



SLOVENSKI STANDARD

oSIST prEN 18037-2:2026

01-november-2026

Smernice za sektorsko oceno kibernetске varnosti - 2. del: Uporaba rezultatov sektorske ocene kibernetске varnosti pri proizvajalcih IKT izdelkov

Guidelines on a sectoral cybersecurity assessment - Part 2: Application of sectoral cybersecurity assessment results by ICT product manufacturers

Leitlinien für eine sektorale Bewertung der Cybersicherheit - Teil 2: Anwendung der Ergebnisse der sektoralen Bewertung der Cybersicherheit durch Hersteller von IKT-Produkten

Sample Document

get full document from standards.iteh.ai

Ta slovenski standard je istoveten z: prEN 18037-2

ICS:

35.030

Informacijska varnost

IT Security

oSIST prEN 18037-2:2026

en,fr,de

Sample Document

get full document from standards.iteh.ai

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

DRAFT
prEN 18037-2

September 2026

ICS 35.030

English version

Guidelines on a sectoral cybersecurity assessment - Part 2: Application of sectoral cybersecurity assessment results by ICT product manufacturers

Leitlinien für eine sektorale Bewertung der
Cybersicherheit - Teil 2: Anwendung der Ergebnisse
der sektoralen Bewertung der Cybersicherheit durch
Hersteller von IKT-Produkten

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

If this draft becomes a European Standard, 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.

This draft European Standard was established by CEN and CENELEC 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.

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. 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 European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.



Contents

Page

European foreword	4
Introduction	5
1 Scope.....	6
2 Normative references.....	6
3 Terms and definitions.....	6
4 Symbols and abbreviated terms.....	7
5 Overview of assessments conforming to EN 18037 from the perspective of ICT product manufacturers.....	7
5.1 ICT products as part of the sectoral ICT system	7
5.2 Role of the product manufacturer in the sectoral cybersecurity and risk assessment.....	7
5.3 Capabilities of EN 18037 in supporting ICT product manufacturers.....	7
5.4 Support for multi-market ICT products.....	9
5.5 Impact of stakeholder's risk treatment decisions on ICT products	9
6 Sectoral information required by ICT product manufacturers.....	10
7 Guidance for the application of EN 18037 by sectoral stakeholders	10
7.1 General.....	10
7.2 Guidelines on general aspects of the sectoral assessment	11
7.2.1 Estimations and assumptions	11
7.2.2 Impartiality and non-discriminatory access.....	12
7.3 Guidance for establishing the sectoral context.....	12
7.3.1 Introduction to the market sector	12
7.3.2 Sectoral stakeholder types and their roles and responsibilities.....	13
7.3.3 Business and operational processes, identification of stakeholder objectives	14
7.3.4 Architecture of the sectoral system	14
7.3.5 Subsystems and identification of information, functional and supporting assets.....	15
7.3.6 Documentation of sectoral CTI information	16
7.4 Guidance for conducting the primary asset assessment	17
7.4.1 General guidance	17
7.4.2 Identification of risks, definition of assessment scenarios per business process	18
7.4.3 Assessment and rating of risks for primary assets.....	19
7.4.4 Identification of security and assurance level requirements per risk scenario	19
7.4.5 Decisions on risk treatment per risk scenario.....	19
7.5 Guidance for the supporting asset assessment of ICT products	21
7.5.1 General guidance	21
7.5.2 Definition and documentation of system level risk mitigation measures	21
7.5.3 Identification of ICT products for the supporting assets assessment.....	21
7.5.4 Aggregation of ICT product-related information	21
7.5.5 Re-assessment of supporting assets per risk scenario	22
7.5.6 Aggregation of re-assessment results per ICT product.....	22
7.6 Mapping of the detected security and assurance requirements	22
7.6.1 General.....	22
7.6.2 Guidance for conducting the gap analysis of supporting assets	23
7.6.3 Identification of potential resolutions	24

