

The design of policies can determine the approaches for global business baseline requirements differ from its domestic and local ones. The policies can be used to evaluate whether the compliance programme is aligned with the legal and regulatory standards. Standards and frameworks are often referenced in support of policies or cited as baseline. In cloud computing environment, considerations are driven by understanding the organization data usage – where, how and who are accessing and using it, to designing the policies. The audit can assess the policies and reinforce or counteract other policies.

Policy approaches include, for example:

— "Privacy by Design" which is included in the General Data Protection Regulation (GDPR), that the current approach in the data protection guidelines, which requires persons responsible to include definitions of the means for processing technical and organizational measures at the time that they are defined in order to fulfil the basics and requirements of "Privacy by Design".

— Binding corporate rules (BCR) are data protection policies adhered to by companies in the EU for transfers of personal data outside the EU within a group of undertakings or enterprises.

7.6.2 Geolocation data

Several countries are challenged with a requirement for assessing and authorizing cloud service products for usage in government and within some industry sector (e.g. energy, financial). The volume and backlog quickly become overwhelming, within a specific geo-jurisdiction assessment and authorization context. This is especially true for PaaS and SaaS cloud service products with thousands of potential cloud service products. Globally, cloud service products are not only trusted but it would gain significant economic benefits if they are also mutually recognized. International standards will be at the core to foster mutual recognition (authorization) of specific cloud service products across multiple geo-jurisdictions.

Control and management of data locality serve to satisfy government regulations such as those pertinent to data security. This includes using cloud service to repatriate sensitive data from cloud platform and hold it on-premises if needed.

7.7 Cloud service agreement (CSA)

The CSA can prescribe terms relating to the audit of the CSP and possibly of the CSC. The primary CSPs can exercise similar agreements with its secondary CSPs. The cloud SLA ordinarily contains a collection of SLOs and SQOs relating to the cloud service, covering aspects of the service. This can include availability, reliability, performance, security, data protection, compliance and data handling. It differs from an SLA for services hosted internally as it includes objective measurement defined for level of service being provided in the cloud computing environment. The cloud SLA can include description of the methods that CSPs can use to demonstrate compliance to regulatory standards for the use of cloud services. Listing of standards, policies and regulations together with list of audits and CSC auditing activities are exemplary document for inclusion in the cloud SLA. ISO/IEC 19086-1 describes the overview, foundational concepts, and definitions for the cloud SLA framework. ISO/IEC 19086-1:2016, Clause 10 provides the cloud service level objective (SLO), cloud service qualitative objective (SQO) to measure the commitment to ten pertinent SLA content areas, namely information security, performance, availability, accessibility, cloud service support, termination of service, governance, service changes, service reliability, attestations certifications, data management, and PII protection.

7.8 Cloud capabilities types, cloud service categories and key characteristics

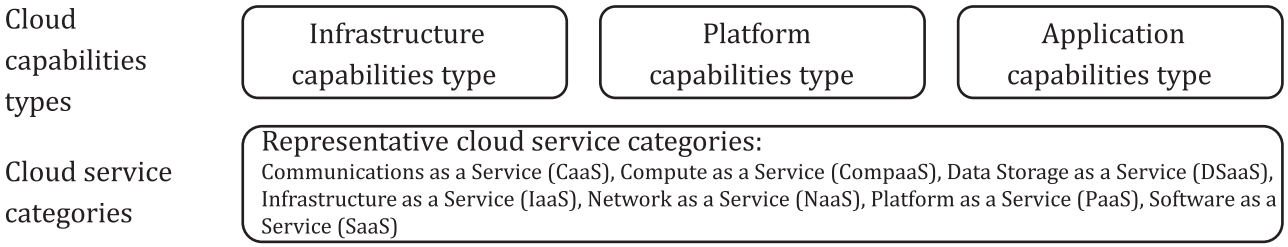

Figure 5 — Cloud capabilities types and cloud service categories

In conducting an audit of cloud service, it is essential to understand how to set the audit specifications in relation to cloud capabilities types and cloud service categories (see Figure 5):

— characteristics of capabilities types and cloud service categories;

Every capabilities type and cloud service category have different characteristics and offer different benefits and limitations, but also risks. As shown in Figure 3, responsibilities are assigned differently to CSCs and CSPs. When CSCs use more than one service provided by different CSPs, the audit matrix and definition are defined for internal and external audit.

