MINISTRY OF FINANCE

Information Management Board

Assessment criteria for information security in public administration (Julkri)

Board

Publications of the Ministry of Finance – 2022:74

Publications of the Ministry of Finance 2022:74

Assessment criteria for information security in public administration (Julkri)

Recommendation and criteria

Ministry of Finance Helsinki 2022

Publication distribution

Institutional Repository for the Government of Finland Valto

julkaisut.valtioneuvosto.fi

Publication sale

Online bookstore of the Finnish Government

vnjulkaisumyynti.fi

Ministry of Finance

ISBN pdf: 978-952-367-193-5
ISSN pdf: 1797-9714

Layout: Government Administration Department, Publications

Helsinki 2022 Finland

Description sheet
14 November 2022

Assessment criteria for information security in public administration (Julkri) Recommendation and criteria

Publications of the Ministry of Finance 2022:74		**Subject**	Board
Publisher	Ministry of Finance		
Group author	Information Management Board		
Language	English	**Pages**	182

Abstract

The Act on Information Management in Public Administration (906/2019) lays down obligations relating to information security measures that apply to information management units and authorities as well as to private individuals or corporations or to corporations subject to public law other than those serving as authorities insofar as they perform public administrative tasks. The Act also lays down provisions on a minimum level for information security measures and on an obligation for organisations to monitor the state of the data security of their operating environment and ensure the data security of their datasets and information systems over their entire lifecycle. Organisations shall determine the material risks related to data processing and scale their data security measures in accordance with a risk assessment. With respect to procurement, organisations shall ensure that appropriate data security measures have been implemented in the information system to be acquired.

The recommendation issued by the Information Management Board describes the assessment criteria for information security in public administration (Julkri) and provides instructions for using them. The assessment criteria support the development and assessment of information security in public administration as a whole. The criteria can be used to assess the fulfilment of the information security requirements laid down in the Information Management Act, Security Classification Decree and partly also in the General Data Protection Regulation.

The Information Management Board approved the collection of recommendations on 11 May 2022.

Publication was updated on 15th February 2023, p. 59.

Keywords board, Information Management Board, Information Management Act, public administration, administrative security, physical security, technical security, preparedness, continuity management, information security, data protection, cyber security, risk management, data systems, information management, evaluation

ISBN PDF	978-952-367-193-5	**ISSN PDF**	1797-9714
URN address	https://urn.fi/URN:ISBN:978-952-367-193-5		

Kuvailulehti
14.11.2022

Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri)
Suositus ja kriteeristö

Valtiovarainministeriön julkaisuja 2022:74		**Teema**	Lautakunnat
Julkaisija	Valtiovarainministeriö		
Yhteisötekijä	Tiedonhallintalautakunta		
Kieli	englanti	**Sivumäärä**	182

Tiivistelmä

Julkisen hallinnon tiedonhallinnasta annetussa laissa (906/2019) on säädetty tietoturvallisuustoimenpiteisiin liittyviä vastuita julkisen hallinnon tiedonhallintayksiköille ja viranomaisille sekä yksityisille henkilöille ja yhteisöille taikka muille kuin viranomaisena toimiville julkisoikeudellisille yhteisöille, siltä osin kuin ne hoitavat julkista hallintotehtävää. Lisäksi laissa säädetään tietoturvallisuustoimenpiteiden vähimmäistasosta sekä velvoitteesta seurata toimintaympäristönsä tietoturvallisuuden tilaa ja varmistua tietoaineistojen ja tietojärjestelmien tietoturvallisuudesta koko niiden elinkaaren ajan. Organisaation on tunnistettava olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. Hankintojen osalta organisaation tulee varmistaa, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet.

Tässä tiedonhallintolautakunnan antamassa suosituksessa kuvataan julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri), ja ohjeistetaan sen käytöstä. Arviointikriteeristö tukee koko julkishallinnon tietoturvallisuuden kehittämisen ja arvioinnin tarpeita. Sitä voidaan käyttää apuna arvioitaessa tiedonhallintalaissa, turvallisuusluokitteluasetuksessa sekä osin myös tietosuoja-asetuksessa säädettyjen tietoturvallisuutta koskevien vaatimusten täyttymistä.

Tiedonhallintalautakunta hyväksyi suosituskokoelman kokouksissaan 11.5.2022.

Julkaisu on päivitetty 15.2.2023, s. 59.

Asiasanat lautakunnat, tiedonhallintalautakunta, tiedonhallintalaki, julkinen hallinto, hallinnollinen turvallisuus, fyysinen turvallisuus, tekninen turvallisuus, varautuminen, jatkuvuuden hallinta, tietoturva, tietosuoja, kyberturvallisuus, riskienhallinta, tietojärjestelmät, tiedonhallinta, arviointi

ISBN PDF	978-952-367-193-5	**ISSN PDF**	1797-9714
Julkaisun osoite	https://urn.fi/URN:ISBN:978-952-367-193-5		

Presentationsblad
14.11.2022

Kriterier för bedömning av informationssäkerheten i den offentliga förvaltningen
Rekommendation och kriterier

Finansministeriets publikationer 2022:74		**Tema**	Nämnder
Utgivare	Finansministeriet		
Utarbetad av	Informationshanteringsnämnden		
Språk	engelska	**Sidantal**	182

Referat

I lagen om informationshantering inom den offentliga förvaltningen (906/2019) finns bestämmelser om ansvar i fråga om informationssäkerhetsåtgärder som gäller informationshanteringsenheter och myndigheter inom den offentliga förvaltningen samt privatpersoner, sammanslutningar och offentligrättsliga samfund som inte är myndigheter till den del som de sköter offentliga förvaltningsuppgifter. I lagen finns också bestämmelser om miniminivån för informationssäkerhetsåtgärder och om skyldigheten att följa upp informationssäkerheten i verksamhetsmiljön och försäkra sig om informationssäkerheten i informationsmaterial och informationssystem under hela deras livscykel. Organisationen ska identifiera relevanta risker som är förenade med informationsbehandlingen och dimensionera informationssäkerhetsåtgärderna utifrån riskbedömningen. Vid upphandlingar ska organisationen säkerställa att de aktuella informationssystemen har lämpliga informationssäkerhetsåtgärder.

Den här rekommendationen av informationshanteringsnämnden beskriver kriterierna för bedömning av informationssäkerheten i den offentliga förvaltningen och ger anvisningar om hur de används. Kriterierna för bedömning stödjer behoven av utveckling och bedömning av informationssäkerheten i hela den offentliga förvaltningen. De kan användas som hjälp vid bedömning av hur kraven på informationssäkerhet i informationshanteringslagen, säkerhetsklassificeringsförordningen och delvis i dataskyddsförordningen uppfylls.

Informationshanteringsnämnden godkände rekommendationerna vid sitt möte den 11 maj 2022.

Publikation uppdaterades den 15 februari 2023, s. 59.

Nyckelord	nämnder, informationshanteringsnämnden, lag om informationshanteringslagen, offentlig förvaltning, säkerhet i förvaltningen, fysisk säkerhet, teknisk säkerhet, beredskap, hantering av kontinuiteten, informationssäkerhet, dataskydd, cybersäkerhet, riskhantering, informationssystem, informationshantering, bedömning		
ISBN PDF	978-952-367-193-5	**ISSN PDF**	1797-9714
URN-adress	https://urn.fi/URN:ISBN:978-952-367-193-5		

Contents

1 Introduction

This is a recommendation of the Information Management Board on the Government Information Security Assessment Criteria, hereinafter referred to as *Julkri*, and its use. Julkri supports the development and assessment of information security in the entire public administration. It can be used to assess compliance with the information security requirements laid down in the Information Management Act, the Security Classification Decree and partly also the GDPR.

The recommendation and the appendices to it have been prepared in the division of the government information security assessment criteria set by the Information Management Board for the term 1 May 2021 to 31 December 2021 and in the information security sector division set for the term 1 January to 31 December 2022. Eelis Laine, Senior Specialist at the Ministry of Finance, chaired the division, and Hanna Heikkinen, Information Security Specialist, and Tuula Seppo, Senior Specialist at the Digital and Population Data Services Agency, served as secretaries. The Information Management Board has appointed specialists from different information management units as members of the division. In addition, the division has heard a large number of external specialists at meetings, workshops and seminars. The draft recommendation was open for comments via the public commenting service between 28 March and 19 April 2022.

With regard to data protection, the criteria have been drawn up in cooperation with the Office of the Data Protection Ombudsman. The Office of the Data Protection Ombudsman is responsible for the data protection criteria (Appendix 1B) and other sections related to data protection and provides further information on these. In other respects, further information is provided by the Information Management Board.

The Act on Information Management in Public Administration (906/2019), hereinafter *TihL* or *Information Management Act*, contains provisions on responsibilities related to information security measures for public-administration information-management units and authorities as well as for private persons and organisations or other public-law entities not acting as public authorities, insofar as they carry out a public administrative task. Below, the term *organisation* is used for these objects of information security regulation. The act also contains provisions on the minimum level of information security measures and the obligation to monitor the state of information security in its operating environment and to ensure the information security of data sets and information systems

throughout their lifecycle. The organisation must identify the relevant risks to data processing and dimension information security measures in accordance with the risk assessment. With regard to procurements, the organisation must ensure that appropriate information security measures have been implemented in the information system to be procured.

The Government Decree on Security Classification of Documents in Central Government (1101/2019) (hereinafter referred to as *TLA or the Security Classification Decree*), the Act on the Openness of Government Activities (621/1999), hereinafter referred to as *JulkL* or *Openness Act*, the General Data Protection Regulation ((EU) 2016/679), hereinafter referred to as *GDPR* and the Data Protection Act (1050/2018) have been taken into account in preparing the recommendation. In addition, consideration has been given to the Information security auditing tool for authorities (Katakri) and the Criteria for Assessing the Information Security of Cloud Services (PiTuKri) to ensure consistency.

The security of the authorities' information systems can be assessed by means of audits in accordance with the Act on the Audits of Information Security in Government Information Systems and Communications Arrangements (1406/2011) (hereinafter the *Audit Act*). More information on the audit and approval process can be found in the guide "Assessment and accreditation process of information systems carried out by the Finnish Transport and Communications Agency Traficom".

Organisations may use data protection accreditation compliant with the GDPR as a means of demonstrating compliance with the obligations imposed on the controller or processor. Accreditation under Article 42 of the GDPR does not reduce the responsibility of the controller or processor for compliance with the GDPR and does not restrict the tasks and powers of the Office of the Data Protection Ombudsman. Further information on the accountability of the processing of personal data can be found in the Data Protection Ombudsman's guide "Demonstrate your compliance with data protection regulations".

A facility security clearance pursuant to the Act on Security Clearance (726/2014) may be used to assess the reliability of services provided to an authority. The audit will target a service produced now or in the future from Finland and to the service provider. Further information is available in the Finnish Security and Intelligence Service's guide "Facility security clearance". The assessments of information systems subject to international information security obligations are carried out in accordance with the procedures laid down in the Act on International Information Security Obligations (588/2004). The Ministry for Foreign Affairs acts as Finland's national security authority in the implementation of international information security obligations. Further information is available in the National Security Authority's guidelines.

2 Criteria

This recommendation and its appendices describe the assessment criteria for information security in public administration (Julkri) and the recommendation for its use. The recommendation contains the following appendices:

- Appendix 1A Julkri criteria
- Appendix 1B Data protection criteria
- Appendix 2 Julkri tool (Excel)
- Appendix 3 Julkri tool manual
- Appendix 4 Glossary

The criterion is classified at different levels based on confidentiality, availability and integrity, from which the tool selects the essential and optional criteria based on the security requirements of the object being assessed and the selected use case. In principle, essential criteria should be included in the assessment. Based on the risk assessment and case-by-case judgement, an organisation may also include optional criteria in the assessment and decide which optional criteria to include.

The criteria can be used to assess compliance with the information security requirements laid down in the Information Management Act, the Security Classification Decree and partly also the GDPR. The criteria constitute a recommendation, and the legal requirements can also be met in a manner other than those described in the criteria. In addition to the Katakri[1] and PiTuKri[2] assessment criteria, Julkri also contains public and secret information, preparedness and continuity management, and data protection criteria.

1 Katakri see Katakri – Information security auditing tool for authorities – Ministry for Foreign Affairs (um.fi)

2 PiTuKri see https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf

2.1 Purpose and benefits

The use of the criteria supports organisations in planning, implementing and assessing information security and the protection of personal data. It can be used in assessing legality and as part of the accountability under the GDPR. Organisations can use Julkri in the following situations:

- **In the planning of the service and the specification of requirements** before development or procurement with the aim of identifying the requirements set for the service.
- **In the supplier assessment** with the aim of identifying the requirements for the supplier in the tendering process or as part of the service agreement and ensuring that the requirements are met in the supplier's operations.
- **In service assessment** in relation to the requirements of the procurement and the service agreement.
- **In the assessment of compliance with data protection requirements.**

The criteria support the organisation's risk-based security management. Predetermined use cases facilitate the situation-specific application of the criteria. In addition, it is possible to define organisation-specific use cases for common assessment situations in Julkri. The use cases are discussed in the Julkri tool manual (appendix 3).

The criteria can be used to assess the processing of secret information, personal data and classified information. For security classification level I (TL I – TOP SECRET), the organisation must also take into account case-specific processing requirements.

2.2 Restrictions

Accessibility is mentioned in Julkri as a general criterion in the administrative and technical section. The criteria do not include more detailed accessibility criteria, which means that organisations must take accessibility requirements into account separately. (Act on the Provision of Digital Services 306/2019).

