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)

Documents
Document Sharing Hub
© ISO/IEC 2022

Full document details: ISO_IEC TR 3445_2022

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2022

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Published in Switzerland

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC TR 3445_2022

Contents

Page

Foreword ... **v**

Introduction ... **vi**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**
3.1 Terms related to the use of audit and assessment ... 1
3.2 Terms related to cloud service audit ... 3

4 Abbreviated terms ... **5**

5 Overview of cloud computing and the activities of a cloud auditor ... **5**
5.1 Overview of cloud computing ... 5
5.1.1 General ... 5
5.1.2 Cloud computing roles, sub-roles and activities ... 6
5.2 Overview of the activities of a cloud auditor ... 7
5.2.1 Cloud auditor ... 7
5.2.2 Responsibilities of a cloud auditor ... 8
5.2.3 Cloud auditor's cloud computing activities ... 9
5.2.4 Relationship of the cloud auditor to CSPs, CSCs, and other CSNs ... 10

6 Overview of the audit of cloud services ... **10**
6.1 General ... 10
6.2 Objectives of an audit of cloud service ... 11
6.2.1 General ... 11
6.2.2 Audit objectives ... 11
6.2.3 Audit boundaries ... 13
6.2.4 Relationship of an audit and the organization ... 13
6.3 Types of cloud audit ... 15
6.3.1 Overview ... 15
6.3.2 Internal audit ... 15
6.3.3 External audit ... 16
6.3.4 Exemplary tests and audits ... 17
6.3.5 Relationship between audit and assessment for cloud computing ... 19
6.3.6 Relationships among audit processes and reports ... 19
6.3.7 Conformity Assessment – Objectives and expectations ... 24
6.4 Cloud audit and trust ... 24

7 Audit specifications and challenges ... **25**
7.1 Overview ... 25
7.2 Establishing audit scope ... 25
7.3 Audit risk assessment ... 25
7.3.1 General ... 25
7.3.2 Risk assessment of cloud computing systems and legacy or non-cloud computing system ... 26
7.4 Security controls assessment ... 26
7.5 Required laws, regulations, and government requirements ... 27
7.6 Policies ... 28
7.6.1 General ... 28
7.6.2 Geolocation data ... 28
7.7 Cloud service agreement (CSA) ... 28
7.8 Cloud capabilities types, cloud service categories and key characteristics ... 29
7.9 Cross-cutting aspects ... 31
7.10 Emerging technologies and cloud native ... 31
7.11 Define metrics and security parameters ... 32
7.12 Determining matrix ... 33
7.13 Assessment of cloud governance ... 33

Documents
Document Sharing Hub

© ISO/IEC 2022 – All rights reserved

Full document details: ISO_IEC TR 3445_2022

7.14 Challenges of conducting an audit of cloud services ... 33
7.14.1 General ... 33
7.14.2 Third party auditability ... 33
7.14.3 Change management ... 33
7.14.4 Patch management ... 34
7.14.5 Multi-tenant environment ... 34
7.14.6 Auditability and assurance ... 34
7.14.7 Availability requirement ... 34

8 Approaches to conducting audits ... 35
8.1 Typical Scenarios ... 35
8.2 Cloud audit – opportunities and meeting objectives ... 35
8.2.1 General ... 35
8.2.2 Stakeholders and related activities on cloud audit ... 36
8.3 Processes – identify, analyse, evaluate ... 36
8.4 Data flow – lifecycle - confidentiality, integrity, availability ... 37
8.5 Automation of cloud service audits and assessments ... 37

Annex A (informative) **Sample list of standards and frameworks applicable to audit of cloud services ... 39**

Annex B (informative) **Compilation of frameworks, schemes, and auditing programs for certification, attestation and authorization which are relevant to cloud security ... 44**

Bibliography ... 49

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC TR 3445_2022

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.

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC TR 3445_2022

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.