— matching and transitioning workload and platform;

It is necessary to see the workload from top down and appropriate approaches to legacy dependency. This includes reviewing profile, version used, function in current environment alignment, managing sharing and securing data across multiple CSPs and cloud capabilities types. The incorporation of various technology such as containers environment and automation across various cloud computing platforms.

— viability of legacy system;

It is relevant to manage the data model and viability to access every representation on every piece of data in the legacy system. This includes managing APIs and portfolio to maintain collaboration and integration between legacy and cloud system.

— importance of cloud management sensitivity;

Managing who has access to what and with which privileges is a real challenge in the cloud environment due to rapid change and large scale. In understanding where are the CSC's users, consumers and employees will help to determining audit boundary, security sensitivity and gaps, and connectivity.

— matching worker skills to the business application;

The consideration is tied to roles and responsibilities in managing credential, governance and compliance in the use of the cloud capabilities types and cloud service categories. Cloud security is a journey not a destination. Business mission and needs, organizational culture and people's skills are influential for this journey. IT and security teams are enabled to control cloud access and to provide 360-visibility across the enterprise and cloud infrastructure in order to add a critical layer of security and governance.

— understand the key characteristics of cloud computing in setting audit specifications;

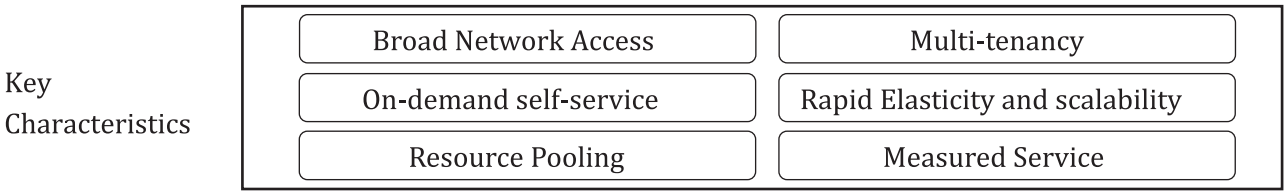

Figure 6 — Key characteristics of cloud computing

These characteristics as shown in Figure 6, are identified as key features and benefits in the use of cloud computing, and they are not necessarily apparent in totality in every environment. Understanding these characteristics helps to identify and verify the appropriate security and risk management that is part of the audit scope. For example, scalability can be impacted when using services that are built upon another CSP.

— managing changes and working with partners (see 7.15.2);

A process can be in place for monitoring and implementing 1) maintenance and versioning, e.g. an automated security assessment [27], a change management plan, and incorporated in the CSA or cloud SLA (ISO/IEC 19086-1:2016, 7.5, 10.10).

— hybrid cloud and multiple CSPs;

Hybrid cloud as defined in ISO/IEC 22123-1 as a cloud deployment model that involves using at least two different cloud deployment models. Many organizations will have a private cloud located on-premises which can be owned and operated by the organization or hosted on-premises by a CSP. These organizations can use public cloud located off-premises. These two separate cloud services can be provided by two different CSPs.

The audit specification in considering cloud service capabilities includes the access points to each cloud service. The visibilities to the services, setting up appropriate metrics and in meeting compliance. In meeting both compliance requirements and the challenge of visibilities, it would be critical to have the capabilities to integrate application, data, cloud-native as well as many business-to-business functions.

Examples include:

- access control - access relationships, patterns and improve the application of access controls; enforce access to cloud infrastructure with predefined policies;
- visibility;
- meeting compliance (many native/custom tools do not support the use of more than one cloud services);
- setting appropriate metrics;
- respond to changes and updates;
- change and network behavior;
- integration of multiple cloud services (cloud management, identity management, security platform management);

— shared security and visibility.

Figure 3 illustrates the shared responsibilities between CSPs and CSCs depending on the use of cloud service models. While three main roles and sub-roles are included in ISO/IEC 17789 as shown in Figure 2, it is possible that the sharing of responsibilities can involve multiple other parties that are described in many documents for example, cloud platform integrator or broker, software development companies for the applications running on top of cloud services, different DevOps teams and other stakeholders.