Julkri does not include the assessment of the information security of international classified information (588/2004). NSA, a security authority subordinate to the Ministry for Foreign Affairs, is responsible for the related guidelines and assessment criteria.

The measures covered by the Emergency Powers Act (1552/2011) concerning the continuity of operations in emergency conditions are excluded from the criteria. However, the section on preparedness (VAR) in the criteria that is based on the Information

Management Act also supports the organisation in meeting the requirements concerning preparedness for emergency conditions.

Sector-specific legislation, such as social and health care or financial sector requirements, or the requirements of the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018), are not taken into account in Julkri.

Even though Julkri does not contain requirements arising from international and sector-specific legislation, organisations must nevertheless, in their own activities, identify and take into account the requirements arising from sector-specific legislation, international legislation and EU regulation.

3 Structure and sub-areas of the criteria

The criteria are grouped into **five areas**. Each sub-area has a unique name, which is also the basis of the first part of the identifier of the criteria of the sub-area. The elements of the criteria and their abbreviations are:

- Administrative security (HAL),
- Physical security (FYY),
- Technical security (TEK),
- Preparedness and continuity management (VAR),
- Data protection (TSU).

A sub-area consists of **main criteria** and their complementary **subcriteria**. There are more than two hundred criteria. The main criterion–subcriterion structure has been used, for example, in cases where requirements related to one topic become stricter when moving to higher security levels. For example, the main criterion concerning secret information can be supplemented by a subcriterion specifying how the requirement for security classification level TL IV information is implemented.

Each criterion is classified at different levels from the perspective of confidentiality, integrity, availability and data protection. Depending on the criterion, it may be related to one or more aspects. For example, the same access criterion can be related to confidentiality, integrity, and data protection.

The general descriptions of the different sub-areas of the criteria are described in the following chapters. Individual criteria can be found in appendices 1A and 1B.

3.1 Administrative security

The administrative security section discusses the methods used to implement information security management as part of the entire organisation's operations. The sub-area covers general criteria for administrative security, personnel security, information systems and their procurement, and operational security. The administrative security criteria aim to ensure that organisations have an adequately functioning information security management system and procedures to ensure the proper operation of the personnel

processing the information. The organisation must also ensure that the obligations concerning the processing of data are complied with in situations where the data is processed on behalf of the organisation.

Many of the criteria in the administrative security sub-area serve as a basis for the criteria in other areas. For example, criteria related to the identification, risk management and documentation of objects to be secured are common and should be used by default in connection with the application of criteria in other areas.

Processes related to administrative security must be handled as a whole. Information security management procedures must be proportionate to the information to be protected on the basis of the risk assessment and to the organisation's operations.

The use of the criteria requires an appropriate definition of context. If some activities have already been assessed, the previous results can be used where applicable. For example, if an organisation's IT network environment has been evaluated during the past year and no significant changes have been made to it, this assessment could be used in the assessment of the new information system to be installed in the IT network environment.

If the organisation processes information classified at different levels in separate environments and processes, it may be appropriate to divide the assessment into separate logical components. For example, the content of instructions for personnel in the information processing environment of information classified at a higher level usually differs significantly from the instructions pertaining to the entire organisation.

Good risk management includes documenting procedures and, in particular, documented risk assessment results. Information security management plans and instructions, and the results and conclusions of the evaluation, should be presented in writing. The documents must be supplemented with information on the implementation of the measures. Here documentation refers to a wide range of recordings that can be made available in writing, such as intranet pages and ERP system work orders.

3.2 Physical security

Physical security (FYY) includes criteria for facilities and storage solutions that prevent and restrict unauthorised access to data. In addition, the sub-area describes criteria related to the processing, storage, transfer, transport, and destruction of data. The physical security sub-area can be used in assessing the physical security measures taken to protect data.

The content of the sub-area is based on the Katakri criteria. In particular, efforts have been made to maintain the content of the criteria for handling classified information consistent with Katakri. The clearest differences in relation to Katakri are the exclusion of criteria based on international information security obligations from the sub-area and the classification of certain criteria as applicable to non-classified information.

The structure of the sub-area has been designed so that the common criteria for different security areas, the criteria for administrative areas only, and the criteria for secured areas only have each been compiled in their own sub-sections. This structure differs from the Katakri structure, where some of the criteria have been repeated with the same content in different security areas.

Data material of authorities must be processed and stored in premises that are sufficiently secure for implementing the requirements related to the confidentiality, integrity, and availability of data (section 15(2) of the Information Management Act). For the physical protection of security classified information, the Security Classification Decree provides for two types of physically secured security areas: administrative areas and secured areas. The concepts of administrative area and secured area are used in Julkri.

It is recommended that information resources containing secret information and the information systems used for processing them be placed in a protected area designated for this purpose by an authority, such as the administrative area described in the Security Classification Decree and this recommendation and the attached criteria.

In practice, an administrative area refers to an area specified by the organisation to which unauthorised parties cannot gain uncontrolled access and in which sufficient measures have been implemented to ensure the security of the information processed and stored in the area. No detailed requirements have been set for the structures and other measures in the area. Instead, organisations can plan them using the criteria of the physical (FYY) sub-area in a risk-based manner.

Physical security means the implementation of physical and technical security measures to prevent unauthorised access to data by:

a) ensuring that the information is properly processed and stored,
b) enabling access to information on a need-to-know basis and, where appropriate, security clearance,
c) preventing, blocking and detecting unauthorised activities and
d) preventing or delaying unauthorised intrusion.

In premises where more than one organisation operates, each organisation processing the information must ensure that the security provided by the shared premises is adequate in relation to the physical security requirements that the organisation is subject to.

3.3 Technical security

The technical sub-area covers the criteria related to the technical measures, secure operation and operating models of information systems and networks. The objective of the criteria is to ensure that information systems and their use implement the requirements of general technical information security and, if necessary, data protection. It should be noted, however, that implementing the criteria of the technical sub-area alone does not guarantee the security of an individual information system, but the criteria in other areas must also be taken into account.

The assessment may target either an individual information system or a data processing environment or a broader entity of information systems. When assessing an entity consisting of several information systems, the fulfilment of the requirements in all individual systems must be taken into account.

The technical sub-area also takes into account the location of systems in security areas and their remote use outside security areas. More detailed requirements for the administrative area and secured area have been defined in the sub-area of physical security.

With regard to several criteria, the criteria refer to the fact that the encryption solution must be sufficiently secure for the use case in question. For example, approvals granted by the NCSA function of the National Cyber Security Centre to protect international classified information can be considered in the security assessment of the encryption solution. Further information is available on the website of the National Cyber Security Centre.

3.4 Preparedness and continuity management

Criteria concerning the preparedness and continuity management of normal conditions have been compiled for the area. The criteria are based on the requirements of the Information Management Act (e.g., section 4, subsection 2, item 2, section 13, subsections 1, 2 and 4 and section 15) and on general requirements for guidelines to be drawn up and information security measures, as well as management methods describing the continuity of information security described in the standard ISO/IEC 27002. The measures covered by the Emergency Powers Act concerning the continuity of operations in emergency

conditions are excluded from the criteria. However, the criteria also support the organisation in meeting the requirements for preparing for emergency conditions.

The criteria in this section mainly concern items classified as important or critical in terms of availability. The availability levels are described in section 4.2 Classification levels. The criteria can also be applied on a risk-based basis to lower availability categories.

However, the examination of continuity requirements and the legislation behind them applies in principle to all organisations.

Key criteria in this sub-area include preparedness measures for various serious disruptions, operational continuity plans and recovery plans for information systems, and training for them. Continuity management is closely related to incident and deviation management processes, the criteria of which are described in the HAL and TEK sub-areas.

3.5 Data protection

Personal data include data that can be used to identify a person directly or indirectly, for example by combining individual data with other data that enable identification. A person can be identified, for example, on the basis of a name, a personal identity code, or technical information that identifies the person, or the devices used by the person.

The processing of personal data must comply with the requirements of the GDPR when the processing is entirely or partly automatic or the data form part of the register. The GDPR protects personal data regardless of the technology used in data processing. The storage method of the data is also irrelevant. Data can be stored, for example, in an information system, a video surveillance system, or a paper archive.

The data-protection sub-area contains only criteria concerning the processing of personal data, such as criteria concerning the lawfulness of the processing, data protection principles and the rights of the data subject. In addition, the processing of personal data is subject to the information security criteria of other Julkri sub-areas. In Julkri, the information security criteria applied in the processing of personal data are mostly consistent with other criteria applied to the securing of information. Each criterion in other sub-areas is classified according to whether it also applies to the processing of personal data and, if applicable, whether it concerns all personal data or only special categories of personal data. In some individual cases, the criteria for the processing of personal data in other sub-areas have been specified by a more detailed criterion in the data protection area.

4 Criteria details

An assessment criterion consists of an identifier, classifications (confidentiality, integrity, availability, personal data), contents (name, requirement, general description, and implementation example) and references to different sources.

Table 1. Example of a risk management criterion.

Identifier	HAL-06, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Risk management
Requirement	The organisation implements information security risk management and has assessed the relevant information risks and dimensioned information security measures in accordance with the risk assessment.
Overview	The information security risk management process consists of specifying the operating environment, assessing (identification, analysis, significance assessment), mitigation of risks, accepting risks, risk communication and information exchange, and monitoring and reviewing risks. Information security risk management is part of the organisation's operations and other risk management. Information security risk management ensures the adequacy of information security measures to protect the confidentiality, integrity, and availability of information. Risk management affects other areas of information security management. Risk management must be planned and instructed so that it systematically and in a planned manner addresses various risks related to information security, such as risks arising from errors in information content, risks related to interruptions in the organisation's operations and risks related to personal data breaches.
Implementation example	– A generally accepted method is used to assess and analyse information security risks. – A scheduled annual action plan with a responsible party is drawn up for information security risk assessments. – A sufficient number of specialists are involved in the management of information security risks. – Risks arising from interest groups and supply chains have been taken into account in the management of information security risks. – Information security risk assessment is used in other information security management processes.

Legislation	TihL 13(1); TLA 6, 7
References	Julkri: FYY-01, TEK-01, TEK-14, TEK-16; Katakri: T-03
Other additional information	SFS-EN ISO/IEC 27001:2017 6.1 and 8–10, SFS-EN ISO/IEC 27005:2018 section 6, SFS ISO 31000:2018, PiTuKri TJ-03; Recommendation on the handling of classified documents 2021:5 section 5.2; Collection of recommendations on the application of certain information security regulations 2021:65-chapter 6

The Risk management criterion of the administrative sector is described above as an example. The criterion ID is HAL-06. In this case, the level of confidentiality (L) is public, integrity (E) is low, availability (S) is low, and this criterion can also be used to assess the processing of personal data (TS). Sections 4.1–4.4 describe in more detail the criteria identifiers and their levels.

4.1 Identifier

A criterion has a unique identifier consisting of the abbreviation of the name of the sub-area, a consecutive number of the main criterion and a consecutive number of the subcriterion. The abbreviations of unique identifiers are administrative (HAL), technical (TEK), preparedness (VAR), physical (FYY) and data protection (TSU). The main criteria are numbered by sub-area and the subcriteria by main criterion. For example, in the sub-area of technical information security, TEK-15 is a main criterion and TEK-15.1 and TEK-15.2 are its subcriteria.

4.2 Classification levels

The criteria are classified from the perspective of confidentiality, integrity, and availability. If a criterion also applies to the processing of personal data, it is also classified from the perspective of data protection. Complementary information security perspectives, such as indisputability or authenticity of information, have been taken into account in the content of the criteria.

A criterion may be related to one or more aspects of information security, and it will be selected for evaluation if it is essential from at least one perspective. For example, a criterion may be rated Normal from the perspective of integrity, which means that the criterion is essential for all data classified as Normal from the perspective of integrity.

Many of the criteria are general in nature and are extensively related to information security management. These include criteria related to the specification of tasks and responsibilities, risk management and documentation.

4.2.1 Levels of confidentiality

Confidentiality is a feature of information that reflects the fact that the information is available only to those entitled to use it and is not disclosed to third parties. This recommendation describes the levels of confidentiality on a scale of public, secret, security classification level IV (TLIV), security classification level III (TLIII), security classification level II (TLII) and security classification level I (TLI). The table describes these levels and examples. The recommendation of the Information Management Board (2021:5) contains recommendations on security classification, labelling of classified documents, and information security measures concerning the processing of classified documents.

Table 2. Levels of confidentiality.

Level	Description	Example
Public	Official documents shall be in the public domain, unless specifically provided otherwise in this Act or another Act. (JulkL section 1)	The minutes of municipal council with respect to their public parts, the public website of an organisation.
Secret	An official document shall be secret if it has been so provided in this Act or another Act, or if it has been declared secret by an authority on the basis of an Act, or if it contains information covered by the duty of non-disclosure, as provided in an Act. (JulkL section 22)	Patient records, information on social welfare clients, psychological tests and aptitude tests.
Security classification level IV (TL IV)	The unauthorised disclosure or unauthorised use of the secret information contained in the document can be **disadvantageous** to the interests to be protected that are referred to in section 18, subsection 1 of the Information Management Act.	Documentation of the security arrangements of an information system that is essential for the interests to be protected referred to in TihL section 18, the disclosure of which does not interrupt the operation, but may require changes in the disclosed plans.