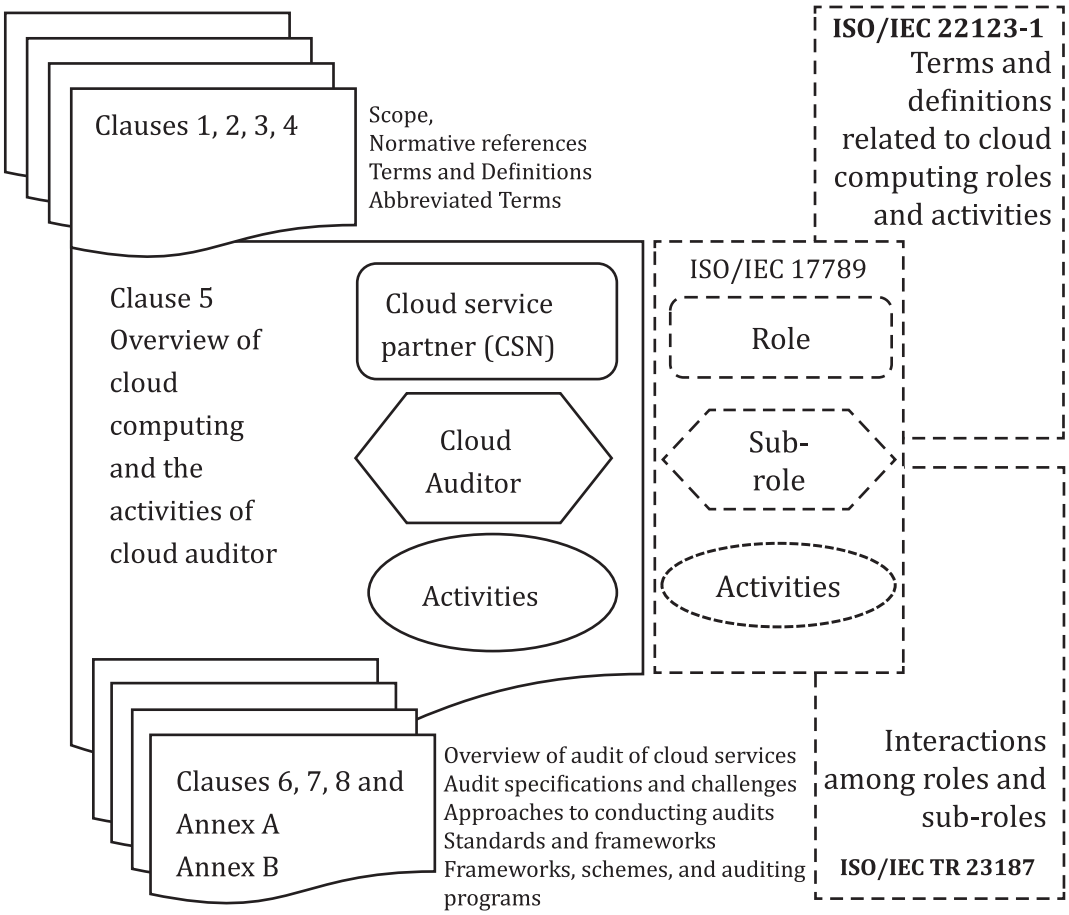

Figure 1 — Structure of the document

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.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC TR 3445_2022

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]

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC TR 3445_2022

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.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC TR 3445_2022

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]

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC TR 3445_2022

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.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC TR 3445_2022

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

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC TR 3445_2022

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.