Figure 3 is only an illustration of how responsibilities are split or shared between providers and users of the cloud services using different cloud capabilities types, i.e. infrastructure capabilities type, application capabilities type and platform capabilities type. In many cases cloud developers can design seamless movement between capabilities types. When auditing such environment, it is not easy categorized separate services to capabilities types.

7.9 Cross-cutting aspects

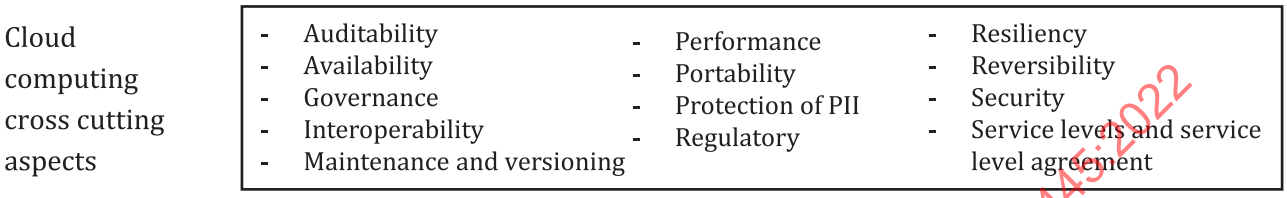

Figure 7 — Cloud computing cross cutting aspects

Cloud computing is becoming the conduit for many technologies like robotic process automation, artificial intelligence, data analytics, and the Internet of Things (IoT). It is also facilitating the fundamental changes in the way people work, extending opportunities to access data remotely and enhancing collaboration throughout organizations from many locations. Across continents, organizations seek to maximize the benefits of cloud computing cross cutting aspects for connectivity, business growth and for the possibilities.

There are challenges and ISO/IEC 19941 highlighted the issues for interoperability and portability in cloud computing that involve interactions affected by technological, information and human aspects. The challenges are likely to intensify and become more difficult to manage as systems grow more complex and interconnected. In cloud computing environments with internationally interconnected systems, the complexities also include matters of corporate policy, regulation and international law (see Figure 7). An audit scope will need to recognize and reconcile these challenges within the perimeter of multi-connected environment.

7.10 Emerging technologies and cloud native

As the use of cloud computing is expanding its influence and becoming more agile, offerings and collaboration between roles is responding to demands. These motivate many different approaches to handle workloads. When deploying an application into the cloud environment, organizations have to deal with a wide range of resources at different levels of functionality among available cloud solutions. Examples for auditor consideration include to:

— understand that traditional approaches cannot meet the demands of edge computing;

— align cloud strategy with the use of more than one cloud services and CSPs;

— align cloud strategy with the incorporation of artificial intelligence and edge computing;

— understand how data compute;

— align perception of security and privacy to address users, process and technology factors;

— assess effectiveness of the use of any emerging technologies in term of accuracy and completeness with which users achieve specified goals;

— assess efficiency in view of resources used in relation to the expected results;

— assess virtualization risks;

— assess identity management risks;

— assess the risk of misconfiguration;

— assess dependencies considerations and cross functional cloud governance.

ISO/IEC TS 23167 discusses a set of common technologies and techniques used in conjunction with cloud computing. These include virtual machines (VMs) and hypervisors, containers and container management systems, serverless computing, microservices architecture, automation, platform as a service systems and architecture, storage services, security, scalability and networking as applied to the cloud computing technologies. The CSC often uses these common technologies with the cloud service(s). The cloud native applications are coupled to virtualization and the control and management of virtualized resources. It is prudent to have a full and complete understanding how the technologies contribute and integrate with the cloud computing environment. This understanding is assessed as part of the law, policies and governance for use of emerging technologies.

The potential challenges that the cloud service developers misaligning security and the framework used by the CSC. In developing the applications to incorporate the technologies in the cloud service, the cloud auditor is to gain visibility to resources so as to assess what is deployed, identify the cloud native application, and apply the appropriate risk profit to locate any misalignment or gaps in security.