Level	Description	Example
Security classification level III (TL III)	The unauthorised disclosure or unauthorised use of the secret information contained in the document can cause **prejudice** to the interests to be protected that are referred to in section 18, subsection 1 of the Information Management Act.	Documentation of the security arrangements of functions that are vital to the interests to be protected referred to in TihL section 18, the disclosure of which requires the interruption of operations.
Security classification level II (TL II)	The unauthorised disclosure or unauthorised use of the secret information contained in the document can cause **significant prejudice** to the interests to be protected that are referred to in section 18, subsection 1 of the Information Management Act.	Documentation of the security arrangements of functions that are vital to the interests to be protected referred to in TihL section 18, the disclosure of which makes it impossible to guarantee the safety of a large group of people and, as a result, operations must be interrupted for a long period of time.
Security classification level I (TL I)	The unauthorised disclosure or unauthorised use of the secret information contained in the document can cause **exceptionally grave prejudice** to the interests to be protected that are referred to in section 18, subsection 1 of the Information Management Act.	The disclosure of information on the functional capacity of society, such as critical infrastructure or critical security arrangements of a vital activity, from the perspective of the interests to be protected referred to in section 18 of the Act, which disclosure is likely to prevent the activities of an authority or other critical infrastructure operator and cause extensive damage.

From the perspective of confidentiality, the criteria have not been classified separately to the level Discretionary availability. Based on the risks, organisations must consider, on the basis of the risks, whether criteria for secret information are included in the assessment of information provided on discretion. This can be accomplished by setting the confidentiality level in the assessment prerequisites to Public, in which case the Julkri tool provides optional criteria for secret information.

4.2.2 Levels of availability

Availability refers to how information, an information system or a service can be used at the desired time and in the required manner. In Julkri, availability levels are minor, normal, important, and critical. The table describes and gives examples of different levels of availability.

Table 3. Levels of availability.

Level	Description	Example
Minor	With regard to the availability of information, disruptions lasting several weeks can be accepted.	Register of personnel parking places, fault register of park benches
Normal	With regard to the availability of information, disruptions lasting days at most can be accepted.	Archive system
Important	With regard to the availability of information, disruptions lasting hours at most can be accepted.	Patient information system
Critical	With regard to the availability of information, disruptions lasting minutes at most can be accepted.	Centralised user authentication services

4.2.3 Levels of integrity

Integrity is a feature of information that means that the information has not been altered without authorisation or that it has not been altered accidentally and that any changes can be verified. The table describes the minor, normal and important levels of integrity used in Julkri, as well as some examples given to the levels.

Table 4. Levels of integrity.

Level	Description	Example
Minor	The loss or alteration of information does not cause material harm.	Office software, system error logs.
Normal	The loss or alteration of information causes reasonable harm, but this can be detected and recovered from.	Human resources systems.
Important	The loss or alteration of information causes significant harm or damage to reputation, and it may be difficult to detect it.	Integration platforms that relay laboratory results, where it may be difficult to detect errors in individual measurements. Log data related to the processing of personal data.
Critical	The loss or alteration of information is not acceptable under any circumstances.	Payment systems essential to the functioning of society or rail traffic control systems

4.3 Contents

The content of the criteria consists of the name, requirement, overview and implementation example.

- The **name** describes, at a heading level, the subject of the criterion. The name is one or a few words describing the subject of the criterion. The name of the subcriteria consists of the name of the main criterion and a qualifier separated by a dash. For example, Access rights – timeliness, which is a subcriterion of timeliness that specifies access rights as the main criteria.
- The **requirement** describes the objective that the organisation must meet. The requirement is a short sentence or a short paragraph. Requirements can be met in several ways. Requirements are specific, i.e., one requirement does not include several different requirements. If a subcriterion does not contain a separate requirement, the subcriterion specifies the main criterion in terms of either the general description or the implementation example.
- The **overview** contains additional information that provides background and justification for the criterion. It is not a requirement but a justification for the criterion. For example, the overview may describe threats that are prevented by means of management methods that comply with the criterion. If several subcriteria are associated with one entity, a common overview will be prepared for the different criteria only once in the main criterion.
- The **implementation example** describes how the organisation can implement the requirement. An implementation example is not a requirement, but it can serve as a guideline for the level of compliance with the requirement.

4.4 References

A criterion may include references to legislation, guidelines and standards, as well as references to the Katakri and PiTuKri assessment criteria and other Julkri criteria. An effort has been made to specify the references so that the corresponding section can be quickly found in the reference material.

- The **legislation** describes the legislation on which the criterion is based.
- **Other additional information** includes references to the recommendations by the Information Management Board related to the criterion, the PiTuKri assessment criteria and standards.
- A **Julkri reference** contains a reference to one or more other Julkri criteria if the criterion forms an applicable whole together with another criterion.
- A **Katakri reference** contains a reference to the corresponding criterion in the Katakri assessment criteria, if one exists.

5 Using the criteria

The criteria can be applied to the activities of an entire organisation, to the activities of a sub-area or to the assessment of a service to be procured. It is recommended that processing environments intended for different levels of data be assessed separately, so that lower-level objects are not subject to excessively high criteria and thus do not unnecessarily increase complexity and costs.

The precise specification and restriction of the subject of the assessment is one of the most important stages in the use of the criteria. The assessment may focus on an individual system, but it must also be ensured that all various evaluations together cover the entire organisation's operations.

The organisation processes information belonging to many different categories of criticality and confidentiality, and many different information systems and services are used in the processing. In addition, common platform services are often used in connection with various information systems. Because of these factors, the organisation should plan the objects to be assessed as logical entities and use previously conducted assessments.

For example, if a new information system is acquired, which will be operated on a common platform whose security has already been assessed, the previously assessed criteria for the common platform can be excluded from the assessment of the new information system.

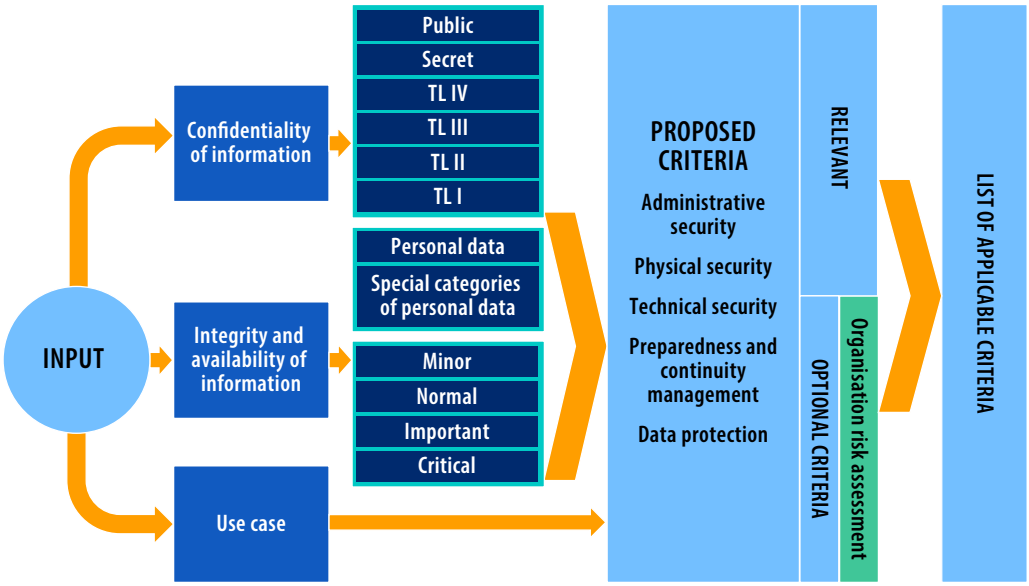
Use cases allow the organisation to specify in advance criteria suitable for different situations and thus facilitate the use of the criteria in similar situations. The use of use cases is described in more detail in appendix 3, Tool manual.

Before using the criteria, the organisation must determine the following aspects of the subject of the assessment:

- confidentiality, integrity, and availability to be required of the object to be assessed,
- whether the object to be assessed includes personal data and whether such data belong to special categories of personal data,
- any areas to be excluded from the assessment,
- use case, if a use case suitable for the assessment exists.

Based on the classification of the object to be assessed, the criteria are relevant, optional or excluded from the assessment. It is recommended that the organisation include the relevant criteria in the assessment. For optional criteria, the organisation decides on the inclusion of each criterion on the basis of a risk assessment and context-sensitive consideration. Figure 1 shows the process of using the criteria.

Figure 1. Illustration of applying the criteria.



When using the Julkri criteria in an organisation's information security assessment, the requirements of the criteria included in the assessment must be met as a rule. However, an organisation may choose not to meet a criterion included in the assessment if the organisation can demonstrate that there is no risk or that the risk is at an acceptable level despite the non-compliance with the criterion. For example, risks have been sufficiently mitigated by other means, using compensatory controls. However, any requirements arising directly from legislation must be met as required by the legislation.

If the organisation needs a certificate of compliance with Julkri criteria, all the criteria included in the assessment must be met in the object of the assessment. However, where the implementation of the criterion is not possible, compensatory procedures must be identified and justified to ensure that the risk remains at an acceptable level despite the non-implementation of the criterion.

The criteria can be used to assess compliance with the information security requirements laid down in the Information Management Act, the Security Classification Decree and partly also the GDPR. The criteria constitute a recommendation, and the legal requirements can also be met in a manner other than those described in the criteria.

5.1 Pre-assessment steps

Before starting the evaluation, it is recommended that the security of procurements be ensured, the risks of legislative derivatives be examined and the contractual terms be suited for the purpose. This applies primarily to assessments of information systems or services. The administrative security criteria HAL-06 and HAL-06.1 and the procurement security criteria HAL-16 and HAL-16.1 can be used in this. The above preceding measures are briefly described in the following sections.

Arrangement of secure data processing

The organisation must ensure in its procurements that appropriate information security measures have been implemented for the information systems and services used. The organisation must ensure in advance that the confidentiality and protection of the information are properly in place.

Risks derived from legislation

The organisation must identify risks derived from legislation, which means the possibilities under the laws of different countries to oblige a service provider to cooperate with the authorities of the country in question and, for example, provide direct or indirect access to secret information of the customers of the service or system.

System and service contracts

It must be verified in the contractual terms of the service or system service provider that they do not limit the suitability of the service or system for the use case in question throughout their lifecycle.

SOURCES

Regulations

Conscription Act (1438/2007). https://www.finlex.fi/fi/laki/ajantasa/2007/20071438. Referenced on 26 April 2022.
Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679. Referenced on 26 April 2022.
(Act on the Provision of Digital Services 306/2019). https://www.finlex.fi/fi/laki/ajantasa/2019/20190306. Referenced on 26 April 2022.
Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018). https://www.finlex.fi/fi/laki/ajantasa/2018/20181054. Referenced on 26 April 2022.
Act on Information Management in Public Administration (906/2019). https://finlex.fi/fi/laki/ajantasa/2019/20190906. Referenced on 26 April 2022.
Act on International Information Security Obligations (588/2004). https://www.finlex.fi/fi/laki/ajantasa/2004/20040588. Referenced on 26 April 2022.
Act on the Audits of Information Security in Government Information Systems and Communications Arrangements (1406/2011). https://www.finlex.fi/fi/laki/ajantasa/2011/20111406. Referenced on 26 April 2022.
Act on the Openness of Government Activities (621/1999). https://www.finlex.fi/fi/laki/ajantasa/1999/19990621.
Referenced on 26 April 2022.
Data Protection Act (1050/2018). https://www.finlex.fi/fi/laki/ajantasa/2018/20181050. Referenced on 26 April 2022.
Security Clearance Act (726/2014). https://www.finlex.fi/fi/laki/ajantasa/2014/20140726. Referenced on 26 April 2022.
Working Time Act (872/2019). https://www.finlex.fi/fi/laki/ajantasa/2019/20190872. Referenced on 26 April 2022.
Act on Collective Agreements for Public Officials in Central Government (664/1970). https://www.finlex.fi/fi/laki/ajantasa/1970/19700664. Referenced on 26 April 2022.
Government Decree on Security Classification of Documents in Central Government (1101/2019). https://www.finlex.fi/fi/laki/ajantasa/2019/20191101. Referenced on 26 April 2022.
Emergency Powers Act (1552/2011). https://www.finlex.fi/fi/laki/ajantasa/2011/20111552. Referenced on 26 April 2022.

Recommendations of the Information Management Board

Recommendation of the Information Management Board – Ministry of Finance 2021:65. Collection of recommendations on the application of certain information security regulations. http://urn.fi/URN:ISBN:978-952-367-897-2.
Recommendation of the Information Management Board – Ministry of Finance 2021:5. Recommendation on the handling of classified documents. http://urn.fi/URN:ISBN:978-952-367-500-1.
Recommendation of the Information Management Board – Ministry of Finance 2022:4. Handling of classified documents in cloud computing services. http://urn.fi/URN:ISBN:978-952-367-906-1

Instructions and other materials

BSI IT-Grundschutz-Compendium 2021. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2021.pdf. Referenced on 26 April 2022
CIS Critical Security Controls. https://www.cisecurity.org/controls. Referenced on 26 April 2022.
Hansel. 2017. Tietosuoja-asetuksen huomioiminen kilpailutettaessa julkisia hankintoja. Version 1. tietosuojaohje.pdf (hansel.fi). Referenced on 28 April 2022.
Katakri 2020 Information security auditing tool for authorities. https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246. Referenced on 26 April 2022.
NIST SP 800 series. https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information. Referenced on 26 April 2022.

