PD ISO/IEC TR 3445:2022



BSI Standards Publication

Information technology — Cloud computing — Audit of cloud services

National foreword

This Published Document is the UK implementation of ISO/IEC TR 3445:2022.

The UK participation in its preparation was entrusted to Technical Committee IST/38, Cloud Computing and Distributed Platforms.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2022
Published by BSI Standards Limited 2022

ISBN 978 0 539 14481 9

ICS 35.210

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 April 2022.

Amendments/corrigenda issued since publication

Date	Text affected

PD ISO/IEC TR 3445:2022

TECHNICAL REPORT

ISO/IEC TR 3445

First edition
2022-03-09

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, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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 23
6.4 Cloud audit and trust 24

7 Audit specifications and challenges **24**
7.1 Overview 24
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 25
7.4 Security controls assessment 26
7.5 Required laws, regulations, and government requirements 26
7.6 Policies 27
7.6.1 General 27
7.6.2 Geolocation data 28
7.7 Cloud service agreement (CSA) 28
7.8 Cloud capabilities types, cloud service categories and key characteristics 28
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 ... 34
8.1 Typical Scenarios ... 34
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 ... 38**

Annex B (informative) **Compilation of frameworks, schemes, and auditing programs for certification, attestation and authorization which are relevant to cloud security ... 43**

Bibliography ... 48

© 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.

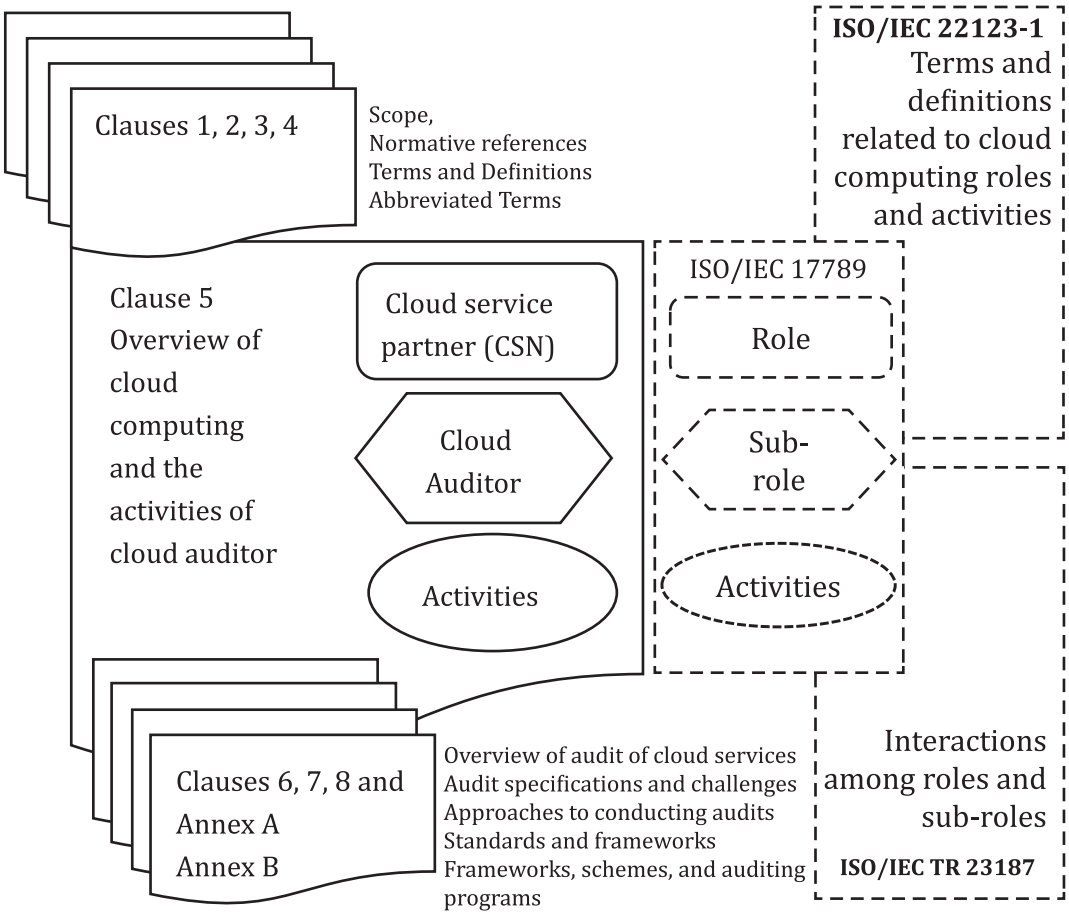


Figure 1 — Structure of the document

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