SLOVENSKI STANDARD
kSIST-TS FprCEN/CLC/TS 18072:2024

01-september-2024

Zahteve za organe za ugotavljanje skladnosti, ki certificirajo storitve v oblaku

Requirements for Conformity Assessment Bodies certifying Cloud Services

Anforderungen an Konformitätsbewertungsstellen, die Cloud-Dienste zertifizieren

Ta slovenski standard je istoveten z: FprCEN/CLC/TS 18072

ICS:

03.120.20	Certificiranje proizvodov in podjetij. Ugotavljanje skladnosti	Product and company certification. Conformity assessment
35.030	Informacijska varnost	IT Security

kSIST-TS FprCEN/CLC/TS 18072:2024 en,fr,de

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

FINAL DRAFT
FprCEN/CLC/TS 18072

June 2024

ICS 03.120.20; 35.030

English version

Requirements for Conformity Assessment Bodies certifying Cloud Services

Anforderungen an Konformitätsbewertungsstellen, die Cloud-Dienste zertifizieren

This draft Technical Specification is submitted to CEN members for Vote. It has been drawn up by the Technical Committee CEN/CLC/JTC 13.

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, Türkiye and United Kingdom.

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.

Warning : This document is not a Technical Specification. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a Technical Specification.

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

Contents

Page

European foreword

This document (FprCEN/CLC/TS 18072:2024) has been prepared by Technical Committee CEN/CLC/JTC 13 “Cybersecurity and Data protection”, the secretariat of which is held by DIN.

This document is currently submitted to the Vote on TS.

This document is developed to support the Cybersecurity Act, EUCSA, Regulation (EU) 2019/881 on information and communications technology cybersecurity certification.

Introduction

The overall aim of certifying products, processes or services is to give confidence to all interested parties that a product, process or service fulfils specified requirements. The value of certification is the degree of confidence and trust that is established by an impartial and competent demonstration of fulfilment of specified requirements by a third party.

ISO/IEC 17065 specifies requirements, the observance of which is intended to ensure that certification bodies operate certification schemes in a competent, consistent and impartial manner, thereby facilitating the recognition of such bodies and the acceptance of certified products, processes and services on a national and international basis and so furthering international trade.

ISO/IEC 17065 gives generalized requirements for operating certification schemes for a broad range of products, processes or services. While the general requirements given by ISO/IEC 17065 are shared by all Certification Bodies, they are a high-level set.

The conformity assessment bodies providing evaluation and certification of cloud services have some specific requirements for evaluation procedures and competence.

To help implementers, this document is numbered identically to ISO/IEC 17065:2012. Supplementary requirements are presented as clauses and subclauses additional to ISO/IEC 17065:2012. Any supplementary requirements are presented in this document with the same clause / subclause number as in ISO/IEC 17065:2012.

1 Scope

This document complements and supplements the procedures and general requirements found in ISO/IEC 17065:2012 for conformity assessment bodies performing certification of cloud services under a dedicated European cybersecurity certification scheme (for example, those defined in Regulation (EU) 2019/881 (Cybersecurity Act), based on concepts defined in this regulation, such as the three assurance levels Basic, Substantial and High).

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 documents (including any amendments) applies.

ISO/IEC 17000, *Conformity assessment — Vocabulary and general principles*

ISO/IEC 17065:2012, *Conformity assessment — Requirements for bodies certifying products, processes and services*

CEN/CLC/TS 18026, *Three-level approach for a set of cybersecurity requirements for cloud services1* [1]

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17000, ISO/IEC 17065 and CEN/CLC/TS 18026[1] 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
appropriateness of evidence
measure of the relevance and reliability of evidence in providing support for the evaluator's conclusion

[SOURCE: International Standard on Assurance Engagements (ISAE) 3000, definition 12.i.ii]

3.2
carve-out method
evaluation method where the description of the system includes the services provided by the subservice provider but the controls and controls objectives from the subservice provider are excluded from the description and the scope of the evaluation

Note 1 to entry: When carve-out method is used, the scope of the evaluation includes controls implemented by the client to monitor the effectiveness of controls which can include the review of assurance documentation of the subservice provider.

[1] Under preparation. Stage at the time of publication: FprCEN/CLC/TS 18026

3.3
complementary user entity control
CUEC
control that the cloud service provider (CSP) assumes, in the design of its service, will be implemented by its customer

3.4
complementary service organization controls
CSOC
controls that the cloud service provider assumes that their subservice providers will have in place in order for them to securely operate their cloud service

3.5
evaluation
combination of the selection and determination functions of conformity assessment activities

Note 1 to entry: Evaluations include initial, surveillance, re-certification evaluations, and can also include special evaluations.

[SOURCE: EN ISO/IEC 17065:2012, definition 3.3]

3.6
evaluation criteria
reference to which conformity is determined

Note 1 to entry: Evaluation criteria include the requirements of a defined scheme for services applicable to a defined evaluation level and corresponding assurance level.

Note 2 to entry: Evaluation criteria include the requirements on the defined processes and documentation of the service operated by the client and of its associated controls.

3.7
fair presentation
accurate, truthful and transparent description of a client’s service

Note 1 to entry: Additional information about the content of a fair presentation is included in the certification scheme.

3.8
inclusive method
evaluation method where the controls from the subservice that supports cloud service provider operations are included in scope and will be reviewed by the evaluators

Note 1 to entry: When inclusive method is used, the description of the client’s service includes the services provided by the subservice provider, the relevant control objectives and related controls if existing.