7.11 Define metrics and security parameters

In defining metrics include discussing the parties and identifying scenarios and the roles they play in the usage metrics and implementing information security measures. The CSCs in using the cloud services prepare to understand the metrics used for service quality and other assurances described in the cloud SLAs. The cloud service business manager, for example, exercises this understanding in performing business administration activity as described in ISO/IEC 17789. The CSPs' activities are driven in providing cloud services and necessitate the use of metrics to measure service level objectives (SLOs) and service qualitative objectives (SQOs). The cloud auditor in carrying out the activities of the audit of the provision and use of cloud services, use a common and unambiguous representation of metrics to provide details of the measurements performed. Apart from the CSPs, CSCs and CSNs, other roles such as regulators and policy makers establish their parameters and associated metrics about cloud service usage.

Metric is defined in ISO/IEC 22123-1 as a standard of measurement that defines the conditions and the rules for performing the measurement and for understanding the results of a measurement. ISO/IEC 19086-2 is scoped specifically to define a model for specifying metrics for Cloud Service Level Agreements (Cloud SLAs). As described in the definition, metric is focused on something that is intended or needed to measure, the data supporting the measures needs to be readily obtainable and thereby the measures to yield quantifiable information.

The metric definition describes what and how this "something" is to be measured and tracked. In developing metric definition depends on the intended users, the intended purpose and how the metric will be used. The metric definition designs to be logical and specific, comparable, and applicable. Establishing metrics and metric definition can be incorporated with the planning of the cloud service audit (3.2.3). Depending on the purpose of the audit, the metric definition can be used by different parties including CSPs, CSCs, and CSNs. As illustrated in ISO/IEC 19086-2:2018, Figure 1, a well-defined metric definition helps to ease any confusion when comparing and evaluating metrics.

Much efforts are preoccupied in selecting controls within the process of implementing an Information Security Management System (ISMS) as represented in ISO/IEC 27002. Information security measures are necessitated in assisting decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. They provide the means for bridging the implementation, efficiency, and effectiveness of security controls to an organization's success in its business mission activities.

If an organization strategizes uses a framework such as the NIST Cybersecurity Framework in defining controls and formulating requirements, metrics based on the framework as a standard measurement helps to formulate relevant, measurable and thereby verifiable. The ISO/IEC 19086 series uses the differentiation of cloud service level objective (SLO) and cloud service qualitative objective (SQO) whereby SLO has quantitative characteristic of a cloud service and SQO has qualitative characteristic of a cloud service. It is not only necessary for the auditor to understand the cloud computing environment

in formulating the metrics to closely applicable to the controls, but the auditor is to ascertain whether the metrics are applicable to manual, semi-automated or automated (continuously) assessment. Metrics designed for traditional manual assessment will not be helpful measurement for use with automated assessment.

7.12 Determining matrix

Matrix brings together gathering of data representation and data collection to cultivate metrics. Subclause 7.12 discusses defining metrics and security parameters, and they are one of many components feeding into any audit programme. The building blocks of a matrix develop a comprehensive list of risks (internal and external) that potentially have a negative impact on the organization, along with the controls in place to defend against those risks.

This clause discusses specifically on matrix for specification of audit and emphasizing the importance of determining meaningful measures of effectiveness and impact on the use of the cloud service. Effectiveness in relation to accuracy and completeness with which users of the cloud service achieve specified goals. The audit specification addresses the infrastructure, process and technologies, but also factoring in the human factor or behaviour in the cloud computing environment.

7.13 Assessment of cloud governance

ISO/IEC 38500 defines governance of IT as a subset or domain of organizational governance, or in the case of a corporation, corporate governance and to promote effective, efficient, and acceptable use of IT in all organizations, whereby organization is defined as person or group of people that has its own functions with responsibilities, authorities, and relationships to achieve its objectives. Governance for a cloud computing environment is different from governance for a traditional organization, and involves different cloud deployment models, roles and responsibilities. This creates complexities in governance as highlighted in 7.5, 7.14, 7.3, Security controls assessment, Figure 2, and Figure 3.

A CSC is responsible in attaining compliance to regulatory standards for the use of cloud services. While a CSP chooses to perform certain audits or obtain certification(s) for a cloud service, this does not necessarily ensure end-to-end regulatory compliance for CSCs (see ISO/IEC 19086-1:2016, 10.9).

NOTE Useful references related to governance: ISACA - COBIT - A Business Framework for the Governance and Management of Enterprise IT, and ISO/IEC 27014.