NIST. In particular, 800–53 (Security and Privacy Controls), 800–37 (Risk Management Framework), 800- 63B (Authentication and Lifecycle Management). https://csrc.nist.gov/publications/sp800. Referenced on 26 April 2022.
PiTuKri 2020 Criteria for Assessing the Information Security of Cloud Services. https://www.kyberturvallisuuskeskus.fi/sites/ default/files/media/file/PiTuKri_v1_1_english.pdf. Referenced on 26 April 2022.
Finnish Security Intelligence Service Finnish Security Intelligence Service guide: Facility Security Clearance". https://supo.fi/yritysturvallisuusselvitys. Referenced on 26 April 2022
Office of the Data Protection Ombudsman Demonstrate your compliance with data protection regulations. https://tietosuoja.fi/osoitusvelvollisuus. Referenced on 26 April 2022.
The Security Committee (2017). Security Strategy for Society. https://turvallisuuskomitea.fi/yhteiskunnan-turvallisuusstrategia/. Referenced on 26 April 2022.
Traficom 2021. Assessment and accreditation process of information systems carried out by the Finnish Transport and Communications Agency Traficom. The perspective of the client organisation. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje_NCSA-toiminnon_suorittamat_tietoturvallisuustarkastukset.pdf. Referenced on 26 April 2022.
Traficom 2021. Cryptography solutions approved by Traficom's NCSA-FI. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/ncsa/liikenne-ja-viestintavirasto-traficomin-ncsa-toiminnon-hyvaksymat-salausratkaisut. Referenced on 26 April 2022.
Ministry for Foreign Affairs. National security authority. https://um.fi/kansallinen-turvallisuusviranomainen. Referenced on 26 April 2022
Ministry of Finance (2020:73). Guidelines on using cloud services. Practical guidelines for public sector organisations on making use of cloud computing services. http://urn.fi/URN:ISBN:978-952-367-503-2

General checklists and hardening instructions

CIS Benchmarks. https://www.cisecurity.org/cis-benchmarks/. Referenced on 26 April 2022.
DISA Security Technical Implementation Guides (STIGs). https://public.cyber.mil/stigs/. Referenced on 26 April 2022.
NIST – National Checklist Program Repository. https://ncp.nist.gov/repository. Referenced on 26 April 2022.

Attachments

Appendix 1A: Julkri criteria

1 Structure and sub-areas of the criteria

The criteria are grouped into **five areas**. Each sub-area has a unique name, which is also the basis of the first part of the identifier of the criteria of the sub-area. The elements of the criteria and their abbreviations are:

- Administrative security (HAL),
- Physical security (FYY),
- Technical security (TEK),
- Preparedness and continuity management (VAR) and
- Data protection (TSU).

A sub-area consists of **main criteria** and their complementary **subcriteria**. There are more than two hundred criteria. The main criterion–subcriterion structure has been used, for example, in cases where requirements related to one topic become stricter when moving to higher security levels. For example, the main criterion concerning secret information can be supplemented by a subcriterion specifying how the requirement for security classification level TL IV information is implemented.

Each criterion is classified at different levels from the perspective of confidentiality, integrity, availability and data protection. Depending on the criterion, it may be related to one or more aspects. For example, the same access criterion can be related to confidentiality, integrity and data protection.

The general descriptions of the different areas of the criteria and the criteria included in the sub-area appear in the following sections. A general description and criteria of the data protection sub-area can be found in appendix 1B Data protection criteria.

2 Administrative security

The administrative security section discusses the methods used to implement information security management as part of the entire organisation's operations. The sub-area covers general criteria for administrative security, personnel security, information systems and their procurement, and operational security. The administrative security criteria aim to ensure that organisations have an adequately functioning information security management system and procedures to ensure the proper operation of the personnel processing the information. The organisation must also ensure that the obligations concerning the processing of data are complied with in situations where the data is processed on behalf of the organisation.

Many of the criteria in the administrative security sub-area serve as a basis for the criteria in other areas. For example, criteria related to the identification, risk management and documentation of objects to be secured are common and should be used by default in connection with the application of criteria in other areas.

Processes related to administrative security must be handled as a whole. Information security management procedures must be proportionate to the information to be protected on the basis of the risk assessment and to the organisation's operations.

The use of the criteria requires an appropriate definition of context. If some activities have already been assessed, the previous results can be used where applicable. For example, if an organisation's IT network environment has been evaluated during the past year and no significant changes have been made to it, this assessment could be used in the assessment of the new information system to be installed in the IT network environment.

If the organisation processes information classified at different levels in separate environments and processes, it may be appropriate to divide the assessment into separate logical components. For example, the content of instructions for personnel in the information processing environment of information classified at a higher level usually differs significantly from the instructions pertaining to the entire organisation.

Good risk management includes documenting procedures and, in particular, documented risk assessment results. Information security management plans and instructions, and the results and conclusions of the evaluation, should be presented in writing. The documents must be supplemented with information on the implementation of the measures. Here documentation refers to a wide range of recordings that can be made available in writing, such as intranet pages and ERP system work orders.

Identifier	HAL-01, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Principles
Requirement	The organisation has information security principles approved by the top management, which describe the connection between the organisation's information security measures and the organisation's operations and are comprehensive and appropriate in terms of data protection.
Overview	The information security principles approved by the top management demonstrate that the management is committed to the organisation's information security principles and that the principles represent the management's intent and support the organisation's operations. The principles can be described in many different ways, for example as an individual document or as part of general operating principles, policies or strategies.
Implementation example	
Legislation	TihL 4(2), 13
References	Katakri: T-01
Other additional information	ISO/IEC 27002:2022 5.1; SFS-EN ISO/IEC 27001:2017 5.1, 5.2, 5.3, 9.3; PiTuKri TJ-01

Identifier	HAL-02, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Tasks and responsibilities
Requirement	The organisation has specified and documented the tasks and responsibilities of information security management, including the responsibilities of service providers.
Overview	The purpose of specifying the tasks and responsibilities of information security work is to ensure that actors have been assigned in the key areas and that they are aware of their own responsibilities and authorisations. The task of the organisation's management is to determine the responsibilities related to information management. It is not a question of delegating information management responsibilities, but of setting them. In particular, responsibilities should be specified for the maintenance of security instructions, risk management, preparedness and for the persons responsible for overall security. The areas of responsibility for information security are usually specified as part of the overall responsibility for security. When specifying responsibilities, the tasks that the supplier is responsible for must also be taken into account. When using cloud services, different service models and their differences in the division of responsibilities between the customer and the service provider must be taken into account.
Implementation example	The organisation has specified the tasks of implementing security and related responsibilities in the following areas: a) security management b) physical security c) technical security d) preparedness and continuity management e) data protection f) risk management g) overall responsibility for security
Legislation	TihL 4(2)
References	Katakri: T-02
Other additional information	ISO/IEC 27002:2022 5.2; SFS-EN ISO/IEC 27001:2017 5.1, 5.2, 5.3; PiTuKri TJ-02; Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa (Recommendations on the implementation of management responsibilities in information management) 2020:18, chapter 3

Identifier	HAL-02.1, C:Secret, I:Important, A:Important, DP:Special category of personal data
Title	Tasks and responsibilities – separation of duties
Requirement	The organisation must ensure that persons do not have work combinations that are hazardous for information security
Overview	The tasks and responsibilities of the organisation must be differentiated in order to reduce the risk of unauthorised or unintentional modification or misuse of the organisation's assets to be protected. Such hazardous combinations include, for example, one person being able to change both information system data and the log data used for monitoring the information system. Hazardous work combinations must also be taken into account in outsourced operations.
Implementation example	- The organisation has specified hazardous work combinations - Hazardous work combinations are reviewed as part of task specifications - Hazardous work combinations are reviewed as part of user rights management, especially in the case of super user and monitoring roles
Legislation	TihL 4(2), 13
References	Katakri: I-06
Other additional information	ISO/IEC 27002:2022 5.3
Identifier	**HAL-03, C:Public, I:Minor, A:Minor, DP:Personal data**
Title	Resources
Requirement	The organisation has sufficient resources and expertise to ensure information security.
Overview	Resourcing and expertise ensure that information security work can be carried out in accordance with the specified principles. Resources of information security work refer to both human resources and financial investments, such as information system investments. As general requirements, it can be considered that the organisation must have persons for the tasks required by information security management and that the persons must have competence and time to perform the required tasks. In addition, the organisation must have the ability and willingness to make investments related to information security that have been identified as necessary on the basis of information security requirements and risk assessment.
Implementation example	- People performing information security tasks have sufficient expertise and there is evidence of the expertise. - The resources, tasks, responsibilities and authorisations of information security work have been specified with sufficient coverage in regard to the organisation's operations, size and risks. - The resources are sufficient to create, implement, maintain and continuously improve the information security management system. - The adequacy of resources is assessed regularly. - The organisation makes the necessary decisions on equipment and other investments required for information security

Legislation	TihL 4(2)
References	Katakri: T-05
Other additional information	SFS-EN ISO/IEC 27001:2017 7.1, 7.2, 5.1
Identifier	**HAL-04, C:Public, I:Minor, A:Minor, DP:Personal data**
Title	Asssets
Requirement	The organisation identifies the assets to be protected and keeps up-to-date documentation of them.
Overview	Listing the assets to be protected is one of the basic requirements for information security management. The assets to be protected include information, information systems, information processing processes, facilities and other objects that may affect the organisation's information security. In today's computing environments, assets to be protected may also include non-traditional IT objects, such as various sensor and analysis devices, and IoT and automation environments. Listing the assets to be protected is a necessary step for systematic and effective information security management. An up-to-date list of the assets to be protected is used as source data in many sub-areas of information security management.
Implementation example	
Legislation	TihL 5(2), 13
References	
Other additional information	ISO/IEC 27002:2022 5.9; Recommendation for an information management model 2020:29
Identifier	**HAL-04.1, C:Public, I:Minor, A:Minor, DP:Personal data**
Title	Assets – responsibilities
Requirement	The organisation specifies the responsibilities for the assets to be protected.
Overview	
Implementation example	
Legislation	TihL 4(2)
References	
Other additional information	ISO/IEC 27002:2022 5.9; Recommendation for an information management model VM 2020:29
Identifier	**HAL-04.2, C:Public, I:Minor, A:Minor, DP:Personal data**
Title	Assets – classification
Requirement	The organisation must classify the information and related systems and processes on the basis of the requirements applicable to them.

Overview	Using legislation as a reference, the organisation must identify the public, secret, classified and personal data it processes and the needs to protect them. Classification refers to the need to protect information at different levels due to different processing requirements. By classifying information processing environments according to the data material, it is easier to demonstrate and justify the information security measures related to each information processing environment. Classification should be included in the organisation's processes and be consistent and harmonised throughout the organisation. Classification serves as input data for several other information security processes. For example, system availability requirements are related to the planning of system fault tolerance and preparedness, and confidentiality requirements are related to the specification of system information security requirements. The classification of an information system or other object containing multiple data sets is primarily determined by the material of the highest classification. When assessing the classification of information systems, the cascade effect should also be taken into account in a risk-based manner. In information systems consisting of a large number of data at a certain level of confidentiality, the subject matter may rise to a higher level than that of individual data. However, this volume is not the only factor: sometimes combining, for example, two different data sources can lead to an increase in the classification of the data repository. Typically, cascading is about classification level IV information (for example, a large volume of security classification level IV information can, as a combination, constitute a security classification level III data warehouse).
Implementation example	- The organisation determines the levels used in classifying information, related information systems and processing with regard to confidentiality, availability, integrity. If necessary, the classification can be extended to cover other aspects, such as whether the data contains personal data. - The organisation determines the criteria for classifying data and other items into different categories. - The categories and the related criteria are based on statutory requirements, but organisations must specify the criteria so that they are appropriate for the persons working in the organisation. - Classification can be performed when listing the items to be protected, and it can be included in the list of data to be protected, for example, in a data management model.
Legislation	TihL 4(2), 5, 13, 18; TLA 3, 4; JulkL 24
References	Katakri: T-08
Other additional information	Collection of recommendations on the application of certain information security regulations 2021:65, chapter 4.1; Recommendation on the handling of classified documents 2021:5 chapter 2, chapter 5.3; ISO/IEC 27002:2022 5.9
Identifier	**HAL-04.3, C:Secret, I:, A:, DP:Special category of personal data**
Title	Assets – cascade effect
Requirement	The cascade effect has been taken into account in the classification of the assets to be protected.
Overview	The classification of an information system or other object containing multiple data sets is primarily determined by the material of the highest classification. When assessing the classification of information systems, the cascade effect should also be taken into account in a risk-based manner. In information systems consisting of a large number of data at a certain level of confidentiality, the subject matter may rise to a higher level than that of individual data. However, this volume is not the only factor: sometimes combining, for example, two different data sources can lead to an increase in the classification of the data repository. Typically, cascading is about classification level IV information (for example, a large volume of security classification level IV information can, as a combination, constitute a security classification level III data warehouse), but the cascade effect must also be taken into account in the protection of unclassified secret information.

