# SLOVENSKI STANDARD
# SIST EN 18037:2025

**01-junij-2025**

---

**Smernice za sektorsko oceno kibernetske varnosti**

Guidelines on a sectoral cybersecurity assessment

Leitlinien für ein sektorales Cybersecurity Assessment

Lignes directrices pour l'appréciation sectorielle de la cybersécurité

**Ta slovenski standard je istoveten z:** **EN 18037:2025**

---



**ICS:**

35.030 Informacijska varnost IT Security



**SIST EN 18037:2025** **en,fr,de**

EUROPEAN STANDARD **EN 18037**

NORME EUROPÉENNE

EUROPÄISCHE NORM March 2025

ICS 35.030

English version

# Guidelines on a sectoral cybersecurity assessment

Lignes directrices pour l'appréciation sectorielle de la cybersécurité

Leitlinien für ein sektorales Cybersecurity Assessment

This European Standard was approved by CEN on 15 December 2024.

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, Türkiye and United Kingdom.



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



Ref. No. EN 18037:2025 E

# Contents

Page

## European foreword

This document (EN 18037:2025) has been prepared 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of an identical text or by endorsement, at the latest by September 2025, and conflicting national standards shall be withdrawn at the latest by September 2025.

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.

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.

According to the CEN-CENELEC Internal Regulations, the national standards organisations 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, Türkiye and the United Kingdom.

# Introduction

This document specifies cybersecurity assessments at the level of a market sector or an application area. It is designed to be used as a preparatory step for the drafting of cybersecurity certification schemes for ICT products, and ICT processes and ICT systems used by a market sector for providing sectoral services to the end users or business customer thus creating sectoral ICT systems.

Sectoral ICT systems can be found in application areas such as mobile networks, digital identity, e-health, public transportation, or payment.

Sectoral ICT systems can involve very large numbers of stakeholder organizations from the same market sector which cooperate in specified roles for provisioning the sectoral services. In certain roles, like Mobile Network Operators or Public Transport Service Providers, the stakeholder organizations are potentially competing.

The stakeholder organizations participating in a sectoral ICT system act according to rules which are typically specified by a “coordinating entity” or a regulator and operate the ICT systems or products under their control as functional components of the sectoral ICT system.

Cybersecurity and assurance are not only relevant from the perspective of the customers of sectoral services. In the sectoral ICT system, a clear and consistent definition of cybersecurity and assurance requirements in relation to the stakeholder role is important to establish trust among the sectoral stakeholder organizations. Since ICT security deficiencies caused by one stakeholder can lead to risks for other stakeholder's business objectives.

As with any ICT system that is intended to meet elevated cybersecurity and assurance requirements, the sectoral stakeholder organizations need to find an appropriate balance between the need for cybersecurity and assurance and the cost of its implementation. When it comes to the definition of cybersecurity and certification requirements to the sectoral ICT system, it is intended to be supported by the identification of the risks for the stakeholder’s business objectives and the attack potential of the relevant attacker types associated with the intended use.

A sectoral ICT system supports numerous sectoral business processes and stakeholder business objectives which can be subject to cybersecurity risks. It can also involve a wide range of stakeholder-operated ICT systems, products and processes which usually need different evaluation and certification approaches for the validation of the implementation of security and assurance requirements. For trusted sectoral services, trust between sectoral stakeholders is essential. This applies also for re-using certificates. Certified components require a definition of assurance and security that provides consistency. For this the specification of requirements and the definition of risk levels for evaluation and certification is the basis.

The sectoral cybersecurity assessment methodology supports the aspects and requirements by the following features:

— The sectoral cybersecurity assessment will provide information about the business processes to be supported by the sectoral ICT system, the related business objectives of the sectoral stakeholders. It also identifies the primary and supporting assets which are critical for the secure implementation of the business processes (see 5. 2 and 6.3.3).

— The stakeholder-operated ICT systems, products or processes which are relevant for the security of the primary assets are identified. A ‘deep dive’ into the sectoral ICT system’s architecture provides detailed information about their intended use (see 6.1).

— Cyberthreat intelligence (CTI) information is used to collect information on potentially relevant attacker types, their motivation, and capabilities. CTI allows to prioritize those risk scenarios, which are most relevant to be considered for further analysis. This allows the most effective use of resources during the analysis and contributes to the information needed to assign cybersecurity