7.6.4	Guidance in case of unavailability of resolutions for product-specific gaps.....	24
7.7	Maintenance of the assessment report.....	24
8	Guidance for the application of EN 18037 by product manufacturers.....	25
8.1	General	25
8.2	Guidance to product manufacturers for documenting the sectoral context.....	25
8.2.1	General guidance	25
8.2.2	Estimating relevant objectives and assets based on the product's intended use	25
8.2.3	Estimating sectoral CTI information	26
8.3	Guidance to product manufacturers for conducting the primary asset assessment	26
8.4	Guidance to product manufacturers for conducting the supporting asset assessment.....	26
8.5	Mapping of the detected security and assurance requirements	26
	Annex A (informative) Example assessment of a fictitious sectoral system	28
	Bibliography	58

Sample Document

get full document from standards.iteh.ai

prEN 18037-2:2026 (E)**European foreword**

This document (prEN 18037-2:2026) 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 CEN Enquiry.

Sample Document

get full document from standards.iteh.ai

Introduction

EN 18037 specifies a methodology for risk and cybersecurity assessments of sectoral multi-stakeholder systems. The assessment is carried out by the sectoral stakeholders with focus on their particular objectives.

This document provides guidance to ensure that the assessment by the sectoral stakeholders also addresses the information needs of product manufacturers that offer ICT products for the particular sector.

Product manufacturers might not have sufficiently access to risk information and security and assurance requirements regarding the sector-specific use of their ICT products. The first aim of this document is to guide the sectoral stakeholders conducting their sectoral assessment according to EN 18037 so that the information needs of product manufacturers are also considered and met. The second aim is to provide guidance to product manufacturers on how they can use EN 18037's methodology for own assumptions of their ICT product's sector-specific risks and security requirements if assessment results from the sectoral stakeholders should not be available or if these are incomplete.

By applying EN 18037 and this document, product manufacturers will benefit from sector-specific risk information and requirements concerning their products. This supports the product manufacturers in the definition of their products and increases the probability that these will be accepted by the sectoral market.

The EN 18037 assessment methodology generates sector-specific information on threats, risks, risk treatment decisions and the resulting security and assurance requirements for the sectoral ICT systems, ICT processes and ICT products but it does not define specific security controls or evaluation and certification means. However, sector-specific standards, product-specific security controls or certification tools that match the requirements identified in the assessment conforming to EN 18037 can be integrated into the sectoral assessment report.

The methodology of EN 18037 and its way to describe security and assurance requirements is compatible with the EN ISO/IEC 15408 series and the SESIP evaluation and certification standard.

1 Scope

This document provides guidance for sectoral stakeholders and product manufacturers in generating ICT product-relevant information based on EN 18037.

Sectoral stakeholders are supported in applying the risk and cybersecurity assessment methodology so that the information needs of product manufacturers are covered by the sectoral assessment report.

Product manufacturers receive guidance in using methodology according to EN 18037 for own assumptions of their ICT product's sector-specific risks and security requirements.

This document uses a step-by-step approach for guiding sectoral stakeholders and product manufacturers through the assessment. For each step, the relevant information provided by EN 18037 is summarized or referenced and the enhancements or clarifications in support of the information needs of the ICT product manufacturers are pointed out.

From the perspective of product manufacturers, the re-use of existing product-specific specifications and certification tools is of particular relevance. Therefore, this document provides guidance how the results of sectoral assessments according to EN 18037 can be connected with these specifications and tools.

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.

EN 18037:2025, *Guidelines on a sectoral cybersecurity assessment*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 18037 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

attack method

how an attack can be carried out

Note 1 to entry: An attack method can require several attack means and can be carried out at different attack potential levels.

3.2

attack path

attacker activities for finding and exploiting a vulnerability

Note 1 to entry: An attack path can include several steps where different attack methods can be used.