Implementation example	
Legislation	TihL 5(2), 13(1)
References	Julkri: HAL-06, TEK-06; Katakri: T-08
Other additional information	
Identifier	**HAL-04.4, C:Secret, I:, A:, DP:Special category of personal data**
Title	Assets – labelling
Requirement	The organisation must label the information in accordance with the legal requirements and the classification principles specified by the organisation.
Overview	The ways in which the information is labelled must cover both physical and digital information and the related property to be protected, such as storage media. The labels should comply with the classification principles specified by the organisation and be easily identifiable. The organisation should provide guidance on where and how to attach the labels. Printouts must also be taken into account in the instructions. In addition, in order to avoid unnecessary work, it is advisable to provide instructions on when labelling is not needed. In certain cases, such as the secrecy markings referred to in the Openness Act, the labels must also indicate to what extent the document must be kept secret and on what grounds the secrecy is based.
Implementation example	
Legislation	TihL 18; TLA 3, 4; JulkL 25
References	Katakri: T-08
Other additional information	Recommendation on the handling of classified documents 2021:5 chapter 3; ISO/IEC 27002:2022 5.13
Identifier	**HAL-04.5, C:Public, I:Minor, A:Minor, DP:Personal data**
Title	Assets – dependencies
Requirement	The organisation has identified and documented dependencies between the assets to be protected.
Overview	
Implementation example	
Legislation	TihL 5
References	
Other additional information	

Identifier	HAL-04.6, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Assets – interest groups
Requirement	The organisation has identified and documented the interest groups involved with the assets to be protected.
Overview	
Implementation example	
Legislation	TihL 5
References	
Other additional information	

Identifier	HAL-05, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Requirements
Requirement	The organisation identifies information security requirements arising from legislation, interest groups and the organisation's operations.
Overview	The organisation must identify and itemise information security requirements arising from legislation, agreements with different interest groups and the organisation's operations. In addition, the organisation must identify and take into account requirements arising from sector-specific legislation, international legislation and EU regulations. The minimum information security requirements based on the Information Management Act and the recommendations on compliance with these requirements are specified in chapter 2 of the Information Management Board's recommendation 2021:65. The organisation's information security requirements consist of the above-mentioned minimum requirements and other identified requirements. The process of implementing each requirement is assessed through a risk assessment process.
Implementation example	
Legislation	TihL 13
References	
Other additional information	SFS-EN ISO/IEC 27001:2017 4.2; Collection of recommendations on the application of certain information security regulations 2021:65 chapters 2 and 4

Identifier	HAL-05.1, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Requirements – monitoring
Requirement	The organisation monitors changes in the set information security requirements and operating environment and takes the necessary measures to respond to them.
Overview	Legislation, contract requirements and changing information security threats require regular monitoring of requirements and threats and responding to changes.
Implementation example	
Legislation	TihL 4(2), 13(1)
References	
Other additional information	SFS-EN ISO/IEC 27001:2017 9.1; Collection of recommendations on the application of certain information security regulations 2021:65 chapter 4.1

Identifier	HAL-05.2, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Requirements – change effects
Requirement	The organisation assesses the impacts of changes in essential administrative reforms and the introduction of information systems in relation to information security requirements and measures.
Overview	In connection with material changes, organisations are required to assess the impact of changes. As part of the impact assessment, the impacts of the changes must be assessed in relation to information security requirements and measures.
Implementation example	
Legislation	TihL 5
References	
Other additional information	Recommendation on the Assessment of the Transformative Impact of Information Management 2020:53; ISO/IEC 27002:2022 5.31

Identifier	HAL-06, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Risk management
Requirement	The organisation implements information security risk management and has assessed the relevant information risks and dimensioned information security measures in accordance with the risk assessment.
Overview	The information security risk management process consists of specifying the operating environment, assessing (identification, analysis, significance assessment), mitigation of risks, accepting risks, risk communication and information exchange, and monitoring and reviewing risks. Information security risk management is part of the organisation's operations and other risk management. Information security risk management ensures the adequacy of information security measures to protect the confidentiality, integrity, and availability of information. Risk management affects other areas of information security management. Risk management must be planned and instructed so that it systematically and in a planned manner addresses various risks related to information security, such as risks arising from errors in information content, risks related to interruptions in the organisation's operations and risks related to personal data breaches.

Implementation example	- A generally accepted method is used to assess and analyse information security risks. - A scheduled annual action plan with a responsible party is drawn up for information security risk assessments. - A sufficient number of specialists are involved in the management of information security risks. - Risks arising from interest groups and supply chains have been taken into account in the management of information security risks. - Information security risk assessment is used in other information security management processes.
Legislation	TihL 13(1); TLA 6, 7
References	Julkri: FYY-01, TEK-01, TEK-14, TEK-16; Katakri: T-03
Other additional information	SFS-EN ISO/IEC 27001:2017 6.1 and 8–10; SFS-EN ISO/IEC 27005:2018 section 6; SFS ISO 31000:2018; PiTuKri TJ-03; Recommendation on the handling of classified documents 2021:5 section 5.2; Collection of recommendations on the application of certain information security regulations 2021:65 chapter 6
Identifier	**HAL-06.1, C:Secret, I:, A:, DP:Personal data**
Title	Risk management – risks derived from legislation
Requirement	Risks related to the service, derived from legislation, have been identified, assessed and managed.
Overview	Risks derived from legislation refer to the possibilities under the laws of different countries to oblige a service provider to cooperate with the authorities of the country in question and, for example, provide direct or indirect access to secret information of the customers of a service. Risks derived from legislation may extend to both the physical location of confidential information and, for example, the disclosure of information through management connections from another country. In many countries, statutory disclosure of information and the right of investigation are limited to the police and intelligence authorities. The organisation must ensure that risks derived from legislation do not limit the suitability of the service for its purpose. The assessment of risks derived from legislation takes into account the supply chain used to provide the entire service and the provisions of the states under which the service is provided, and the risk of unauthorised disclosure of information to the authorities of those states. In accordance with the recommendation Handling of classified documents in cloud computing services (Ministry of Finance 2022:4), it is recommended in order to manage the risks associated with cloud services that only cloud services and providers assessed as reliable by the authorities be used. In addition, if classified data are processed in international cloud services, it is recommended that the classified data to be processed be strictly limited and selected on the basis of use cases and related official processes and in such a way that they can be disclosed to states under whose jurisdiction the cloud service provider and its subcontractors fall.

Implementation example	The risk assessment should cover risks derived from legislation for at least the following factors: a) the physical location of the information processed in the service throughout its lifecycle, including any subcontracting and outsourcing chains b) the physical location of the various functions of the service (e.g., maintenance and management solutions, backups) and components throughout the data lifecycle c) any other parties involved in the provision of the service, such as subcontracting and outsourcing chains d) the legislation and jurisdiction applicable to the use of the service and the information processed in the service e) entities that may have access to the data processed in the service due to applicable legislation In order to assess risks derived from legislation, the service provider must be required to provide descriptions of the risks derived from legislation associated with the information processed in the service in question. The descriptions must be such as to enable a reliable assessment of the overall suitability of the service in question for the customer's use case. The descriptions must cover the use of the service and the entire lifecycle of the data processed in the service, also taking into account the contents of the aforementioned items a–e. It is recommended that the general principles of further evaluation described in PiTuKri (EE-02/table 2) be followed in the assessment. When protecting secret information that is not security classified, it should be noted that the protection of such information can be subject to more extensive risks derived from legislation than security classified information.
Legislation	TihL 13(1); TLA 6, 7
References	Julkri: FYY-01, TEK-01, TEK-14, TEK-16, TSU-18; Katakri: T-03
Other additional information	SFS-EN ISO/IEC 27001:2017 6.1 and 8–10; SFS-EN ISO/IEC 27005:2018 section 6; SFS ISO 31000:2018; PiTuKri TJ-03 and EE-02; Recommendation on the handling of classified documents 2021:5 section 5.2; Collection of recommendations on the application of certain information security regulations 2021:65 chapter 6
Identifier	**HAL-07, C:Public, I:Minor, A:Minor, DP:Personal data**
Title	Monitoring and supervision
Requirement	The organisation has organised monitoring and supervision of the functioning of information security processes and compliance with the requirements.
Overview	The organisation must monitor the state of information security in its operating environment and ensure the information security of information materials and information systems throughout their lifecycle. The lifecycle of information begins at the production or reception stage and ends with the permanent storage of the data in the archive or the destruction of the data. The lifecycle of data covers all stages of data processing, which are data production or receipt, storage, use, sharing, transfer and archiving or destruction. Indicators based on the performance and effectiveness of management methods, which can be numerical or qualitative, can be used as indicators for monitoring information security. The monitoring is based on observed deviations, on the basis of which proposals for developing information security are prepared. The indicators can be, for example, numerical threshold values (e.g., availability of services at least 99%) or verification of compliance (e.g., assessments and reviews according to the year schedule have been carried out as planned).

Implementation example	An organisation that handles a lot of confidential information has specified, for example: a) what needs to be monitored and measured b) which monitoring, measurement, analysis or evaluation methods ensure valid results c) when monitoring and measurement must be carried out d) who carries out monitoring and measurement e) when the results of monitoring and measurement must be analysed and evaluated f) who analyses and evaluates the results obtained
Legislation	TihL 4(2), 13(1)
References	Katakri: T-01, I-19
Other additional information	SFS-EN ISO/IEC 27001:2017 9.1; Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa (Recommendations on the implementation of management responsibilities in information management) 2020:18, chapter 7
Identifier	**HAL-07.1, C:Public, I:Minor, A:Minor, DP:Personal data**
Title	Monitoring and supervision – use and disclosure of data
Requirement	The organisation has identified the requirements related to the collection of log data and, based on them, ensured the adequacy of the collection and monitoring of log data.
Overview	Log data are one of the most important means of monitoring the use and disclosure of data. Under the Information Management Act, log data must be collected if the use of the information system requires identification or other login. In addition, the obligation under the GDPR to demonstrate the security of personal data processing often requires in practice the collection and monitoring of log data. The log data must be collected on the use of the information system and the disclosures of the data, but the collection of the data is linked to the necessity. If secret information or personal data is disclosed from the information system by means of APIs or viewing connections, disclosure log data must be collected in the disclosing system to ensure that there has been a legal basis for disclosing the information. In addition, access log data must be collected at least from information systems that process personal data or secret data.
Implementation example	An organisation that handles a lot of confidential information can implement the following measures, for instance: - As part of the procurement of services and information systems, the organisation specifies the related requirements for the collection of log data and ensures their fulfilment. - The organisation specifies the needs and procedures for monitoring data use and disclosure by information system. - Monitoring procedures are reviewed periodically. - The organisation specifies the responsibilities for the storage, destruction and protection of log data and ensures that they are fulfilled. - If the use of log data is wide-ranging, the organisation may consider migrating to centralised log information management (SIEM).
Legislation	TihL 17
References	Katakri: I-10
Other additional information	National Cyber Security Centre, Collecting and using log data; Collection of recommendations on the application of certain information security regulations 2021:65, chapter 14; ISO/IEC 27002:2022 5.31, 8.15

Identifier	HAL-08, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Incident management
Requirement	The organisation has specified processes and instructions for handling information security incidents and deviations.
Overview	The purpose of managing information security incidents is to ensure that the organisation is able to act effectively in undesired, unexpected situations, minimising damage and restoring the situation to normal, and to ensure that a similar incident is not possible elsewhere in the organisation. The organisation must have an incident-handling process that addresses at least the determining of the severity of the situation, preventing additional damage, collecting evidence, investigating the situation, communicating about the situation, implementing corrective measures and learning from the situation. The handling procedure must take into account the time-critical nature of the service, and when planning it, the needs for managing disruptions occurring outside office hours must be assessed. The organisation must also examine which national and international regulations or agreements concluded by the organisation require reporting information security incidents or suspected incidents to the authorities. The criteria, responsibilities, contact details and deadlines for communication have been specified and documented.
Implementation example	Management of information security disruptions has been - planned taking into account the entire service chain and disruptions occurring outside office hours, - instructed and trained, - documented at an adequate level, - practised, and - agreed with respect to communications practices and responsibilities
Legislation	TihL 4(2) and 13; TLA 7
References	Katakri: T-07
Other additional information	ISO/IEC 27002:2022 5.24; PiTuKri TJ-04

Identifier	HAL-09, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Documentation
Requirement	Information-security-related policies, processes, instructions and the results of process implementation have been documented.
Overview	
Implementation example	- The organisation has specified the documents required for information security management and the documents created in the different processes of information security management. - Maintenance and distribution processes have been specified for the documentation. - The rights and safeguards of the documentation have been specified.
Legislation	TihL 5, 6, 13(1)
References	Katakri: T-01
Other additional information	ISO/IEC 27002:2022 5.37

Identifier	HAL-09.1, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Documentation – timeliness
Requirement	The documentation related to information security is up to date.
Overview	
Implementation example	- The organisation has a process to monitor the coverage and timeliness of the documentation - Shortcomings in documentation are reacted to
Legislation	TihL 5, 6, 13(1)
References	
Other additional information	ISO/IEC 27002:2022 5.37

Identifier	HAL-10, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Personnel reliability assessment
Requirement	The organisation identifies tasks whose execution requires special reliability from the organisation's personnel or people working for the organisation.
Overview	Tasks requiring special reliability can be identified, for example, by determining situations in which a person processes classified or significantly and regularly secret information, or works in premises where the person may other than randomly become aware of classified or secret information.
Implementation example	- The organisation prepares a description of tasks related to the processing of data that require special reliability. - A security clearance is sought for the persons assigned to these tasks, if this is justified under the Act on Security Clearance. - In addition, the Information Management Unit maintains a list of these tasks.
Legislation	TihL 12;
References	Katakri: T-10
Other additional information	Act on Security Clearance 726/2014; ISO/IEC 27002:2022 6.1

Identifier	HAL-10.1, C:Secret, I:Critical, A:Critical, DP:Special category of personal data
Title	Personnel reliability assessment – security clearance
Requirement	The organisation assesses the need for a security clearance and, if one is required, grants the persons access to the assets to be protected only after the security clearance has been passed.
Overview	Provisions on the prerequisites for carrying out a personal security clearance are laid down in the Act on Security Clearance (726/2014). A personal security clearance can be carried out for a person who, in his or her work, has access to a space that is important for security, or processes confidential information. The scope of the security clearance depends on the person's duties and the necessary access rights to, for example, the processing of secret information. The scope of the clearance determines which sources of information are used in carrying out the clearance. The person can be interviewed if necessary. In most cases, the employer seeks security clearance, and the employee first fills in the forms related to the security clearance.

