EESTI STANDARD EVS-EN ISO/IEC 27017:2021

# Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services (ISO/IEC 27017:2015)

| EESTI STANDARDI EESSÕNA | NATIONAL FOREWORD |
|---|---|
| See Eesti standard EVS-EN ISO/IEC 27017:2021 sisaldab Euroopa standardi EN ISO/IEC 27017:2021 ingliskeelset teksti. | This Estonian standard EVS-EN ISO/IEC 27017:2021 consists of the English text of the European standard EN ISO/IEC 27017:2021. |
| Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas. | This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation and Accreditation. |
| Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 20.01.2021. | Date of Availability of the European standard is 20.01.2021. |
| Standard on kättesaadav Eesti Standardimis-ja Akrediteerimiskeskusest. | The standard is available from the Estonian Centre for Standardisation and Accreditation. |

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.030

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

# EN ISO/IEC 27017

January 2021

ICS 35.030

English version

# Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services (ISO/IEC 27017:2015)

Technologies de l'information - Techniques de sécurité - Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage (ISO/IEC 27017:2015)

Informationstechnik - Sicherheitsverfahren - Anwendungsleitfaden für Informationssicherheitsmaßnahmen basierend auf ISO/IEC 27002 für Cloud Dienste (ISO/IEC 27017:2015)

This European Standard was approved by CEN on 20 December 2020.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

**CEN-CENELEC Management Centre:**
**Rue de la Science 23, B-1040 Brussels**

Ref. No. EN ISO/IEC 27017:2021 E

## European foreword

The text of ISO/IEC 27017:2015 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology” of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 27017:2021 by Technical Committee CEN/CLC/JTC 13 “Cybersecurity and Data Protection” the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by July 2021, and conflicting national standards shall be withdrawn at the latest by July 2021.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

## Endorsement notice

The text of ISO/IEC 27017:2015 has been approved by CEN as EN ISO/IEC 27017:2021 without any modification.

## FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). 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 worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, 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 which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

## NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

## INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

## CONTENTS

## Introduction

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

Specifically, this Recommendation | International Standard provides guidelines supporting the implementation of information security controls for cloud service customers and cloud service providers. Some guidelines are for cloud service customers who implement the controls, and others are for cloud service providers to support the implementation of those controls. The selection of appropriate information security controls and the application of the implementation guidance provided, will depend on a risk assessment and any legal, contractual, regulatory or other cloud-sector specific information security requirements.

**INTERNATIONAL STANDARD**
**ITU-T RECOMMENDATION**

# Information technology – Security techniques – Code of practice for 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 implementation guidance for relevant controls specified in ISO/IEC 27002;
- additional controls with implementation guidance that specifically relate to cloud services.

This Recommendation | International Standard provides controls and implementation guidance for both cloud service providers and cloud service customers.

## 2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

### 2.1 Identical Recommendations | International Standards

- Recommendation ITU-T Y.3500 (in force) | ISO/IEC 17788: (in force), *Information technology – Cloud computing – Overview and vocabulary*.
- Recommendation ITU-T Y.3502 (in force) | ISO/IEC 17789: (in force), *Information technology – Cloud computing – Reference architecture*.

### 2.2 Additional References

- ISO/IEC 27000: (in force), *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.
- ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls*.

## 3 Definitions and abbreviations

### 3.1 Terms defined elsewhere

For the purposes of this Recommendation | International Standard, the terms and definitions given in ISO/IEC 27000, Rec. ITU-T Y.3500 | ISO/IEC 17788, Rec. ITU-T Y.3502 | ISO/IEC 17789 and the following definitions apply:

**3.1.1** The following term is defined in ISO 19440:

- **capability**: Quality of being able to perform a given activity.

**3.1.2** The following terms are defined in ISO/IEC 27040:

- **data breach**: Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored, or otherwise processed.
- **secure multi-tenancy**: Type of multi-tenancy that employs security controls to explicitly guard against data breaches and provides validation of these controls for proper governance.

  NOTE 1 – Secure multi-tenancy exists when the risk profile of an individual tenant is no greater than it would be in a dedicated, single-tenant environment.

  NOTE 2 – In very secure environments, even the identity of the tenants is kept secret.