DRAFT International Standard

ISO/IEC DIS 20996

Information technology — Cloud computing — Cloud service customer business continuity and resilience

ICS: 35.210

ISO/IEC JTC **1**/SC **38**

Secretariat: **ANSI**

Voting begins on:
2026-07-01

Voting terminates on:
2026-09-23

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 20996:2026(en)

© ISO/IEC 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

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

Contents

Foreword v
Introduction vi
1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 Symbols and abbreviated terms 2
5 Overview of business continuity and resilience 2
5.1 General 2
5.2 Business continuity and resilience in cloud computing ..... Error! Bookmark not defined.
6 Cloud specific considerations from ISO 22313:2020 6
6.1 Risk management and continuity planning 6
6.1.1 Guidance to CSCs 7
6.1.2 Business Impact Analysis Framework 7
6.1.4 Principles of Resiliency 8
6.2 Operational planning and control 9
6.2.1 Guidance to CSCs 9
6.2.2 Operational Planning and Control for Smaller Firms 10
6.3 Supply chain continuity planning 10
6.3.2 Supply Chain Management 11
6.3.3 CSP Certifications and Third Party Validations 11
6.4 Leadership in cloud service management 12
6.4.1 Guidance to CSCs 13
6.5 Stakeholder identification and engagement 14
6.5.1 Guidance to CSCs 14
6.6 Exercising and testing 15
6.6.1 Guidance to CSCs 15
6.7 Regulatory compliance and governance 16
6.7.1 Guidance to CSCs 17
6.8 Resource allocation and competency development 18
6.8.1 Guidance to CSCs 19
6.8.2 Resource Allocation and Competency Development for Small Firms with Limited Resources 19
6.9 Communication and documentation 20
6.11 Understanding the cloud service environment 21
6.12 Monitoring and evaluation 22
6.12.1 Guidance to CSCs: 23
6.12.2 Monitoring and Escalation Framework 24
6.12.3 Monitoring and Evaluation for Smaller Firms and Firms with Limited Resources 24
Internal audit and compliance assurance 25
Guidance to CSCs: 25
Management review of cloud service performance 25

© ISO/IEC 2026 – All rights reserved

Guidance to CSCs **26**
Nonconformity management and corrective action **26**
Guidance to CSCs **26**
6.16 Continual improvement of cloud service strategies **27**
Guidance to CSCs **27**
6.17 Cloud Optimization **28**
6.17.1 Cloud Optimization and Financial Management for Small Organizations **28**
6.18 Security Operations **28**
6.18.1 Security Operations for Small Organizations **28**
6.19 Performance Efficiency **29**
6.20 Operational Excellence **29**
Annex A (informative) Considerations on business continuity planning (BCP) for large-scale natural disasters and pandemics **30**
Annex B (informative) Financial Services **32**
Annex C (informative) Energy Sector **35**
Bibliography **42**

© ISO/IEC 2026 – All rights reserved

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO 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).

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.

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 should be found at www.iso.org/members.html.

© ISO/IEC 2026 – All rights reserved

Introduction

The world is undergoing digital transformation, and many organisations now serve their customers through digital channels (for example, via websites, apps, and interactive voice response systems), or are reliant on digital technology within their own organisations to support key business processes. The availability of cloud services is fueling digital transformation, and opening up new digital channels to many organisations.

When an organisation moves its products and services to digital channels, those products and services need to be resilient to disruptions, not just able to recover from failure. Organizations needs to conduct systematic assessments to determine critical business functions and their dependencies, potential impacts of disruptions on operations, revenue, and reputation, required recovery time and point objectives, and appropriate resource allocation for resilience measures

This document provides cloud-specific implementation guidance that complements ISO 22313:2020. It is written for organizations acting as cloud service customers (CSCs) and shows how to meet business continuity and resilience requirements when using cloud services delivered by cloud service providers (CSPs) in alignment with the CSC's resiliency targets. The guidance addresses risk assessment and business impact analysis, shared responsibility between CSPs and CSCs, operational planning and control, resource allocation and competency development, monitoring and evaluation, and industry-specific considerations for financial services, healthcare, energy, and public sectors

Organizations of all sizes can use this guidance to develop appropriate continuity and resilience strategies. The document includes specific considerations for small organizations with limited resources, providing phased implementation approaches that align with organizational capabilities and priorities.