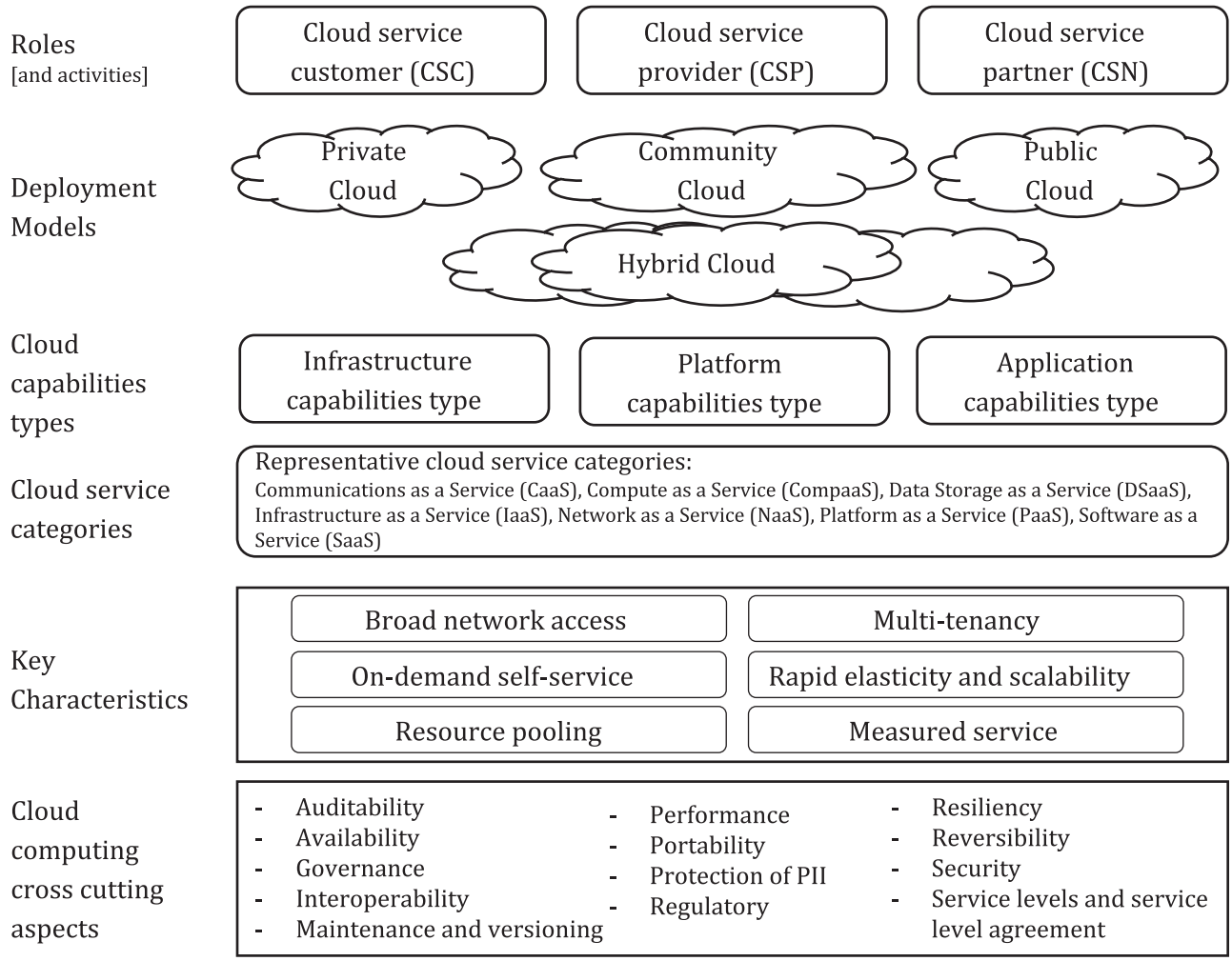

Figure 2 — Overview of cloud computing

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

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC TR 3445_2022

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.

