SLOVENSKI STANDARD
oSIST prEN ISO/IEC 27017:2025

01-april-2025

Informacijska varnost, kibernetska varnost in varstvo zasebnosti - Kontrole informacijske varnosti, ki temeljijo na ISO/IEC 27002 za storitve v oblaku (ISO/IEC DIS 27017:2025)

Information security, cybersecurity and privacy protection - Information security controls based on ISO/IEC 27002 for cloud services (ISO/IEC DIS 27017:2025)

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Informationssicherheitsmaßnahmen auf der Grundlage von ISO/IEC 27002 für Cloud-Dienste (ISO/IEC DIS 27017:2025)

Sécurité de l'information, cybersécurité et protection de la vie privée - Contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage (ISO/IEC DIS 27017:2025)

Ta slovenski standard je istoveten z: **prEN ISO/IEC 27017**

ICS:

03.100.70	Sistemi vodenja	Management systems
35.030	Informacijska varnost	IT Security
35.210	Računalništvo v oblaku	Cloud computing

oSIST prEN ISO/IEC 27017:2025 **en,fr,de**

DRAFT International Standard

ISO/IEC DIS 27017

Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for cloud services

ICS: 35.030

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2025-02-03

Voting terminates on:
2025-04-28

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/IEC DIS 27017:2025(en)

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

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating, and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a world-wide basis. The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups that, in turn, produce Recommendations on these topics. The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1. In some areas of information technology that fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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 Technical Committee ISO/IEC JTC 1 Information technology, Subcommittee SC 27, Information security, cybersecurity and privacy protection, in collaboration with ITU-T. The identical text is published as ITU-T Recommendation X.1631.

This second edition cancels and replaces the first edition (ISO/IEC 27017:2015 | ITU-T Recommendation X.1631), which has been technically revised.

The main changes are as follows:

— the title has been modified;

— the structure of the document has been changed, presenting the controls using a simple taxonomy and associated attributes;

— some controls have been merged, some have been removed and several new controls have been introduced. The complete correspondence can be found in Annex B.

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.

Introduction

The guidelines contained within this Recommendation | International Standard are in addition to and complement the guidelines given in ISO/IEC 27002:2022.

Specifically, this Recommendation | International Standard provides guidance supporting the implementation of information security controls for cloud service customers (CSCs) and cloud service providers (CSPs). Some guidance are for CSCs who implement the controls and others are for CSPSs to support the implementation of those controls. The determination of the appropriate information security controls and the extent of the utilisation of the guidance provided will depend on the results of the relevant risk assessment and the existence of any legal, regulatory, contractual, or other cloud-computing specific information security requirements.

Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for cloud services

1 Scope

This Recommendation | International Standard gives guidelines for information security controls applicable to the provision and use of cloud services by providing:

— additional guidance for relevant controls specified in ISO/IEC 27002:2022;

— additional controls with guidance that specifically relate to cloud services.

This Recommendation | International Standard provides controls and guidance for CSCs and CSPs.

This Recommendation | International Standard excludes any and all aspects of conformity assessment.

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 22123-1:2023, *Information technology — Cloud computing — Part 1: Vocabulary*

ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27002:2022, ISO/IEC 22123-1:2023, 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/

3.1.1
capability
ability to perform a specific activity

[SOURCE: ISO 19440:2020, 3.5]

3.2 Abbreviated terms

CSC	cloud service customer
CSN	cloud service partner
CSP	cloud service provider
CSU	cloud service user
IaaS	infrastructure as a service
ICT	information and communication technology
PaaS	platform as a service
PII	personally identifiable information
RTO	recovery time objective
RPO	recovery point objective
SaaS	software as a service
SLA	service level agreement

4 Cloud computing specific concepts

4.1 General

4.1.1 Overview

This Recommendation | International Standard provides additional cloud-specific guidance based on ISO/IEC 27002 and provides additional controls to address cloud-specific information security threats and risks considerations.

Users of this Recommendation | International Standard should refer to Clauses 5 to 8 in ISO/IEC 27002:2022 for attributes, controls, purposes, guidance and other information. Because of the general applicability of ISO/IEC 27002:2022, many of the controls, guidance and other information apply to both the general and cloud computing contexts of an organization. For example, "5.3 Segregation of duties" of ISO/IEC 27002 provides a control that can be applied whether the organization is acting as a CSP or not. Additionally, a CSC can derive requirements for segregation of duties in the cloud environment from the same control, e.g. a CSC segregating the CSCs' cloud service administrators from other CSUs.

As an extension to ISO/IEC 27002:2022, this Recommendation | International Standard further provides cloud service specific controls, attributes, purposes, guidance and other information that are intended to mitigate the risks that accompany the technical and operational features of cloud services (see clause 4.1.2 for the structure of this document). Annex B provides a mapping for backwards compatibility with ISO/IEC 27017:2015. The CSCs and the CSPs can refer to ISO/IEC 27002:2022 and this Recommendation | International Standard to determine controls with the guidance and add other controls if necessary. This process can be done by performing an information security risk assessment and risk treatment in the organizational and business context where cloud services are used or provided (see clause 4.2.3).

NOTE This Recommendation | International Standard is applicable to all different cloud deployment models including the private cloud. Even in this case, the controls and guidance of this document are applicable, although adjustments can be needed to adjust to the relationships and abilities of the internal departments of an organization.

4.1.2 Structure of this International Standard

This Recommendation | International Standard is structured in a format similar to ISO/IEC 27002:2022.