7.14 Challenges of conducting an audit of cloud services

7.14.1 General

There are some potential challenges when conducting an audit of cloud services. Major challenges of cloud audit are often alluded to visibility, accountability and transparency, and the following are examples of contributing factors.

7.14.2 Third party auditability

A CSC can be using a cloud service from a CSP that includes application such as word processing app from a third party. This app provider will issue certification on the app for vendor assurance. The CSC will not be able to audit the app. The CSPs and CSCs share responsibilities and control of resources in cloud service system. The CSC continues to maintain level of certification.

7.14.3 Change management

The challenge of managing and meeting the pace of changes has increased in complexity and risk to processes across organization and involve multiple systems and locations. Additional complexities exist for some organizations where the enterprises are not standardized across various CSPs, and cloud services are not aligned with on-premises operation. The assessment inspects evidence to

confirm that changes are defined and documented, approved for development, tested, and approved for implementation.

7.14.4 Patch management

In a traditional IT environment, patch management is focused within the perimeter of operating systems, servers, third party apps and legacy applications, and includes every endpoint, e.g. workstations, laptops, servers, devices and more. In a cloud computing environment, the boundary is harder to define e.g. employees connecting remotely on multiple devices. The challenge of monitoring patch management increases with consideration of cloud deployment models, cloud services and different applications and CSPs albeit in certain scenarios, patching is the responsibilities of CSPs.

7.14.5 Multi-tenant environment

As explained eloquently in ISO/IEC 22678:2019, 6.4.7, that since cloud resources such as computers, storage, and networks are pooled resources shared by many CSCs and/or tenants, commercial auditors or government inspectors are not given physical access to equipment specific to one CSC without potentially violating the confidentiality of other CSCs using the same pooled resource. Some data can be spread across multiple shared storage resources using "sharding". ISO/IEC 22678:2019, 8.1.2 further expands on issues relating to formulating policies for multi-tenancy environment.

7.14.6 Auditability and assurance

Auditability is essentially an important part of conducting audit. It is concerned with the capability of collecting and making available necessary evidential information related to the operation and use of a cloud service. Any issues with achieving the capability jeopardize the objectives of an audit. Audits are generally performed to verify that processes and systems meet requirements (e.g. requirements of a standard), and thereby to provide assurance that such processes and systems are operating to meet expectations (typically expectations of a governing body or of senior management).

As a rule, an audit of cloud service or services is not much different from an audit of traditional IT system. The approach is often viewed as an extension as demonstrated in several documents e.g. ISO/IEC 27017 where additional controls with implementation guidance that specifically relate to cloud services are extended from documents covering IT system or ISMS. Cloud computing offers substantial benefits and much more as seen in the definition, "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" (ISO/IEC 22123-1). The key characteristics and cross cutting aspects as shown in Figure 2 are testament to its offerings, but it also leads to a complicated view beyond the traditional boundary. The paradigm introduces differences to traditional network and includes dependencies on third party infrastructure. CSPs generally do not provide access to their controls and environments, e.g. multi-tenant environments and data centres. Thus, auditability is not only necessary but essential in building trust with verification and assurance.

7.14.7 Availability requirement

In balancing the three key considerations for information security – confidentiality, integrity, and availability, users of cloud services determine the acceptable solutions to focus on prioritizing the considerations and the business impact. This will help in formulating the requirements, definition and measurement for the organization and CSPs in making the data and services available. An audit evaluates the controls around the information with respect to confidentiality, integrity, and availability. One of the key concerns in auditing, IT and cloud systems, is the availability of resources and expertise to perform the audit in considering the diverse CSPs, cloud services and cloud computing environment.

8 Approaches to conducting audits

8.1 Typical Scenarios

Table 4 presents typical scenarios for the use of cloud services and possible areas for assessment in an audit.

