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/IEC 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

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

© ISO/IEC 2022 – All rights reserved

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

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

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.

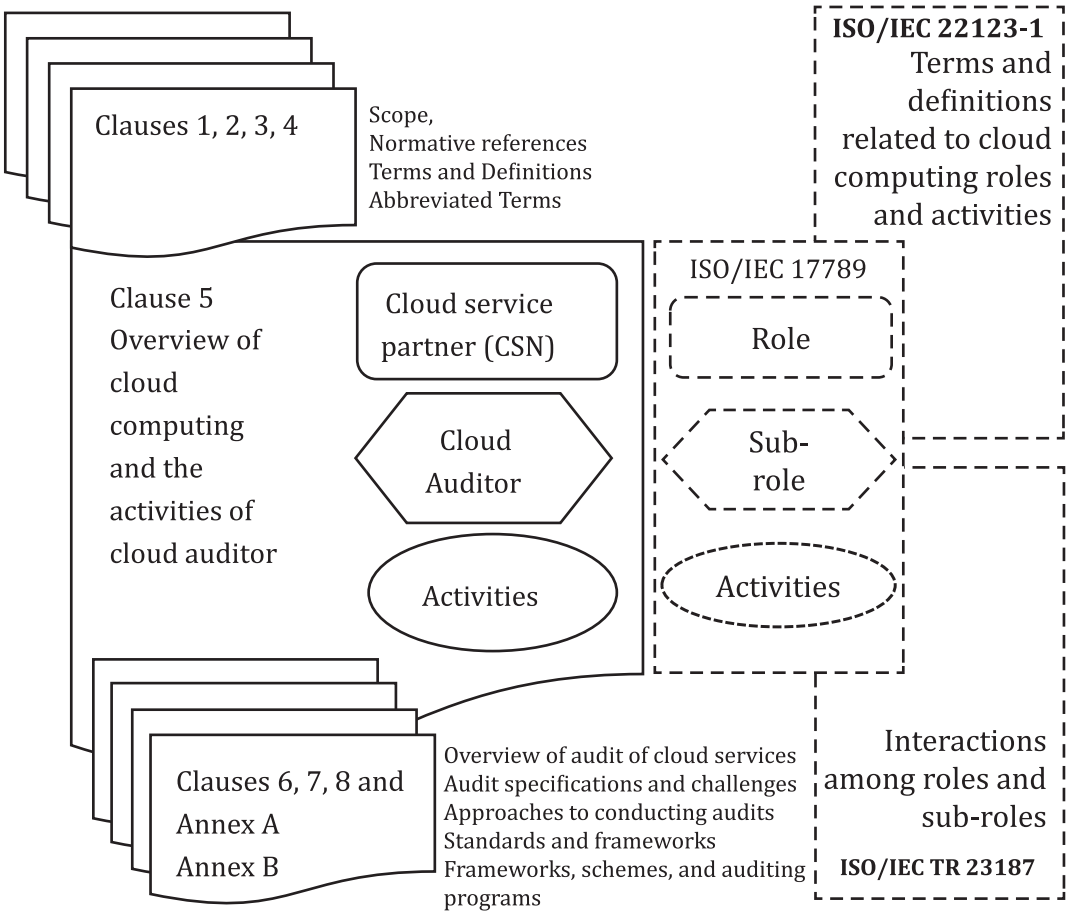


Figure 1 — Structure of the document

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

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

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

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

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

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