3.9
suitability of the design of a control
control design which ensures that actions or events that comprise a risk are prevented, or detected and corrected

Note 1 to entry: Typical risk are information security risks.

4 General requirements

4.1 Legal and contractual matters

4.1.1 Legal responsibility

The requirements of ISO/IEC 17065:2012, 4.1.1 apply.

4.1.2 Certification agreement

The requirements of ISO/IEC 17065:2012, 4.1.2 apply. In addition, the following requirements and guidance apply.

The certification agreement shall include the scope and the evaluation level.

4.1.3 Use of license, certificates and marks of conformity

The requirements of ISO/IEC 17065:2012, 4.1.3 apply.

4.2 Management of impartiality

4.2.1 General

The requirements of ISO/IEC 17065:2012, 4.2 apply. In addition, the following requirements and guidance in 4.2.2 apply.

4.2.2 Nonconflicting activities

The certification body (CB) and its personnel may carry out additional activities provided they do not constitute a risk to its impartiality. These activities may include:

a) organizing and participating in information meetings about the certification scheme in general;

b) arranging and participating as a lecturer in training courses, provided that, where these courses relate to cloud services, related security requirements and controls, evaluations or auditing, lecturers shall confine themselves to the provision of generic information and advice which is publicly available;

c) activities prior to evaluation, solely aimed at determining readiness for evaluation; however, such activities shall not result in the provision of recommendations or advice for specific solutions and shall not result in a reduction in the eventual evaluation duration;

d) performing third party evaluations according to standards, publicly available specifications or regulatory requirements other than those being part of the scope of accreditation; or

e) adding value during evaluations without recommending specific solutions.

NOTE Adding value during evaluations may include identifying opportunities for improvement, as they become evident during the evaluation.

4.3 Liability and financing

The requirements of ISO/IEC 17065:2012, 4.3 apply.

4.4 Non-discriminatory conditions

The requirements of ISO/IEC 17065:2012, 4.4 apply.

4.5 Confidentiality

The requirements of ISO/IEC 17065:2012, 4.5 apply.

4.6 Publicly available information

The requirements of ISO/IEC 17065:2012, 4.6 apply.

5 Structural Requirements

5.1 Organizational structure and top management

The requirements of ISO/IEC 17065:2012, 5.1 apply.

5.2 Mechanisms for safeguarding impartiality

The requirements of ISO/IEC 17065:2012, 5.2 apply.

6 Resource Requirements

6.1 Conformity assessment body personnel — Determination of competence criteria

The requirements of ISO/IEC 17065:2012, 6.1 apply. In addition, the following requirements and guidance apply.

The output of the process for determining the competence criteria for personnel involved in the management of evaluations or other certification activities shall be the documented criteria of required knowledge and skills necessary to effectively perform evaluation and certification tasks to be fulfilled to achieve the intended results.

Annex A provides a summary of competence requirements for personnel involved in specific certification functions.

6.2 Resources for Evaluation

The requirements of ISO/IEC 17065:2012, 6.2 apply.

7 Process requirements

7.1 General requirements

The requirements of ISO/IEC 17065:2012, 7.1 apply.

7.2 Application

The requirements of ISO/IEC 17065:2012, 7.2 apply.

7.3 Application review

7.3.1 The requirements of ISO/IEC 17065:2012, 7.3.1 apply. In addition, the following requirements apply.

The CB shall conduct additional review of the information obtained to ensure that:

a) the application contains all the information required by the certification scheme including the identification of subservices operated by subservice providers used by the client in the operation of its cloud service;

b) the client has acknowledged and understands its responsibilities as defined in the certification scheme;

c) the CB understands the area of activity of the client and the associated business risks;

d) the CB has the competence and capability to perform the certification activity;

e) CB has the resources, capabilities and competences are available to perform all evaluation activities.

7.3.2 The requirements of ISO/IEC 17065:2012, 7.3.2 apply.

7.3.3 The requirements of ISO/IEC 17065:2012, 7.3.3 apply.

7.3.4 The requirements of ISO/IEC 17065:2012, 7.3.4 apply. In addition, the following requirement apply.

When the CB declines an application for certification as a result of the review of the application, the reasons for declining an application shall be documented and made clear to the client.

7.3.5 The requirements of ISO/IEC 17065:2012, 7.3.5 apply.

7.4 Evaluation

7.4.1 General

The requirements of ISO/IEC 17065:2012, 7.4 apply. In addition, requirements and guidance in 7.4.2 – 7.4.6 apply.

NOTE ISO/IEC 17065 refers to "evaluation" and is applicable to the various types of product, process and services certification schemes which incorporate conformity assessment activities including inspection, testing and audit.

7.4.2 Types of evaluations

There are different types of evaluations, depending on both the nature of the evaluation (initial, surveillance, recertification and special) and on the assurance level ('Basic', 'Substantial' or 'High') associated to the selected evaluation level.

7.4.3 Preparation of the evaluation

7.4.3.1 General

During the preparation phase, the CB shall

a) determine the evaluation objectives, scope and criteria, based on the evaluation programme;

NOTE This encompasses vulnerability identification (including penetration testing) activities if required for the evaluation level.

b) select and appoint an evaluation team;

c) determine the evaluation time;

d) determine matters related to confidentiality and information security of records obtained during the evaluation;

e) determine the logistics and communications arrangements, including specific arrangements for the locations to be evaluated (e.g. datacentre visits); and