Table 4 — Typical scenarios of audit of cloud services

Organizations of all types and sizes	CSC	CSP
Considering and planning cloud strategy	— initiate an internal assessment of system – capabilities, risk profiles, assess data protection, identify management — assess cloud service models and plan on how to achieve benefits of cloud characteristics — review and evaluate cloud service providers and their offerings	— assess CSPs and align their availabilities, capabilities and functionalities in meeting business mission and goals. — request or assess publicly available compliance reports — review CSPs offerings and other associated services
Considering continuing monitoring security posture, CSPs offerings and considering future business needs	— assess audit objective evidence against CSA or cloud SLA, and identify vulnerabilities and necessary improvement — assess configuration, security and log of additional virtualization	— assess any unauthorized access to CSC's data by third parties — assess separation of perimeter in a multi-tenant cloud computing environment
Expanding to add more cloud computing solutions, continuing their cloud strategy journey while aligning cloud strategy with data storage, financial, IT security, etc. or assess current use of cloud computing strategically.	— assess governance in monitoring cloud services from multiple CSPs — assess managing connectivity security — assess the value of moving selected services to the cloud computing environment — assess control of sensitive data — assess how to protect data from tampering with the use of multiple cloud services and multiple CSPs	— assess security and privacy compliance from different CSPs — assess control of sensitive data

8.2 Cloud audit – opportunities and meeting objectives

8.2.1 General

An internet search on audit is generally directed to an official and independent examination of an individual's or organization's financial account and statements. The audit opinion is intended to provide reasonable but not an absolute assurance, and the audit is designed to give a true and fair view based on compliance to standards and the financial reporting framework. This presents a certain assurance and understanding of the information risk.

As organizations are using information systems and processing information in digital form, the objectivity of conducting systematic, independent and documented audit process remains unchanged but review and examination of objective evidence in meeting the audit criteria is based on information generated from the information systems in real time. An audit, either it is a financial audit or an

ISMS audit, adds credibility to an organization's implied affirmation of its representation and overall performance. An ISMS audit of an organization based on the use of cloud computing system conducted against a range of audit criteria as described in ISO 19011:2018. ISO 19011:2018, 5.3 identifies risks and opportunities that it is necessary for the cloud auditor to communicate to the audit client so that they can be addressed appropriately.

Before an organization can explore the opportunities harvested from an assessment and audit, the audit scope for each audit can be aligned with the organization's overall audit programme and objectives. The information put forward to define the audit scope and objectives, advocates the careful selection from many frameworks, standards, controls, and certification and helps the organizations to clarify the governance for data security, how responsibilities are shared, and the organization's risk appetite or avoidance. Depending on the cloud services and whether the services are utilising shared resources with other customers, any testing, scans and audit can be coordinated with prior authorisation from the CSPs and related suppliers. The audit client in setting the audit perimeter and controls is to consider the inter-relationship between roles, components and departments.

The audit programme objectives direct the planning and conducting of audits and ensure the audit programme is implemented effectively. Clause 7 expands on audit specifications, e.g. scope (7.2), challenges (7.15), metrics (7.12), and governance (7.14).

8.2.2 Stakeholders and related activities on cloud audit

The audit client, which can be either the CSP or the CSC, is responsible for defining the audit programme objectives. The audit of the provision and use of the cloud services is planned and conducted according to the objectives defined by the cloud auditor. The assessor or auditor is to work with cloud service developer in reviewing and identifying any unknown software deviation, create a baseline for comparison, and for following-up on potential misconfigurations or, misalignment across security controls, routine upgrades, and maintenance operations.

Clause 5.2.4 discusses relationship and interaction between cloud auditor with CSPs, CSCs, and CSNs and Clause 5.2.3 discusses the responsibilities of a cloud auditor. These roles and activities are related to performing assessment and audit. There are principal stakeholders of the organization, suppliers, regulators, senior management, employees and customers who provide relevant contributions to the audit process while they are not directly performing the audit – see exemplary scenarios 8.1 and various processes 6.2. An audit of an organization's ISMS and cloud computing system focuses on information system and also presents a certain assurance and understanding of the information risk.

8.3 Processes – identify, analyse, evaluate

Process is a critical component of an audit. It defines a set of interrelated or interacting activities that use inputs to deliver an intended result of an audit. Figure 8 illustrates an example of an audit process for internal and external audits, and ISO 19011:2018 Figure 1 illustrates the process flow for the management of an audit programme. It exemplifies the steps can be duplicated for either an internal or external audit albeit the purpose and roles can deviate. Once an audit process is set, it is important to adhere and document it faithfully to ensure the audit is completed properly with consistent audit quality, to provide effective communication of audit expectations, to use defined activities for automating repetitive tasks effectively, and mitigate risks.