Implementation example	- In connection with recruitment, task changes and external service procurements, it is checked whether the task requires a security clearance, - if necessary, the organisation has specified a process for applying for security clearances
Legislation	TihL 12; TLA 9
References	Katakri: T-10
Other additional information	State Civil Servants' Act 750/1994 8c
Identifier	**HAL-11, C:Secret, I:, A:, DP:Personal data**
Title	Obligation to secrecy and obligation of non-disclosure
Requirement	Information security principles and measures concerning the protection of data and the processing of documents have been clarified to the persons processing data.
Overview	
Implementation example	- A person is informed of the principles of data protection before accessing the data, - as proof of receipt of the information, the person may sign a written non-disclosure agreement, and the signature is listed in the "NDA list" or - there is a digital procedure for providing the commitment, which is automatically handled at the time of the first login
Legislation	TihL 4(2); TLA 6, 8; JulkL 25, 26(3)
References	Katakri: T-11
Other additional information	ISO/IEC 27002:2022 6.6; PiTuKri HT-03
Identifier	**HAL-12, C:Public, I:Minor, A:Minor, DP:Personal data**
Title	Guidelines
Requirement	The organisation has up-to-date and comprehensive instructions for ensuring information security.
Overview	By providing instructions on matters that are essential for information security, the aim is to ensure that operations are not dependent on individuals. The organisation should have up-to-date instructions on data processing, use of information systems, data processing rights, implementation of information management responsibilities, implementation of information access rights and information security measures. The instructions cover processes and processing environments related to data throughout the data lifecycle.
Implementation example	- The procedures and instructions required to protect data and ensure information security have been documented. - Security instructions are implemented taking into account the needs of the personnel's tasks. - The coverage and timeliness of the security instructions are regularly monitored and the instructions are available to the necessary parties.
Legislation	TihL 4(2), 13(1); TLA 6, 8
References	Julkri: TEK-17.2; Katakri: T-04
Other additional information	ISO/IEC 27002:2022 5.37; SFS-EN ISO/IEC 27001:2017 7.5; PiTuKri HT-04; Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa (Recommendations on the implementation of management responsibilities in information management) 2020:18, chapter 4

Identifier	HAL-13, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Training
Requirement	Through orientation, training and communication, the organisation ensures that the personnel and those working on behalf of the organisation are familiar with valid information security policies and instructions.
Overview	The management must see to it that training is provided within the organisation to ensure that the personnel and those acting on behalf of the organisation are familiar with the valid regulations, orders and instructions concerning information security, information management, data processing, publicity and secrecy, and the risks and threats to the information that the organisation is responsible for. In particular, training sessions must take into account threats and instructions related to remote use, the administration of information systems and other higher-risk processing situations.
Implementation example	- Persons processing data have been informed of the security rules and procedures for protecting the data. - the training is implemented taking into account the needs of the personnel's tasks. - The content of the training is documented. - A record of the participants is kept.
Legislation	TihL 4(2); TLA 6, 8
References	Katakri: T-12
Other additional information	ISO/IEC 27002:2022 6.3; PiTuKri HT-04; Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa (Recommendations on the implementation of management responsibilities in information management) 2020:18, chapter 5
Identifier	**HAL-14, C:Public, I:Minor, A:, DP:Personal data**
Title	Access and processing rights
Requirement	The organisation ensures that access rights to information systems and data processing rights are determined according to the needs of the tasks and kept up to date.
Overview	The management of access and processing rights enables the authorised use of data and prevents unauthorised access. The user is granted access rights and authorisations only to information systems that are necessary for the tasks. The right to process data may be granted only to those who, due to their duties, need to receive or otherwise process data, who have been informed of instructions on data protection and who are familiar with the obligations concerning the processing of data.
Implementation example	- The organisation has specified the principles according to which access and processing rights are granted - Responsibilities and procedures have been specified for the approval of rights - Responsibilities and procedures have been specified for the enforcement of rights - The granting of access rights is documented so that it can be reviewed afterwards
Legislation	TihL 4(2) and 16; TLA 8, 11(1) item 3
References	Katakri: T-13, I-6
Other additional information	ISO/IEC 27002:2022 5.15, 5.18; PiTuKri HT-05; Collection of recommendations on the application of certain information security regulations 2021:65, chapter 13; Recommendation on the handling of classified documents 2021:5, chapter 7.6

Identifier	HAL-14.1, C:TL III, I:, A:, DP:
Title	Access and processing rights – up-to-date list
Requirement	The organisation ensures that it has up-to-date lists of individuals' access and processing rights.
Overview	A central government authority shall keep a list of persons who have the right to handle documents at security classification levels I, II or III. The list shall state the person's task on which the need to handle classified information is based.
Implementation example	
Legislation	TLA 8
References	Katakri: T-13
Other additional information	ISO/IEC 27002:2022 5.18; Recommendation on handling security classified documents 2021:5 section 4.1
Identifier	**HAL-14.2, C:Secret, I:Critical, A:, DP:Special category of personal data**
Title	Access and processing rights – termination
Requirement	The organisation ensures that anyone who no longer performs the tasks on which the right to process the data is based returns or destroys the data in an appropriate manner.
Overview	
Implementation example	
Legislation	TihL 13(1), 21(2); TLA 8
References	Katakri: T-13
Other additional information	ISO/IEC 27002:2022 5.18; Recommendation on handling security classified documents 2021:5 section 4.1
Identifier	**HAL-15, C:Public, I:Minor, A:Minor, DP:Personal data**
Title	Information security of work throughout the employment relationship or engagement
Requirement	The organisation sees to the information security of the work throughout the employment relationship or engagement.
Overview	Special attention must be paid to measures during recruiting and changes in work tasks and when the employment relationship ends. Measures at the beginning and during the employment relationship include personal security clearances, processing, use rights and access rights, understanding of the obligation of secrecy and non-disclosure, security training and the possible updating of these and training of changes. Procedures related to the termination of employment include the handing over of access keys, credentials and materials, as well as the removal of processing, use and access rights. At the end of the employment relationship, it is also essential to point out the obligation of secrecy and non-disclosure.

Implementation example	The measures typically require procedure guides that are trained and available to the required personnel. For example, the procedure guides can be divided into entities in accordance with the lifecycle of the employment relationship. Instruction sets may include recruitment instructions, orientation instructions, instructions for changes during the employment relationship, instructions for termination of the employment relationship and instructions for more detailed measures, such as instructions for changes in processing, use and access rights.
Legislation	TihL 4(2), 12, 16 TLA 6, 8
References	Katakri: T-09
Other additional information	ISO/IEC 27002:2022 6.1, 6.2, 6.3, 6.5; PiTuKri HT-01; Collection of recommendations on the application of certain information security regulations 2021:65, chapter 5; Recommendation on the handling of classified documents 2021:5
Identifier	**HAL-16, C:Public, I:Minor, A:Minor, DP:Personal data**
Title	Procurement security
Requirement	The organisation ensures in advance that information systems and services to be procured are secure and ensures their security in situations of change throughout the system's lifecycle.
Overview	In procurements, it must be ensured that the information systems and services to be procured meet the information security requirements of the data sets to be processed and that the information systems are suitable for the effective and efficient performance of the authorities' tasks. Before a procurement decision is made, it is advisable to identify alternatives and eliminate at an early stage those that cannot meet the minimum legal requirements. One method for making such a preliminary qualification is to become familiarised with the descriptions produced by the service provider candidates and to pre-assess the system or service to be procured on the basis of them in relation to the minimum requirements. One commonly used method for ensuring the security of services is the auditing of information systems and their service providers, which is described in more detail in chapter 4 of the recommendation "Handling of classified documents in cloud computing services". Some service providers offer their customers the opportunity to introduce new functionalities that are in the preview or testing phase. If such functionalities are to be introduced in the processing of secret information, it is recommended that, for example, the responsibilities related to the introduction be taken into account in the risk assessment. There may still be security shortcomings in the implementation of new functionalities, and compensation for any damage caused by these shortcomings has often been allocated to the customer in the contracts.

Implementation example	The organisation specifies information security requirements in procurement and development processes and ensures that they are met. In order to ensure the adequacy of the requirements, the organisation requires that the information security requirements are specified, reviewed and approved before the procurement process proceeds, and that information security testing has been carried out acceptably before the deployment of the information systems. The provider/supplier of the service or system to be procured must be able to establish at least the following: 1) A system description of the service exists. Based on the description of the service provider, it must be possible to assess the overall suitability of the service in question for the customer's use case. The system description must indicate at least: a) the service and implementation models of the service and the related service-level agreements b) the principles, procedures and security measures, including monitoring measures, for the lifecycle of the provision of the service (development, use, decommissioning) c) a description of the infrastructure, network and system components used to develop, maintain/manage and operate the service d) the principles and practices of change management, in particular processes for handling changes that affect security e) the handling processes for significant events deviating from normal use, such as procedures for significant system failures f) the roles related to the provision and use of the service and the division of responsibilities between the customer and the service provider The description must clearly indicate the actions that the customer is responsible for in ensuring the security of the service. The service provider's responsibilities must include a duty to cooperate, especially in the investigation of deviations. g) Activities transferred or outsourced to subcontractors The description of the infrastructure, network and system components must be sufficiently detailed to allow for assessing the overall suitability and risks of the service in relation to the customer's use case. Cf. PiTuKri KT-01 (System description to support continuity and operational security). In the description of the infrastructure, the software code on the basis of which the infrastructure is built can also be used, with certain limitations.
Legislation	TihL 13(4); TLA 6; JulkL 26
References	Katakri: I-13
Other additional information	ISO/IEC 27002:2022 5.19, 5.20, 5.21, 8.29, 8.30; Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa (Recommendations on the implementation of management responsibilities in information management) 2020:18, chapter 6; Collection of recommendations on the application of certain information security regulations 2021:65 chapter 8; Recommendation Handling of classified documents in cloud computing services 2022:4 chapter 4; PiTuKri EE-01 and KT-01

Identifier	HAL-16.1, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Procurement security – agreements
Requirement	The organisation ensures that information security requirements and their retention throughout the lifecycle are taken into account in the agreements. Furthermore, the contractual terms may not restrict the suitability of the service for the use case in question.
Overview	Cloud services in particular are under constant change. Cloud services are characterised by rapid and strong development, which requires continuous monitoring and supervision of contracts and change management. The changes increase the risk that a service, its provider or any new feature becomes non-compliant or that change-of-control risks are realised. A change of ownership of a service provider also involves risks that must be taken into account in the contracts to a sufficient extent. In addition, it should be noted that it may be impossible to ensure information security that lasts throughout the lifecycle of the information with service providers that reserve a one-sided right to change their contractual terms in their contracts. The reliability of the contract must also be assessed on a risk basis, and it must be ensured that the matters agreed upon by the bidder in the contract have also been implemented as agreed. Especially in agreements related to cloud services, the tasks that the service provider is responsible for and those that are the responsibility of the customer must be clearly specified. From the perspective of data protection regulation, the processing of personal data may also be prevented if the service provider is unable to offer an agreement in accordance with data protection regulation that cannot be changed unilaterally, i.e., without the consent of the customer of the service. The assessment must take into account the requirements of section 4 of article 28 of the EU General Data Protection Regulation when using sub-processors. A service provider (controller) must conclude a written agreement with the processor. Service agreements and their terms of use may also involve different vendor-specific ways of determining the countries where the service or part of it is physically located. The transfer of personal data outside the EU/EEA must always be carried out in accordance with the conditions laid down in the EU's General Data Protection Regulation (chapter V). With regard to, for example, risks derived from legislation, and continuity and preparedness, it should also be noted that the information of the customer of the service must be located only in the physical locations described in the contract throughout the information's lifecycle. An exception to this is a situation where the customer of the service has approved in advance in writing the transfer or processing of data in other physical locations. Meeting such needs is generally not credible in situations where the service provider reserves the possibility to modify its contractual terms unilaterally, i.e., without the consent of the customer. It should also be noted that an authority must ensure in advance that the secrecy and protection of the information is ensured appropriately (621/1999, section 26). The authority must also ensure in advance that the protection of a classified document is adequately ensured if the authority provides a classified document to a non-governmental authority (TLA section 6).
Implementation example	
Legislation	TihL 13; TLA 6; JulkL 26; GDPR article 28.4
References	Katakri: I-13
Other additional information	ISO/IEC 27002:2022 5.20; Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa (Recommendations on the implementation of management responsibilities in information management) 2020:18, chapter 6; PiTuKri TJ-07

