TECHNICAL SPECIFICATION **CEN/TS 18026**

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION April 2024

ICS 35.030; 35.210

This document is a preview generated by EVS

English version

Three-level approach for a set of cybersecurity requirements for cloud services

Mehrschichtiger Ansatz für einen Anforderungskatalog für Informations-/Cybersicherheitsmaßnahmen für Cloud Dienste

This Technical Specification (CEN/TS) was approved by CEN on 27 February 2024 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN and CENELEC will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN and CENELEC members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

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.

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

© 2024 CEN/CENELEC All rights of exploitation in any form and by any means reserved worldwide for CEN national Members and for CENELEC Members.

Ref. No. CEN/TS 18026:2024 E

Contents

Page

This document is a preview generated by EVS

European foreword

This document (CEN/CLC/TS 18026:2024) has been prepared by Technical Committee CEN/CLC /JTC 13 “Cybersecurity and Data protection”, the secretariat of which is held by DIN.

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.

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

Any feedback and questions on this document should be directed to the users’ national standards body. A complete listing of these bodies can be found on the CEN website.

This document is a preview generated by EVS

Introduction

General

This document presents requirements for cybersecurity of cloud services. These requirements are also strongly related to information security. ISO 27100 states that cybersecurity is primarily concerned with protecting entities including people, society, organisations and nations from cyber risks, while information security addresses maintaining confidentiality, integrity and availability of information with consequences. Information security and cybersecurity therefore have different perspectives and concerns while they are closely related and overlapping as both address cyber threats. The requirements primarily address the cloud service, but unavoidably also raise expectations and impose requirements on organisations developing and operating such services.

Organisations wishing to demonstrate conformance to these requirements might prefer to do so using a single free-standing certification or build on existing certifications held by that organisation or the cloud service. To facilitate this, the requirements are written so as to allow coverage by composition of multiple certifications, or a single-step complete coverage via a single certification.

In addition, the organisational requirements align closely with the requirements and controls of ISO/IEC 27001, ISO/IEC 27002 and other international schemes for cybersecurity and information security requirements and controls. This means that organisations already holding certifications, for the organisation or the service, can build from those prior audits and certifications. Similarly, if the requirements of this document are the first ones ever certified for this organisation or service, the evaluation materials will have the potential to be used to support additional certifications thereafter. Further guidance on this issue is available in <EUCS2>.

This document presents a set of requirements for cybersecurity of cloud services with two key concepts:

- It provides for three different assurance levels, i.e. Basic, Substantial and High: some requirements are present at all levels, sometimes being extended at higher levels, while others only come into effect at the higher levels; and
- A risk assessment is undertaken to determine the cloud service specific risks, taking also into account the opportunities with the level and the cloud service specific cyber risks; risk treatment then involves the selection of appropriate controls by the organisation to satisfy the requirements for that level. The requirements themselves that are included in the document are mandatory for the chosen level.

Nothing written in this document is to be taken as indicating requirements for how evaluations will be conducted by bodies offering conformance testing for certification schemes. Requirements for bodies offering conformance testing for certification schemes based on this document are given in <EUCS2>.

The three assurance levels: Basic, Substantial and High offer increasing levels of assurance as to the security of the cloud service. As this document addresses cybersecurity for cloud services, it is important to appreciate that an information security management system (ISMS) certification alone is not sufficient to demonstrate conformance with the requirements in this document. Nonetheless, having an ISMS will assist the organisation in developing and operating their cloud services and in satisfying some requirements in this document.

Assurance level Basic should be suitable for cloud services that are designed to meet typical security requirements on services for non-critical data and systems, while Substantial targets cloud services that are designed to meet typical security requirements on services for business-critical data and systems. Assurance level High should be suitable for cloud services that are designed to meet specific (exceeding level ‘substantial’) security requirements for mission-critical data and systems. Similarly, the assurance levels are intended to be achievable for cloud services being offered to cloud service customers (CSCs) who themselves target the indicated data and systems, and related criticality levels. The EUCS is not intended to address the needs of national security purposes and the activities of the State in areas of criminal law.

This document is a preview generated by EVS

Assurance levels

The requirements defined in the document are labelled Basic, Substantial or High:

- Requirements labelled Basic apply to assurance level Basic. They carry over to assurance levels Substantial and High, unless replaced by stronger requirements;
- Requirements labelled Substantial apply to assurance level Substantial and will in some cases be considered as guidance for level Basic (*i.e.*, the reference method to achieve the Basic requirements, which are often less detailed); and
- Requirements labelled High only apply to assurance level High.

Typically, the requirements corresponding to a cybersecurity objective are organized as follows:

- Basic requirements define a baseline in bold text, often with limited details or constraints;
- Substantial requirements add to that baseline further details and constraints in bold text. In addition, specific Substantial requirements are introduced; and
- High requirements add further details or constraints in bold text. Some are also related to automated monitoring, or to additional testing and review requirements, contributing to an increase in confidence in the security of the service.

Certification schemes define evaluation levels as a combination of assurance components that corresponds to an assurance level (and the requirements defined for this assurance level), and to appropriate levels of depth and rigour in the assessment, corresponding to a category of security problems.