3.3

attacker scenario

relevant attacker type's capacities, means and motivation to conduct actions that could potentially impact functional and information assets in the context of a risk scenario

3.4

intended use

role and purpose of an ICT product in an ICT system, in particular the supported ICT functions, the data processed, relevant threats and the operational environment

4 Symbols and abbreviated terms

For the purposes of this document, the following symbols and abbreviations apply:

APL	Attack potential level
AVA_VAN	Assurance family defined by EN ISO/IEC 15408-3 that addresses the vulnerability analysis
CAR	Common Assurance Reference
CSL	Common security level
CTI	Cyberthreat intelligence
EAL	Evaluation assurance level
IC	Impact class
ICT	Information and communication technology
IoT	Internet of Things
MRC	Meta-risk class
PL	Probability level

5 Overview of assessments conforming to EN 18037 from the perspective of ICT product manufacturers

5.1 ICT products as part of the sectoral ICT system

Sectoral ICT systems and their characteristics are documented in EN 18037:2025 Clause 6. According to this model, the sectoral ICT system supports the sectoral services provided to consumers or business customers. ICT products serve as components of the sectoral system.

The sectoral system's architecture defines the ICT product's particular role, purpose and the conditions under which the ICT product is operated, the ICT product's intended use.

5.2 Role of the product manufacturer in the sectoral cybersecurity and risk assessment

The cybersecurity and risk assessment of a sectoral or application-specific ICT system is conducted by the sectoral stakeholders. They decide if manufacturers of ICT products are directly involved in the assessment. For manufacturers of ICT products which are not specifically designed for the sector, this is typically not the case.

5.3 Capabilities of EN 18037 in supporting ICT product manufacturers

The 1st stage of the cybersecurity assessment in accordance with EN 18037 prepares the risk assessment in accordance with EN ISO/IEC 27005. As per EN ISO/IEC 27005, the assessment starts with the documentation of the sectoral context, followed by the identification of assets, potential threats, attackers and attack paths and a first estimation on the criticality of ICT products.

prEN 18037-2:2026 (E)

The context documentation describes the environment in which the sectoral or application-specific risk and cybersecurity assessment should be carried out. Technical, operational and business-related information required for the following stages of the assessment is documented:

- Identification of stakeholders of the sectoral system and a description of their roles and responsibilities within the sectoral system;
- Documentation of business or operational processes to be supported, the involvement and responsibilities of stakeholders and their objectives per process;
- Identification of the sectoral stakeholder's business objectives, obligations and, based on this, the definition of the sectoral primary assets;
- Documentation of the sectoral ICT system architecture down to the ICT product level, including a description of functions and data supported by the ICT product in its intended use;
- Documentation of sectoral cyber threat intelligence (CTI), which includes in particular assumptions on potentially relevant attacker types, their attack potential and their motivation and approaches to conduct attacks targeting the sectoral system.

The documentation of the sectoral context provides the option to document the intended use of an ICT product in its sectoral or application-specific context in very detail. This includes the product's role in the sectoral ICT system's architecture, the functions and the information supported by the ICT product in this role, the operational environment and the sectoral stakeholder type in charge for the operations of the ICT product.

Based on the documentation of the sectoral context, a first identification of potentially critical system functions and data are conducted. This can be used for a first estimation, if the ICT product in its intended use should be considered as security-critical. If so, the product is classified as "supporting asset" and threats, attacker types and attack paths that could be relevant for the ICT product in its intended use should be estimated.

The 2nd stage of the cybersecurity and risk assessment in accordance with EN 18037, the primary asset assessment, encompasses a risk assessment in accordance with EN ISO/IEC 27005. It starts with the identification of primary assets which are typically related to the stakeholder's objectives or obligations rather than the technical implementation of the system. Thereafter, the risks to these assets are identified and assessed by using risk scenarios. The risk ratings are conducted by the sectoral stakeholders. If they decide to treat the risk, the security and assurance level requirements are determined with the potential of the relevant attacker types serving as leading parameter.

The primary asset assessment focuses on risks concerning the primary assets and does not regard the individual ICT product. However, the security and assurance level requirements resulting from these risks are inherited by those ICT products that could contribute to the primary asset's risk scenarios if compromised. What is particularly important for product manufacturers is that the need to apply dedicated controls depends on the risk treatment decision of the sectoral stakeholders. If they, for instance, should decide that the potential consequences of the risk do not justify the cost for its mitigation, the risk may be accepted.