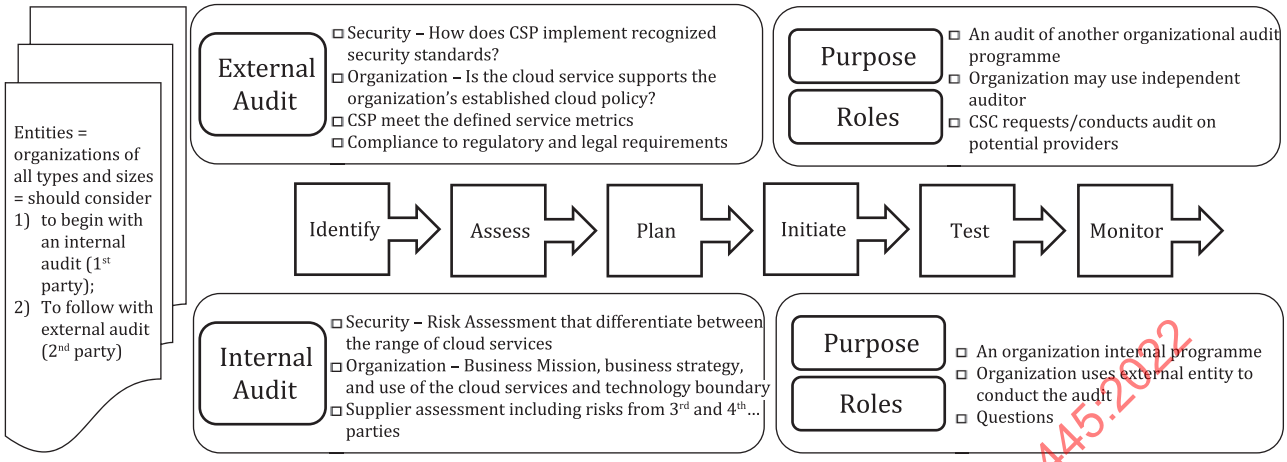

Figure 8 — Example of audit process

8.4 Data flow – lifecycle - confidentiality, integrity, availability

In cloud computing, a CSC can also be a data owner who stores on cloud service servers where users can access the data any time and from any place. This can lead to data outsourcing in vast amount on cloud service system. This increases security challenges for data integrity, authenticity and confidentiality.

It is important for organizations as data holders to be able to control the use and disclosure of personal information. One of the first steps is to categorize the data and to have proper data retention policies or processes. Another step is to determine user access rights to data and user provisioning can be automated or manual depending on the use of the type of cloud services. Standards provide pertinent guidance in implementing the processes and governance. ISO/IEC 19944-1:2020 elaborates on data categories and data identification qualifiers as a mean to address transparency in acquisition, processing, and use of the data in the use of cloud services.

It is possible to have a public auditability as to allow Third party auditor to verify the correctness of the cloud data. Privacy preserving as well as security are to be considered and incorporated in the audit for data storage security and data integrity.

8.5 Automation of cloud service audits and assessments

Organizations have audit and assessment management programs of varying scopes and complexity that require significant resources. An organization's compliance program can include evaluation of audit and assessment control requirements, objectives, scope, risk, identification of applicable application and system owners, evidence collection, and remediation plans. For many organizations, the audit and assessment of such a complex control environment is manual, particularly in the evidence collection, assessment of control requirements, and objective satisfaction. Managing audit and assessment processes manually can increase the risk of errors and omissions due to human error. Furthermore, audit of a conventional IT system is significantly adapted to the cloud computing environment. For instance, constant changes in the use of cloud services necessitate the need to automatically collect data to present near real-time visibility on compliance. Automating compliance program processes improves the efficiency and efficacy of audits and assessments by reducing the required resources, improving accuracy, and providing near real-time control and environment statuses.

Automating evidence collection, assessment of control requirements and objective satisfaction can be achieved by implementing an automated assessment system. An automated assessment system collects and compares machine-readable desired state specifications (i.e. the control objective) with machine-readable actual state assessment objects (i.e. evidence) and reports the statuses and findings to a collection system. The collection system collects data, defects, and inventory of controls and displays reports, statuses, and summaries to a dashboard [27].