Applicability of requirements

The risk assessment and risk treatment that the Cloud Service Provider (CSP) performs in accordance with RM-01 includes the determination of controls that are needed to satisfy the requirements in this document and to address identified risks. The implementation of controls may vary depending on the characteristics of the certified cloud service. The CSP can design further controls or determine them from other resources to address the results of the risk assessment, in addition to the requirements in the document. The similarities with this document's requirements to controls and or requirements in existing EN standards such as the ISO 27000 series can support the fulfilment of requirements by using these documents in addition. The CSP provides justifications for all the requirements present in this document applicable to the cloud service and to which level of assurance. The CSP explains in the description of the cloud service if individual Basic, Substantial, and High requirements are not applicable due to the design and implementation of the cloud service and how these requirements are addressed in other ways. Based on the information provided by the CSP, conformity assessment will be conducted to cover the scope for certification of the cloud service for the actual assurance level, as defined in the assessment methodology <EUCS2>.

Automated monitoring

The requirements related to "automated monitoring" or "monitor with automation", are about gathering and pre-processing data by non-human means. Automated monitoring should be distinguished from continuous monitoring. The latter refers to monitoring for an enduring period of time that can be applied both with or without automation. The introduction of automated monitoring requirements is intended to utilize the available technology, and to manage the complexity of security monitoring of cloud services, since standards focus on outcomes (i.e. "what" shall be achieved) there will be limited references to methods (i.e. "how" it shall be achieved) except in instances where automated monitoring requirements are specifically needed. For instance, automated monitoring will be required for processing, logging and

This document is a preview generated by EVS

storing large amounts of data to increase the efficiency of business processes and the cybersecurity of cloud services.

Structure of the document

This document presents twenty categories of requirements, each category is divided into themes. Each theme is structured as follows:

- A cybersecurity objective that the requirements aim to achieve.
- Requirements to be satisfied in the context of the cybersecurity objective with each requirement associated to an assurance level.
- The requirements within a single theme have to be read as a flow.

There are many cross-references between requirements and themes. For instance, the ISP-02 theme, which defines how policies and procedures are to be defined, is referenced many times.

The categories, and their intended purposes, are (with their clause numbers):

4. Organisation of Information Security

   Plan, implement, maintain and continuously improve the information security framework applicable to the cloud service.

5. Information Security Policies

   Provide an information security policy, derived into topic-specific policies and procedures regarding security of the cloud service to support business requirements.

6. Risk Management

   Provide a risk management framework, to manage the risks associated to the cloud service, from identification to treatment.

7. Human Resources

   Ensure that personnel understand their responsibilities based on job role descriptions, are aware of their responsibilities with regard to information security, and that the assets that are used to provide the cloud service are protected in the event of changes in responsibilities or termination.

8. Asset Management

   Identify the assets that are used to provide the cloud service and ensure an appropriate level of protection throughout their lifecycle.

9. Physical Security

   Prevent unauthorised physical access and protect against theft, damage, loss and outage of operations.

10. Operational Security

    Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.

11. Identity, Authentication and Access Control Management

    Limit access to information and information processing facilities.

12. Cryptography and Key Management

    Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of information.

This document is a preview generated by EVS

13. Communication Security

    Ensure the protection of information in networks and the corresponding information processing systems.

14. Portability and Interoperability

    Enable the ability to access the cloud service via other cloud services or IT systems of the CSCs, to obtain the stored data at the end of the contractual relationship and to securely delete it from the cloud service.

15. Change and Configuration Management

    Ensure that changes and configuration actions to information systems guarantee the security of the delivered cloud service.

16. Development of Information Systems

    Ensure information security in the development cycle of information systems.

17. Procurement Management

    Ensure the protection of information that suppliers related to the cloud service can access and monitor the agreed services and security requirements.

18. Incident Management

    Ensure a consistent and comprehensive approach to the capture, assessment, communication and escalation of information security incidents related to the cloud service.

19. Business Continuity

    Plan, implement, maintain and test procedures and measures for business continuity and emergency management for the cloud service.

20. Compliance

    Avoid non-compliance with legal, regulatory and contractual information security and compliance requirements related to the cloud service.

21. User Documentation

    Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for CSCs.

22. Dealing with Investigation Requests from Government Agencies

    Ensure appropriate handling of government investigation requests for legal review, information to CSCs, and limitation of access to or disclosure of data.

23. Product Security

    Provide appropriate cybersecurity mechanisms and controls in cloud services and the underlying infrastructure, products and components relied upon by the CSCs.

This document is a preview generated by EVS

1. Scope

This document provides a set of cybersecurity requirements for cloud services.

This document is applicable to organisations providing cloud services and their subservice organisations.

2. Normative references

There are no normative references in this document.

3. Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

- IEC Electropedia: available at https://www.electropedia.org/
- ISO Online browsing platform: available at https://www.iso.org/obp

3.1
access control
means to ensure that physical and logical access to assets is authorised and restricted based on business and information security requirements

[SOURCE: ISO/IEC 27002:2022, 3.1.1]

3.2
access right
permission for a subject to access a particular object for a specific type of operation

[SOURCE: ISO/IEC 2382:2015, 2126298]

3.3
account data
class of data specific to each cloud service customer that is required to administer the cloud service

Note 1 to entry: Account data is typically generated when a cloud service is purchased and is under the control of the cloud service provider.

Note 2 to entry: Account data consists of data elements provided by the cloud service customer, such as; name, address, telephone, etc.

[SOURCE: ISO/IEC 22123-1:2023(en), 3.9.4]

3.4
activity
specified pursuit or set of tasks

[SOURCE: ISO/IEC 22123-1:2023(en), 3.3.8]

This document is a preview generated by EVS