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC TR 3445_2022

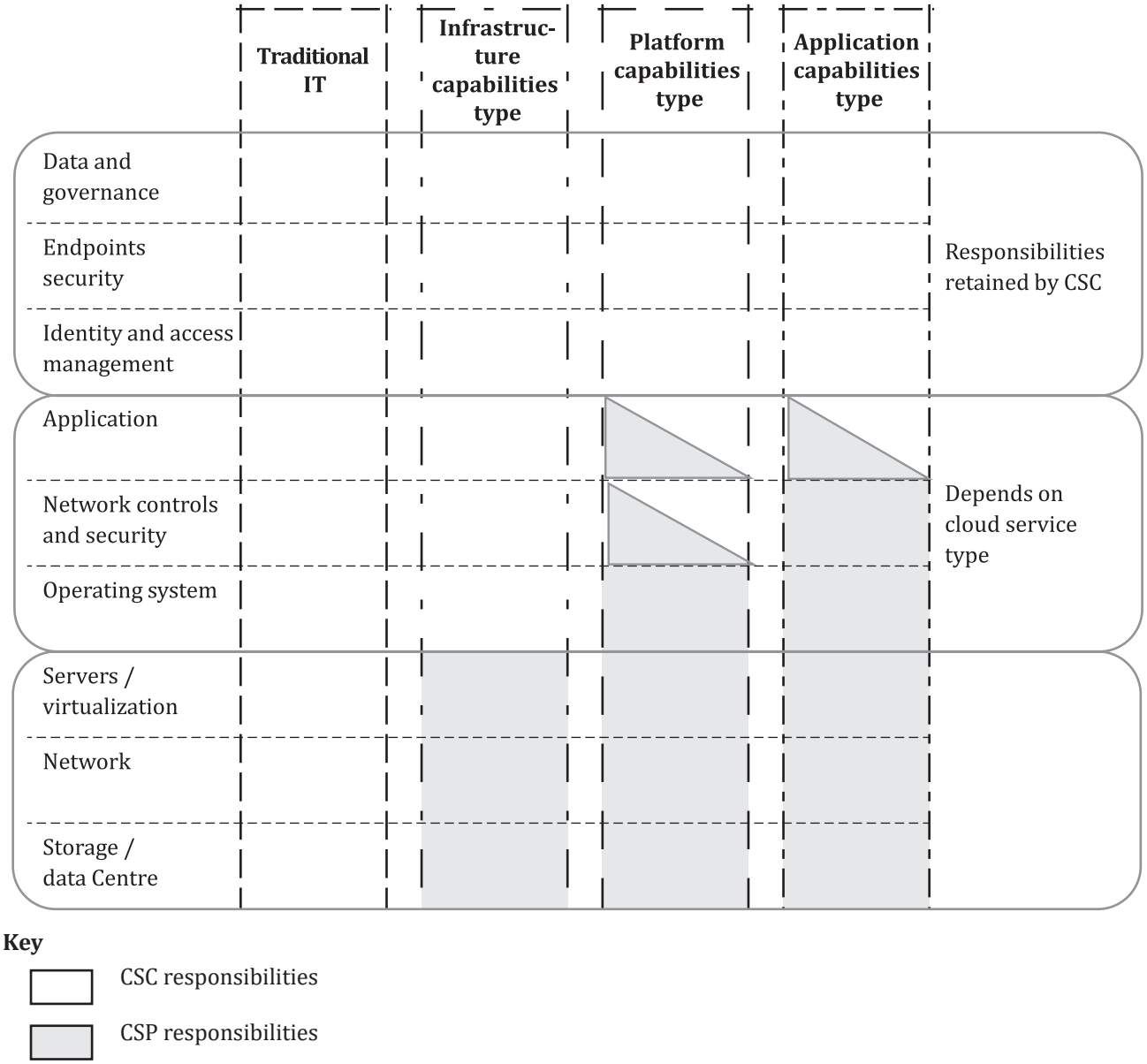

Figure 3 — An example of CSP and CSC responsibilities

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.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC TR 3445_2022

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.

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC TR 3445_2022

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.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC TR 3445_2022

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).

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC TR 3445_2022

— 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;

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC TR 3445_2022