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)

COPYRIGHT PROTECTED DOCUMENT

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.

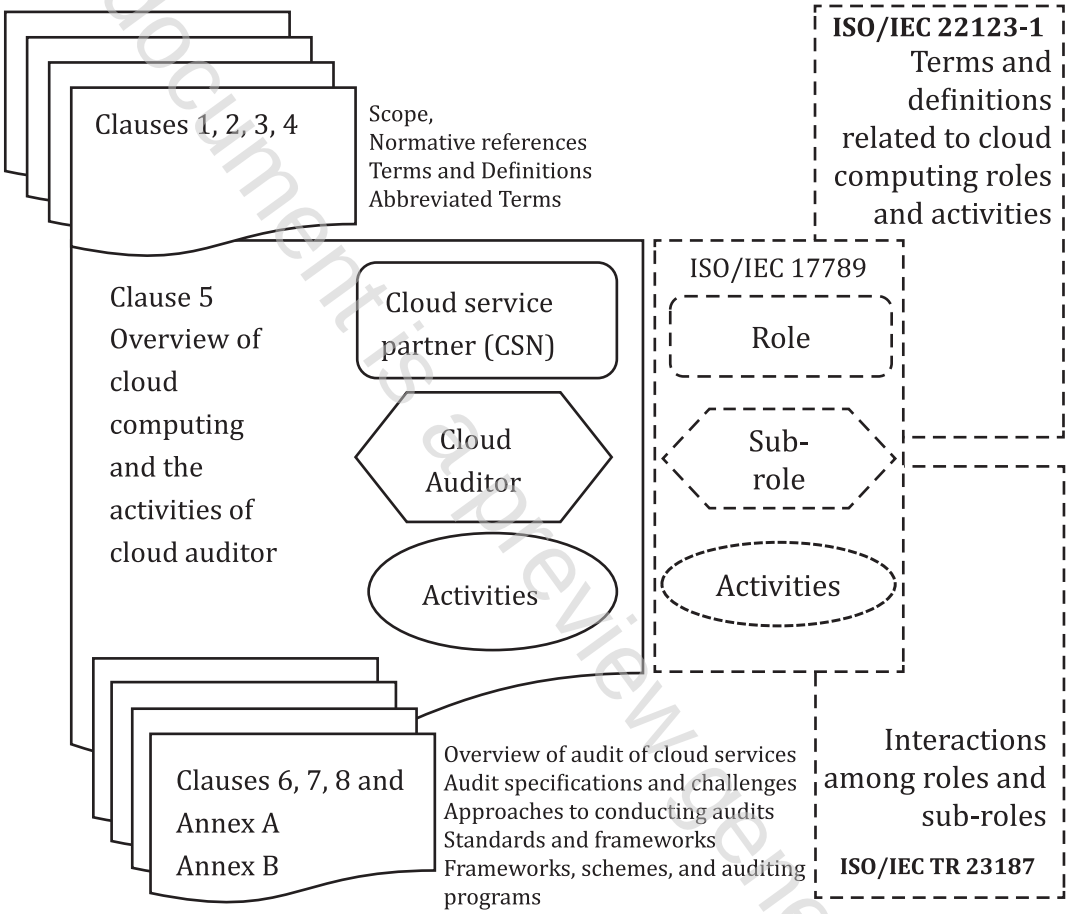

Figure 1 — Structure of the document

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]