Identifier	HAL-17, C:, I:Important, A:Important, DP:
Title	Functional usability and fault tolerance of information systems
Requirement	Through regular testing, the organisation ensures the fault tolerance and functional usability of information systems that are essential for the performance of its tasks.
Overview	Essential information systems refer to information systems that are critical to the implementation of the authority's statutory tasks, especially when providing administrative services to customers. From the user's perspective, functional usability refers to ensuring that an information system is easy to learn and that its operating logic is easy to remember, its operations support the tasks that the user must perform with the information system and the information system promotes the accuracy of its use.
Implementation example	- The organisation identifies and lists information systems that are essential for the performance of tasks, for example as part of the listing of assets to be protected and the classification of information. - The organisation specifies the availability criteria for essential information systems against which fault tolerance can be tested. The availability classification of information systems can be used in the specification of system-specific availability criteria. - The organisation specifies the criteria for operational usability. - The requirements related to operational availability and fault tolerance have been taken into account in the organisation's procurement processes and procurement instructions. - The organisation documents fault tolerance tests.
Legislation	TihL 13(2)
References	
Other additional information	ISO/IEC 27002:2022 8.29; Collection of recommendations on the application of certain information security regulations 2021:65 chapter 7
Identifier	**HAL-17.1, C:Public, I:Minor, A:Minor, DP:Personal data**
Title	Functional usability and fault tolerance of information systems – accessibility
Requirement	The organisation must ensure the accessibility of digital services to the extent required by legislation.
Overview	Accessibility means that as many different people as possible can access websites and mobile applications as easily as possible. Accessibility means taking people's diversity into account in the design and implementation of websites and mobile applications. Three areas must be taken into account in the design and implementation of accessible digital services: technical implementation, ease of use, and clarity and comprehensibility of content. Because accessibility does not fall within the competence of the Information Management Board, accessibility is only included in Julkri criteria as a top-level verification criterion. The Julkri criteria are thus not used in the assessment of accessibility, but the criterion is there to remind organisations that accessibility issues should also be ensured as part of the design and implementation of digital services. More detailed instructions and requirements can be found on the www.saavutettavuusvaatimukset.fi website maintained by the Regional State Administrative Agency for Southern Finland.
Implementation example	
Legislation	Act on the Provision of Digital Services 306/2019
References	
Other additional information	www.saavutettavuusvaatimukset.fi

Identifier	HAL-18, C:Public, I:, A:, DP:
Title	Implementation of document publicity
Requirement	The organisation ensures that information systems, information structures of information repositories and the related information processing are designed so that the publicity of documents can be easily implemented.
Overview	The requirement applies to authorities that in practice are responsible for the availability of information in the data sets. The requirement emphasises the fact that it must be possible to use the search functions in the information system of an authority to generate the authority's documents in order to ensure the publicity of the authority's activities.
Implementation example	- Organisations specify the information needs related to the information materials they are responsible for, taking into account, in particular, the requirements concerning the publicity of the authorities' data. - In implementation and procurement processes, organisations take into account the requirements for easy implementation of document publicity. - The organisation monitors needs related to the implementation of document publicity and maintains old information systems as necessary.
Legislation	TihL 13(3)
References	
Other additional information	

Identifier	HAL-19, C:Public, I:, A:, DP:Personal data
Title	Information processing
Requirement	The organisation ensures that information is processed and stored in such a way that access to it is protected against third parties.
Overview	The information security of information processing and storage is influenced, among other things, by the security of physical facilities, the security of information systems and terminal devices used in information processing, and the instructions and training of the persons processing the information. The organisation's security management processes must be used to ensure that the necessary measures have been taken in all the areas listed above. More detailed criteria for the processing and storage of information classified at different security levels are set out in the physical and technical security sub-areas.

Implementation example	The organisation has ensured the security of information processing, for example with the following measures: - The organisation has ensured that the facilities intended for the processing and storage of information meet the requirements set by the information and information systems processed or stored within them, as well as the required administrative areas and secured areas - The organisation has provided instruction on which premises information classified at different security levels may be processed and stored in - The organisation has provided instruction on how access to information should be protected from outsiders in different processing environments - The organisation has specified how information systems intended for processing different types of information should be stored - The organisation has specified the requirements for equipment used in data processing
Legislation	TihL 13, 15(2); TLA 10(1)
References	Julkri: FYY-03, FYY-04, TEK-09; Katakri: I-17
Other additional information	ISO/IEC 27002:2022 5.15; Collection of recommendations on the application of certain information security regulations 2021:65 chapter 4

3 Physical security

Physical security (FYY) includes criteria for facilities and storage solutions that prevent and restrict unauthorised access to data. In addition, the sub-area describes criteria related to the processing, storage, transfer, transport, and destruction of data. The physical security sub-area can be used in assessing the physical security measures taken to protect data.

The content of the sub-area is based on the Katakri criteria. In particular, efforts have been made to maintain the content of the criteria for handling classified information consistent with Katakri. The clearest differences in relation to Katakri are the exclusion of criteria based on international information security obligations from the sub-area and the classification of certain criteria as applicable to non-classified information.

The structure of the sub-area has been designed so that the common criteria for different security areas, the criteria for administrative areas only, and the criteria for secured areas only have each been compiled in their own sub-sections. This structure differs from the Katakri structure, where some of the criteria have been repeated with the same content in different security areas.

Data material of authorities must be processed and stored in premises that are sufficiently secure for implementing the requirements related to the confidentiality, integrity, and availability of data (section 15(2) of the Information Management Act). For the physical protection of security classified information, the Security Classification Decree provides for two types of physically secured security areas: administrative areas and secured areas. The concepts of administrative area and secured area are used in Julkri.

It is recommended that information resources containing secret information and the information systems used for processing them be placed in a protected area designated for this purpose by an authority, such as the administrative area described in the Security Classification Decree and this recommendation and the attached criteria.

In practice, an administrative area refers to an area specified by the organisation to which unauthorised parties cannot gain uncontrolled access and in which sufficient measures have been implemented to ensure the security of the information processed and stored in the area. No detailed requirements have been set for the structures and other measures in

the area. Instead, organisations can plan them using the criteria of the physical (FYY) sub-area in a risk-based manner.

Physical security means the implementation of physical and technical security measures to prevent unauthorised access to data by:

a) ensuring that the information is properly processed and stored;
b) enabling access to information on a need-to-know basis and, where appropriate, security clearance;
c) preventing, blocking and detecting unauthorised activities; and
d) preventing or delaying unauthorised intrusion.

In premises where more than one organisation operates, each organisation processing the information must ensure that the security provided by the shared premises is adequate in relation to the physical security requirements that the organisation is subject to.

Identifier	FYY-01, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Physical security risk assessment
Requirement	Physical security measures must be scaled in accordance with the risk assessment.
Overview	The risk assessment must take into account, for example, the principles of the need for information, separation of duties, and least privilege to be included in the management of access rights and other processes related to security arrangements. The risk assessment of physical security measures must be regular and part of the organisation's risk management system. The assessed risks have designated owners. The risks associated with changes to approved physical security measures must be assessed in connection with the changes. Especially with regard to substitute physical security measures, it must be possible to provide justifications for the selected security measures.
Implementation example	All relevant factors must be taken into account in the risk assessment, particularly the following: a) the security class and grounds of secrecy of the data b) the way the information is processed and stored and its volume, taking into account that a high volume or aggregation of information may require the application of more stringent risk management measures c) time of processing and storing of information d) environment of the location of information processing and storage: the environment of the building, location in the building, space or part thereof e) response time related to alarm situations f) outsourced activities, such as maintenance, cleaning, facility and security services g) estimated threat to information from intelligence services, criminal activities and own personnel
Legislation	TihL 13(1), 15(2)
References	Julkri: HAL-06; Katakri: F-02
Other additional information	Recommendation on the handling of classified documents 2021:5, page 36

Identifier	FYY-01.1, C:TL III, I:, A:, DP:
Title	Physical security risk assessment – TEMPEST
Requirement	When assessing the processing of information in a terminal device and the location of security areas, the TEMPEST risk must also be taken into account to a sufficient extent.
Overview	When assessing the processing of information in a terminal device and the location of security areas, the TEMPEST risk, i.e., the risk from electromagnetic radiation, must also be taken into account to a sufficient extent. The TEMPEST risk can usually be reduced by changing the location of the information-processing site within the property.
Implementation example	
Legislation	TLA 11(2)
References	Julkri: TEK-15; Katakri: F-05.8, F-06.10
Other additional information	

Identifier	FYY-02, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Choosing physical security measures (defence in depth)
Requirement	Measures to prevent, block and limit acts compromising the protection of the security area, measures to detect and trace acts compromising the protection, and measures to restore without delay the level of security prevailing prior to an act compromising the security area must be taken, applying the multi-layer protection principle. Equipment must be inspected and maintained at regular intervals.
Overview	Information resources containing secret information and documents and the information systems used for processing them must be placed in a protected area designated for this purpose by an authority, such as the administrative area described in the Security Classification Decree, or the information must be protected by means of other security controls in a risk-based manner. It is recommended that the equipment and systems included in the multi-layer protection solution comply with European standards and their minimum requirements. The selection of the correct standard category is always based on a risk assessment. The Target level column, which is added to the individual requirements, shows the appropriate standard class or guide for most multi-layer protection solutions. However, the approval of individual security measures does not require meeting the target level, because the assessment of physical security measures is based on a risk assessment and the whole of multi-layer protection. In some situations, security measures at a level higher than the individual target level may also be required based on risk assessment. When assessing equipment and systems, it must be ensured that they are operational and suitable for their intended use. Documentation of acceptance inspections of equipment and systems, inspections during use and maintenance should be available. When assessing system rights, particular attention should be paid to the implementation of the principle of least privilege and separation of duties. The location space of the equipment and systems should be located in the security area they protect. Installation, inspection, maintenance and cleaning of equipment and systems and the locations they are placed in are carried out only by or under the supervision of a person who has been granted an independent right of access to the area. Based on the risk assessment, remote connections and installation of devices and systems must be implemented in a sufficiently secure manner, so that access to devices and systems is possible only from authorised devices and networks, and so that the interfaces of data connections and devices and systems are protected so that outsiders do not have access to the transmitted data. The processing of secret information is possible also in shared work environments where several different organisations can work. In this case, the level of physical security is agreed upon in advance, if necessary, so that the space enables the appropriate processing and storage of secret information, taking into account the needs of each organisation. In these cases, it is the responsibility of the information processor to process the information so that an unauthorised person does not gain access to it.

Implementation example	Defence in depth consists of administrative, operational and physical means, such as: a) structural barriers: a physical barrier to delimit security areas and their surrounding spaces and to impede and slow down unauthorised access b) physical access control: physical access control restricts access to security areas and surrounding facilities. The aim is to detect unauthorised attempts to enter the area, prevent unauthorised persons from gaining access, and supervise those moving in the area. Physical access control may target an area, one or more buildings in an area, or areas or rooms in a building. Mechanical, electrical or electromechanical technical systems or other physical means may be used in the monitoring. Security personnel, reception officers or own personnel may also participate in the supervision c) intrusion detection system: an intrusion detection system (break-in alarm system) may be used to improve the level of security provided by a structural barrier. The system can also be used instead of or to support supervision by security personnel d) security personnel: trained, supervised, equipped and, if necessary, appropriately security-cleared security personnel may be used, for example, to support physical access control and to detect and prevent the intent of persons planning access to the security area or its surrounding facilities e) camera surveillance: camera surveillance may be used in or around the security area, in particular to prevent illegal reconnaissance, prevent occurrences of deviations, verify alarms and investigate occurrences of deviations. Security personnel can use camera surveillance as real-time, active image monitoring or afterwards as passive image material analysis f) procedures that maintain security: specifying responsibilities and tasks, various processes and operating models, such as physical access rights and key management, personnel guidance and orientation, and service and maintenance of systems g) lighting: a potential intruder can be detected by lighting, and security personnel can effectively monitor the area, either directly or by using a camera surveillance system h) other appropriate physical measures designed to prevent and detect unauthorised access or to prevent loss or damage to classified information
Legislation	TihL 13(1), 15(2); TLA 7
References	Katakri: F-03
Other additional information	Recommendation on the handling of classified documents 2021:5, page 33; ISO/IEC 27002:2022 7.1, 7.2, 7.3

Identifier	FYY-03, C:Secret, I:, A:, DP:Special category of personal data
Title	Data processing
Requirement	Information must be processed in such a way as to protect access to it from third parties.
Overview	Prevention refers to the protection of information both from persons without the need to know the information and from illegal reconnaissance. In practice, protection means, for example, preventing direct visual or audio contact with classified information. The handling of security classified information in security areas (administrative area or secured area) is the main rule, but there are situations, such as remote work or work tasks outside security areas, where the information must also be processed outside specified security areas. Information can be processed in both paper form and with a qualifying device within or outside secured areas and administrative areas, provided that access to the information is protected from third parties. Processing is permitted up to security classification TL II, but the data repositories containing security classification level II or III documents and the information systems used to process these documents must be placed in a secured area.
Implementation example	
Legislation	TihL 13(1), 15(2); TLA 10
References	Julkri: HAL-19; Katakri: F-04
Other additional information	Recommendation on the handling of classified documents 2021:5, page 29

Identifier	FYY-03.1, C:TL I, I:, A:, DP:
Title	Information processing – TL I
Requirement	A security classification I document may be processed only in a secured area.
Overview	
Implementation example	
Legislation	TLA 10(2)
References	Julkri: HAL-19; Katakri: F-04
Other additional information	Recommendation on the handling of classified documents 2021:5, page 29

Identifier	FYY-04, C:Secret, I:, A:, DP:Special category of personal data
Title	Information storage
Requirement	Information must be stored in such a way as to prevent access to it by third parties.
Overview	In practice, protection means, for example, the storage of information or a terminal device containing information in a sufficiently secure manner. In addition, in the processing of information, the activities during breaks must be taken into account, as documents and devices must be placed in a suitable security area and/or storage unit for the duration of the break. Information storage refers to any situation where information is not under the immediate control of its processor.
Implementation example	
Legislation	TihL 13(1), 15(2); TLA 10
References	Julkri: HAL-19; Katakri: F-04
Other additional information	Recommendation on the handling of classified documents 2021:5, pages 28–29
Identifier	**FYY-04.1, C:TL IV, I:, A:, DP:**
Title	Data storage – TL IV
Requirement	The organisation stores paper documents and other non-electronic information - in a secured area or administrative area in office furniture deemed suitable or - temporarily outside security areas, if the information processor is committed to complying with the substitute measures specified in the security instructions issued The organisation retains information in electronic format - in a secured area or administrative area in a device or electronic medium that meets the requirements, or - outside security areas, in a controlled space or in appropriate locked office furniture in a security bag or similar manner, in a terminal device or electronic medium that meets the requirements
Overview	
Implementation example	If the area does not have a storage solution that is deemed sufficient for information storage, the walls, floor, ceiling, windows and doors of the area should meet a minimum level of protection equivalent to that of classification RC3 of SFS-EN-1627. If locked office furniture is used as a storage unit for classified information, it must be ensured that a trace of burglary is left in case of intrusion.
Legislation	TLA 10
References	Katakri: F-04
Other additional information	
Identifier	**FYY-04.2, C:TL IV, I:, A:, DP:**
Title	Data storage – Repositories and information systems – TL IV
Requirement	Information repositories containing security classification level IV documents and the information systems used to process these documents must be located in a security area (administrative area or secured area).