The 3rd stage of the cybersecurity and risk assessment in accordance with EN 18037, the supporting asset assessment, focusses on consolidating the security and assurance requirements to those ICT products that are relevant for the treatment of a particular risk.

As starting point, the risk-relevant supporting assets inherit the security and assurance level requirements identified for a dedicated risk scenario in the previous assessment stage. This assessment is being repeated for each relevant supporting asset, now considering product-specific attacker and threat information as well as the ICT product's intended use, technology and operational environment.

As result, the risk scenario-specific security and assurance level requirements for the supporting asset in its intended use are determined.

An ICT product could be a relevant supporting asset for multiple risk scenarios and could have, on top of that, multiple intended uses in the sectoral ICT system. This is considered in the next step by documenting the overall set of specific security and assurance requirements to an ICT product, which consists of the aggregate of the risk-scenario specific requirements and, if applicable, of the requirements related to different intended uses of the ICT product. This aggregated set of security and assurance requirements is what the manufacturer needs to address by implementing appropriate security controls and certification for the ICT product targeting the sectoral system.

The 4th stage of the risk and cybersecurity assessment in accordance with EN 18037 supports the identification of appropriate controls and product certification schemes that match the requirements to the ICT product determined in the previous stages.

In a first step, existing security specifications and certification schemes are applied to the product as far as possible. Then, an analysis detects the gaps that remain between the security measures already defined for the product and the security and assurance requirements identified by the previous assessment steps. If the requirements are not completely covered, the remaining gaps should be addressed by developing security controls and, for addressing assurance requirements, feasible security targets, protection profiles or even product certification schemes. This last step requires expert knowledge concerning the security implementation of the ICT product and related evaluation and certification. Typically, sectoral stakeholders conducting the assessment involve product and certification experts.

5.4 Support for multi-market ICT products

In many cases, product manufacturers target more than one market sector with their ICT products.

NOTE Multi-market products with intended uses in multiple targeted market sectors must comply with requirements for all intended uses in all targeted sectors.

The risk and cybersecurity assessment in accordance with EN 18037 is conducted per market sector or application area by the stakeholders of a particular sector. For multi-market ICT products, the product manufacturer should have the sectoral assessment reports from all targeted market sectors.

The aggregation of the product-specific requirements from these market sectors by the product manufacturer requires that the statements concerning risk level and, most important, the security and assurance level requirements are comparable.

The cybersecurity and risk assessment in accordance with EN 18037 provides comparability of security and assurance level requirements across sectoral assessment reports by using the attack potential as leading parameter for product-specific security and assurance level requirements.

5.5 Impact of stakeholder's risk treatment decisions on ICT products

The assessment in accordance with EN 18037 encompasses a risk assessment in accordance with EN ISO/IEC 27005 and a dedicated decision on how the identified and rated risks should be treated. The risk treatment decisions are taken by the sectoral stakeholders and risk owners and are documented in the sectoral assessment report.

The risk treatment decision determines the security and assurance requirements for the ICT product. If the sectoral stakeholders and risk owners decide that the risk does not merit mitigation, the application of security controls or certification of the ICT product are not required for this risk. Therefore, the availability and accessibility of sectoral risk treatment decisions is crucial for the product manufacturer.

6 Sectoral information required by ICT product manufacturers

Product manufacturers need sectoral information from their targeted market sectors to ensure that their ICT products fulfil the sectoral market's requirements and are accepted by the sectoral clients. Typically, the product should support the following capabilities and properties:

- a) Conformance of the ICT product with the sector-specific functional, security and assurance requirements;
- b) Appropriate protection against threats potentially targeting the ICT product and consequences that could occur if the ICT product should be compromised;
- c) Conformance with technical standards and legal or regulatory obligations relevant for the ICT product;
- d) Commercial competitiveness, in particular by optimization of product development and production cost.