With the statuses and findings automatically and continuously reported to a single collection system dashboard, an organization can identify defects quickly and report on the status of control requirement and objective satisfaction in near real-time. This status can be used to accelerate the review of an auditor or assessor, improving the efficiency of CSP, CSC, and CSN audit and assessment processes.

Annex A
(informative)

Sample list of standards and frameworks applicable to audit of cloud services

A.1 Standards supporting the audit of cloud services

Table A.1 includes a sample list of published documents addressing audit, management system auditing, and guidance on audit and certification but not necessarily be specific to cloud service audit (3.2.3). The following documents can also be used for individuals/organizations managing the audit programme and not necessarily focused on the cloud computing roles and sub-roles.

Table A.1 — International Standards relating to audit

Document No.	Description in relation to audit	Audit in General	Privacy	Security
ISO/IEC 15408 Series (Common Criteria)	— ISO/IEC 15408-1 establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of ISO/IEC 15408 which in its entirety is meant to be used as the basis for evaluation of security properties of IT products — ISO/IEC 15408-2 defines the required structure and content of security functional components for the purpose of security evaluation — ISO/IEC 15408-3 defines the assurance requirements of the evaluation criteria — ISO/IEC 15408-4, Framework for the specification of evaluation methods and activities	√		√
ISO/IEC 17021-1	— contains principles and requirements for the competence, consistency and impartiality of bodies providing audit and certification of all types of management systems	√		
ISO 19011	— provides guidance on auditing management systems, including the principles of auditing, managing an audit programme and conducting management system audits — concentrates on internal audits (first party) and audits conducted by organizations on their external providers and other external interested parties (second party)	√	√	
ISO/IEC 27002	— gives guidelines for organizational information security standards and information security management practises including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s)			√
ISO/IEC 27006	— specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS)	√		
ISO/IEC 27007	— provides guidance on managing an information security management system (ISMS) audit programme, on conducting audits, and on the competence of ISMS auditors, in addition to the guidance contained in ISO 19011	√		

Table A.1 *(continued)*

Document No.	Description in relation to audit	Audit in General	Privacy	Security
ISO/IEC TS 27008	— provides guidance on reviewing an organization's information security controls, e.g. in the organization, business processes and system environment, including technical assessment — offers guidance on how to review and assess information security controls being managed through an Information Security Management System specified by ISO/IEC 27001	√		√
ISO/IEC 27009	— defines the requirements for the use of ISO/IEC 27001 in any specific sector (field, application area or market sector). It explains how to include requirements additional to those in ISO/IEC 27001, how to refine any of the ISO/IEC 27001 requirements, and how to include controls or control sets in addition to ISO/IEC 27001:2013, Annex A	√		√
ISO/IEC 27017	— gives guidelines for information security controls applicable to the provision and use of cloud services by providing: — additional implementation guidance for relevant controls specified in ISO/IEC 27002; — additional controls with implementation guidance that specifically relate to cloud services. — provides controls and implementation guidance for both CSPs and CSCs	√		√
ISO/IEC 27018	— establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment — specifies guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of PII which can be applicable within the context of the information security risk environment(s) of a provider of public cloud services		√	
ISO/IEC 27006-2	— specifies requirements and provides guidance for bodies providing audit and certification of a privacy information management system (PIMS) according to ISO/IEC 27701 in combination with ISO/IEC 27001, in addition to the requirements contained within ISO/IEC 27006 and ISO/IEC 27701. It is primarily intended to support the accreditation of certification bodies providing PIMS certification		√	
ISO/IEC 27701	— specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization — specifies PIMS-related requirements and provides guidance for PII controllers and PII processors holding responsibility and accountability for PII processing		√	

A.2 Available frameworks for audit schemes, certification, and authorization

Frameworks can complement or contribute to an assessment and audit. They can be a good tool to layout risk management, priorities, security constraints, risk tolerances, and assumptions that are established and used to support operation risk decisions. Establishing and maintaining a mapping to one or more frameworks involves organization's resources and time and careful determination on the applicable framework(s) that best serve the business function and organization's system. Frameworks can be considered a good complementary tool but cannot be considered as an assurance or guarantee