This document adds no new certification requirements but interprets existing ISO 22313 clauses in a shared-responsibility cloud context. It provides practical recommendations on integrating cloud services into business continuity management systems.

© ISO/IEC 2026 – All rights reserved

Information technology – Cloud computing – Cloud service customer business continuity and resilience

1 Scope

This document provides guidance to cloud service customers on business continuity and resilience when using cloud services.

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 22300 - Security and resilience — Vocabulary

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

ISO 22301 – Security and resilience — Business Continuity management — Requirements

ISO 22313 – *Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 22123-1, ISO 22300 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1 board

board of directors

management committee

group of people mandated to assume legal responsibility to manage and/or oversee an organization

Note 1 to entry: The board should be known by different names in different countries.

[Source: ISO 18716:2024 (en), 3.2]

3.2 **observability**

Capability to understand the internal state and behavior of a system by examining its external outputs, including logs, metrics, traces, and events.

Note 1 to entry: Observability extends beyond traditional monitoring by enabling diagnosis of unknown Problems and emergent behaviors.

Note 2 to entry: In cloud environments, observability tools are typically provided by CSP but configured and interpreted by the CSC.

Note 3 to entry: Effective observability supports both operational management and incident response capabilities.

3.3 operational teams

Entity that defines operational needs and implements cloud service strategies

3.4 senior management

individual or group(s) who directs and controls an organization including strategic level management positions

© ISO/IEC 2026 – All rights reserved

EXAMPLE:
Chief Executive Officer (CEO), Chief Technology Officer (CTO), Chief Operating Officer (COO), Chief Financial Officer (CFO).

Note 1 to entry: Senior management are sometimes referred to, within organizations, as executive management, top management, upper management and higher management.

[Source: ISO/TS 5441:2024(en), 3.16]

3.5 shared responsibility

A collaborative approach where the responsibilities for security and operational management are divided between a service provider and its customers based on service type and configuration.

3.6 shared responsibility model

A framework that outlines the division of roles and obligations between a cloud service provider and its customers, specifying that the provider manages the underlying cloud infrastructure while the customer is responsible for securing and configuring their use of the cloud services according to their specific needs.

4 Symbols and abbreviated terms

CSC	cloud service customer
CSP	cloud service provider
CSU	cloud service user
ICT	information and communication technology
BCMS	Business Continuity Management System
SLA	service level agreement

5 Overview of business continuity and resilience

5.1 General

Business continuity in cloud computing refers to the strategies and processes that organizations implement to maintain or quickly restore the operation of their critical business functions in the event of a disruption. In a cloud environment, this involves leveraging the cloud provider's infrastructure, tools, and services to maintain the availability, integrity, and performance of essential applications and data.

Business continuity and resiliency plan solutions may also utilize CSPs within a single or multiple locations, addressing the identified risks and needs of the cloud service customer.

5.2 Business continuity in cloud computing

Cloud computing enables organizations to implement architectural patterns that enhance business continuity and resilience through automated, programmatic approaches. These patterns include designing systems that anticipate and automatically respond to failures, implementing self-healing mechanisms that detect and replace failed components, and using infrastructure as code to ensure consistent, repeatable deployments across environments. For example, an organization can implement automated health checks that detect when an application instance becomes unresponsive and trigger automatic replacement with a new instance, all while maintaining service availability. This approach is complemented by immutable infrastructure patterns, where infrastructure components are never modified in place but rather replaced entirely with new versions, reducing configuration drift and improving recovery reliability. These architectural patterns, when properly implemented, enable organizations to maintain service continuity even during component failures and significantly reduce recovery times during disruptions.

© ISO/IEC 2026 – All rights reserved