In order to support the needs listed above, the following information should be generated and documented by the sectoral assessment per ICT product:

- a) Sectoral stakeholders responsible for deployment, operations, security and maintenance of the ICT product;
- b) Technical standards and legal or regulatory obligations relevant for the ICT product;
- c) Attacker types potentially targeting the ICT product, their attack potential and assumed attack paths;
- d) Intended uses per ICT product
 - Description of the ICT product's purpose and role in the sectoral ICT system and the sectoral business processes;
 - Functional and information assets supported by the ICT product;
 - Operational environment of the ICT product;
- e) Assets and risks associated with the ICT product
 - Risks to primary assets potentially resulting from compromises of the ICT product;
 - Risk scenarios involving the ICT product in its role as supporting asset, including potentially impacted primary assets, relevant attacker types, the identified risks and the risk rating;
- f) Risk treatment decisions affecting the security and assurance requirements to the ICT product;
- g) Security and assurance requirements per ICT product, aggregated from all risk scenario-specific requirements and, if appropriate, different intended uses of the ICT product in the sectoral system.

7 Guidance for the application of EN 18037 by sectoral stakeholders

7.1 General

The sectoral cybersecurity and risk assessment is typically carried out by the sectoral stakeholders. The guidance given in this clause is intended to support these sectoral stakeholders in conducting the context

establishment and the following steps of the assessment in a manner that ensures that all information required by product manufacturers is generated and documented. It also includes some general suggestions, for instance to ensure impartiality and non-discriminatory access for all interested product manufacturers to the sectoral market.

Clause 6 describes the information that the sectoral cybersecurity and risk assessment should generate and document to support product manufacturers.

As depicted in EN 18037:2025 Figure 1, sectoral assessments are carried out according to EN 18037 in three phases:

- a) The documentation of the sectoral context;
- b) The sectoral risk and cybersecurity assessment, which provides a normalized representation to risk, cybersecurity and assurance and is carried out in two steps, the primary asset assessment and the supporting asset assessment;
- c) The mapping of the security and assurance requirements identified by the sectoral assessment to the specifications and certifications tools of the ICT systems and ICT products used for by the sector.

For the first two phases, the guidance provided in the following subclauses focusses on making sure that the information needs of product manufacturers are considered by the sectoral stakeholders.

The mapping of the detected security and assurance requirements to ICT systems and ICT products, the third phase of the sectoral assessment, should build on existing horizontal and vertical specifications that are applicable for the sectoral ICT systems and ICT products. Therefore, detailed expertise concerning the particular ICT systems and ICT products and the relevant standards is required for this last step of the assessment. If needed and possible, the sectoral stakeholder should reach out to competent standardization bodies, industry organizations and potentially also manufacturers.

Starting with subclause 7.3 it is explained in a step-by-step approach how sectoral stakeholders should implement the assessment according to EN 18037 so that not only their own but also the product manufacturer's information needs are served.

7.2 Guidelines on general aspects of the sectoral assessment

7.2.1 Estimations and assumptions

For most sectors, there are no reliable sources of CTI information available. Information on relevant attacker types, their capacities and motivation, typical attack paths etc. should be estimated based, for instance, on information from public sources or based on observations and assumptions of the sectoral stakeholders.

The same applies in principle for ICT products. Here, the product manufacturers are typically the main sources of information on relevant threats, attack paths etc.

Risk ratings and risk treatment decisions are largely depending on the risk perception and the risk tolerance of those stakeholders whose assets could be impacted.

CTI information, risk ratings etc. are essential for the subsequent steps of the assessment and the resulting security and assurance requirements to ICT products. However, these are often based on estimations, assumptions or individual views.

Assessment-relevant information that is based on estimations or assumptions should be flagged. The sources and the rationale behind those estimations and assumptions should be documented so that plausibility checks can be conducted whenever required.

7.2.2 Impartiality and non-discriminatory access

The sectoral stakeholders might want to use the expertise of product manufacturers for the assessment. These will commonly be involved in the assessment if ICT products are specifically designed for the sector and the manufacturers work on behalf of the sector. However, if generic ICT products are acquired from the market, the product manufacturer's involvement in the sectoral assessment should ensure impartiality and non-discriminatory participation. The following guidance is intended to accomplish this:

- Practicality will likely require that only few selected product manufacturers can be involved in the assessment. Their competitors could see this as inappropriate advantage.
- If product manufacturers will be involved in the assessment, provisions should be taken that they cannot use their participation to position competitive advantages for their products or technologies.
- All assessment steps and results should be documented and made available to all interested parties.
- If possible, expertise from standardization organizations or industry bodies should be involved to ensure that preferential treatment of individual product manufacturers is excluded.
- If public tenders are used for acquiring ICT products, depending on the sectoral or legal rules, the participation of individual product manufacturers in the sectoral assessment could be seen as participation in the preparation of the tender. This could disqualify them for participating in the tender. In this case, expertise from standardization organizations, commercial chambers or industry bodies should be used.

7.3 Guidance for establishing the sectoral context

7.3.1 Introduction to the market sector

The documentation of the sectoral context starts with a general introduction to the market sector or application area.

This should include the following information:

- The services typically provided by the sector;
- Typical clients of these sectoral services;
- The societal relevance of these services, particularly if the services are of public interest and are associated with dedicated obligations;
- The area in which these services are provided, for instance if these are offered in a certain region, nationally or internationally;
- Interactions with other market sectors or infrastructure, for instance the employment of Identity, payment or mobile network services;
- Legal or regulatory obligations that apply for the sector or its services.

To specifically support product manufacturers, the introduction to the market sector should characterize the relationship between the particular sector and its product manufacturers. The following questions are intended as guidance for identifying and documenting the sectoral situation:

- Are there specific requirements, beyond the technical requirements to the product, that the product manufacturer shall fulfil, for instance legal or regulatory obligations, sectoral governance rules etc.?

- Are there product manufacturers that are considered stakeholders of the sector?
- Does the sector typically use market-customary ICT products that are also used by other sectors?
- Are sector-specific ICT products employed which are specifically designed for the sector?
- Is the sector in the position to obtain sector-specific products or sector-specific features from the market or does it need to rely on common-market ICT products?
- Does the sector typically work with system integrators for the definition and implementation of the sectoral ICT system?
- Does the sector typically involve product manufacturers in the specification of the sectoral system or in the specification of the ICT products?
- Does the sector employ specific product manufacturers as suppliers?

7.3.2 Sectoral stakeholder types and their roles and responsibilities

The detailed documentation of the sectoral context starts with the documentation of the sectoral stakeholder types and their roles and responsibilities, those entities that actively contribute to the provisioning of the sectoral services or that consume those.

First, it should be checked if a sectoral specification of the stakeholder types and their roles is available. If so, like for instance in mobile networks, credit card payment or eIDAS-conformant identification, this specification should be re-used.

As first step of the documentation, the sectoral stakeholder types are identified. Stakeholders qualify as sectoral stakeholders if the sectoral market is an area of their activities and if they act according to governance rules defined for the sectoral role play.

Sectors that require a coordinated cooperation between multiple stakeholder types often employ a coordinating stakeholder role, called coordinating entity in EN 18037. This coordinating entity takes care for tasks overarching the sectoral system like defining sectoral technical specifications and governance rules, acting as registrar or security manager, coordinating daily operations and last but not least conducting sectoral risk and cybersecurity assessments.

For any sectoral stakeholder types, the following information should be identified and documented:

- Stakeholder types should be identified and given a descriptive name;
- The role and the responsibilities of the stakeholder type in the sectoral context, in particular in provisioning or consuming the services provided by the sector;
- The stakeholder type's relation with other sectoral stakeholder types;
- The stakeholder type's relation with external suppliers of services or products;
- The relation between stakeholders of the same stakeholder type, in particular if these potentially are competing with each other.

Typically, a sector cannot completely rely on own stakeholders but has dependencies from external service providers and suppliers that do not necessarily follow the sectoral governance rules. Examples are mobile device suppliers, mobile network operators, ID service providers, payment service providers etc. These external stakeholders and the sectoral dependencies on their ICT services or ICT products should be documented as well.