Overview	
Implementation example	
Legislation	TLA 10(3) item 3
References	Julkri: HAL-19; Katakri: F-04
Other additional information	Recommendation on the handling of classified documents 2021:5, pages 28–29
Identifier	**FYY-04.3, C:TL III, I:, A:, DP:**
Title	Data storage – Repositories and information systems – TL III
Requirement	Information repositories containing security classification levels II or III documents and the information systems used to process these documents must be located in a secured area.
Overview	
Implementation example	
Legislation	TLA 10(3) item 2
References	Julkri: HAL-19; Katakri: F-04
Other additional information	Recommendation on the handling of classified documents 2021:5, pages 28–29
Identifier	**FYY-04.4, C:TL III, I:, A:, DP:**
Title	Data storage – TL III
Requirement	The organisation stores paper documents and other non-electronic information in a secured area in a storage solution deemed suitable. The organisation retains information in electronic format - in a secured area in a device or electronic medium that meets the requirements, or - outside secured areas, in a controlled space or in appropriate locked office furniture in a security bag or similar manner, in a terminal device that meets the requirements
Overview	
Implementation example	
Legislation	TLA 10
References	Katakri: F-04
Other additional information	

Identifier	FYY-04.5, C:TL II, I:, A:, DP:
Title	Data storage – TL II
Requirement	The organisation stores paper documents and other non-electronic information in a secured area in a storage solution deemed suitable. The organisation stores information in electronic format in a secured area on a device or electronic medium that meets the requirements.
Overview	
Implementation example	
Legislation	TLA 10
References	Katakri: F-04
Other additional information	

Identifier	FYY-04.6, C:TL I, I:, A:, DP:
Title	Data storage – TL I
Requirement	A security classification level I document may be stored only in a secured area.
Overview	
Implementation example	
Legislation	TLA 10(2)
References	Julkri: HAL-19; Katakri: F-04
Other additional information	Recommendation on the handling of classified documents 2021:5, page 29

Identifier	FYY-05, C:Secret, I:, A:, DP:Special category of personal data
Title	Security area
Requirement	Security areas, i.e., administrative areas and secured areas, must comply with the recommendations given in this criterion.
Overview	Many physical security recommendations are common to both administrative and secured areas. This criterion contains joint recommendations that must be taken into account in the evaluations of both administrative areas and secured areas.
Implementation example	
Legislation	TihL 13(1), 15(2); TLA 9
References	Katakri: F-05.4, F-06.6
Other additional information	Recommendation on the handling of classified documents 2021:5, page 39

Identifier	FYY-05.1, C:TL IV, I:, A:, DP:
Title	Security area – Soundproofing
Requirement	The soundproofing of the area must prevent unauthorised persons from hearing, in clearly audible language, discussions related to the information to be protected. Soundproofing must also be taken into account within the area if information to be protected is discussed there such that not everyone needs to know.
Overview	Prevention refers to the protection of information both from persons without the need to know the information discussed and from illegal reconnaissance. The soundproofing requirement applies only to premises in the area where the information to be protected is discussed. Soundproofing can be assessed, for example, by listening to the discussion outside the space at the doors, walls and air conditioning pipes and other inlets. The soundproofing of the space can also be compared, if necessary, with the sound reduction requirement for structures.
Implementation example	The requirement may be determined in accordance with standard SFS-EN-ISO 717-1. Airborne sound reduction can be verified by a measurement made in accordance with SFS-EN-ISO 16283-1. In addition to airborne sound reduction, the assessment must also take into account mechanical sound insulation. If necessary, the soundproofing requirement can be achieved by, for example, redoing the layout of the space, by improving the insulation of structures and inlets, or by using background noise of spaces outside the area to be assessed.
Legislation	TihL 13(1), 15(2); TLA 10(1)
References	Katakri: F-05.4, F-06.6
Other additional information	Recommendation on the handling of classified documents 2021:5, page 39
Identifier	**FYY-05.2, C:Secret, I:, A:, DP:Special category of personal data**
Title	Security area – Prevention of viewing in secret
Requirement	If the information is subject to a risk of viewing secretly or unintentionally, appropriate measures must be taken to prevent the risk.
Overview	
Implementation example	The risk of viewing in secret can be reduced, for example, through the placement of workstations and the use of portable partitions, curtains or privacy filters.
Legislation	TihL 13(1), 15(2); TLA 10(1)
References	Julkri: HAL-19; Katakri: F-05.6, F-06.8
Other additional information	Recommendation on the handling of classified documents 2021:5, pages 40 and 45

Identifier	FYY-05.3, C:TL II, I:, A:, DP:
Title	Security area – Premises and equipment inspections
Requirement	The organisation must inspect all electronic devices before they are used in an area where information classified at level II is processed, if the threat to the information is assessed to be high. The premises must also be physically or technically inspected at regular intervals and in the event of unauthorised entry or suspicion thereof.
Overview	If it is not possible to reliably inspect the electronic devices in question (e.g., mobile phones, smartwatches, etc.), the devices must be left outside the space, for example, in a storage solution reserved for this purpose.
Implementation example	
Legislation	TLA 7, 10(1), 11(2)
References	Katakri: F-05.7, F-06.9
Other additional information	Recommendation on the handling of classified documents 2021:5, pages 40 and 46

Identifier	FYY-05.4, C:Secret, I:, A:, DP:Special category of personal data
Title	Security area – Physical access rights and key management procedures
Requirement	The organisation must specify the procedures and roles for physical access rights and key management for the area.
Overview	The restriction of access to the area may be implemented either mechanically, electronically or based on personal identification. A person responsible for the area must be designated to take care of physical access rights and key management procedures. The area's spare keys are stored securely and closed in a sealed storage case with closing date and acknowledgement, or alternatively in a key cabinet connected to physical access control. The keys are handed over in connection with the work task and against an acknowledgement. The procedure is described in the security management instructions. The area must not be accessible with a master key suitable for lower-class spaces. It is recommended that the equipment and systems included in the multi-layer protection solution comply with European standards and their minimum requirements. Standards that can be used as a reference when assessing an appropriate solution: Locks with ferrules: SFS 7020+5970, categories 1 to 4, target level 3; electronic access control systems: SFS-EN 60839-11-1 and 2; note, for example, the requirements of SFS-EN 50131 if the access control system is part of an intrusion detection system.

Implementation example	A person responsible for the area has been designated to take care of the following physical access rights and key management procedures. - physical access rights and key management procedures and roles have been created, documented and instructed - there is a list of the holders of physical access rights and keys - physical access rights are regularly checked and kept up to date - responsibilities have been assigned for actions concerning additional orders and changes to keys and physical access codes - key cards, unallocated keys and physical access codes are stored appropriately - key handover basis is documented - keys are handed over only to persons who have been granted independent access to the area - if necessary, changes in personnel are reflected in the right to possess a key
Legislation	TihL 15(2); TLA 9
References	Katakri: F-05.2, F-06.3
Other additional information	Recommendation on the handling of classified documents 2021:5, pages 39 and 44; ISO/IEC 27002:2022 7.2
Identifier	**FYY-05.5, C:TL IV, I:, A:, DP:**
Title	Security area – Visitors
Requirement	Persons not duly authorised by the organisation (visitors) always have an escort.
Overview	The host of the guests must have independent access to the security area to which they take the guests and the right to host the guests. Visiting procedures must ensure that the confidentiality of the information processed or stored in the area is not compromised during the visit. Maintenance in the area is carried out only by or under the supervision of a person who has been granted an independent right of access to the area. The processing of information in the area is prohibited during maintenance, installation and cleaning operations if there is a risk that the personnel performing the aforementioned operations will become aware of the information to be protected. It is possible to accept an unescorted visitor procedure for visitors in the area who meet the requirements for granting access rights.
Implementation example	A code of conduct has been approved by the organisation for visitors. The visitor code can deal with, for example, the following matters: - the guest is identified and equipped with a guest card - the visit is recorded - visitors are not allowed or are left unsupervised in the areas, and the host is responsible for external persons throughout the visit - personnel have been instructed regarding the hosting of visitors - ensuring that a guest cannot unlawfully see, hear or otherwise gain access to information to be protected - personnel have been instructed to respond to persons roaming about without an identifier
Legislation	TLA 9
References	Katakri: F-05.3, F-06.4
Other additional information	Recommendation on the handling of classified documents 2021:5, pages 39 and 44

Identifier	FYY-06, C:Secret, I:, A:, DP:
Title	Administrative area
Requirement	An administrative area must meet the recommendations presented in this section and the risk-based specifications, so that the objectives of the security measures are achieved.
Overview	Information resources containing secret information and documents and the information systems used for processing them must be placed in a protected area designated for this purpose by an authority, such as the administrative area described in the Security Classification Decree, or the information must be protected by means of other security controls in a risk-based manner. An administrative area refers to areas and spaces intended for normal work, such as an office space or an entity consisting of several office spaces. The administrative area must meet the minimum requirements set out in this section. In addition to the minimum requirements, other risk management measures based on risk assessment and the multi-layer protection principle must be planned, assigned, implemented and maintained so that residual risks on classified information can be accepted and the objectives of security measures achieved. In addition, the administrative area must meet all the common requirements for security areas described in the criterion "Security area".
Implementation example	
Legislation	TihL 13(1), 15(2); TLA 9
References	Julkri: FYY-05; Katakri: F-05
Other additional information	Recommendation on the handling of classified documents 2021:5, page 38

Identifier	FYY-06.1, C:TL IV, I:, A:, DP:
Title	Administrative area – boundary and structures of the area
Requirement	The area must have a clearly specified, visible boundary, but no specific requirements are set for the structure delimiting the area (walls, doors and windows, floor and ceiling structures).
Overview	The objective of physical security measures must be met before security areas can be approved. The structure of the area can be a normal office structure. Structures bordering the area should be reinforced if classified information is stored in the area and the risk of breaking in is assessed as likely. These reinforcements must be assessed in relation to the other security provided by the facilities surrounding the area and the response time of the security personnel. It must be possible to lock or close openings of the area that are not in use for passage to, from or within the area, for proper management of access to the area. If a mechanical lock has been used at the boundaries of the administrative area, copying of the lock keys should be prohibited by patent protection. If possible, emergency escape routes must not pass through a secured area. It is recommended that the solutions included in the defence in depth principle comply with European standards and their minimum requirements:

Implementation example	Standards that can be used as a reference for the assessment of structures bounding the area: Walls and doors and floor and ceiling structures: SFS-EN 1627, RC1-RC6; Windows (armoured glass): SFS-EN 356, P4A-P5A and P6B-P8B
Legislation	TihL 13(1), 15(2); TLA 9(1) item 1
References	Katakri: F-05.1
Other additional information	Recommendation on the handling of classified documents 2021:5, page 39
Identifier	**FYY-06.2, C:TL IV, I:, A:, DP:**
Title	Administrative area – physical access control
Requirement	Access to the area must be controlled, if this is expedient based on a risk assessment.
Overview	Physical access control may be expedient, for example, if security classification level III or higher information is processed in the area.
Implementation example	Recommendation on implementing access control: - The organisation uses photo ID cards or similar visible identifiers. - A person only has the physical access rights necessary for the performance of their duties. - The grounds for granting physical access rights are recorded in the document, and only designated persons have a physical access right to the area. - If necessary, changes in personnel are reflected in the physical access rights. - The management of the physical access control system may be outsourced if it is well managed.
Legislation	TLA 7, 9
References	Katakri: F-05.2
Other additional information	
Identifier	**FYY-06.3, C:Secret, I:, A:, DP:**
Title	Administrative area – granting of physical access rights
Requirement	Only duly authorised persons have independent access to the area. Independent access to the area can be granted by the organisation responsible for the information or, through agreed procedures, by the service provider responsible for managing the physical space, such as a cloud service provider.
Overview	The restriction of access to the area may be implemented either mechanically, electronically or based on personal identification.
Implementation example	
Legislation	TLA 9
References	Julkri: FYY-05.4; Katakri: F-05.2
Other additional information	Recommendation on the handling of classified documents 2021:5, page 39; PiTuKri FT-03

Identifier	FYY-06.4, C:TL IV, I:, A:, DP:
Title	Administrative area – intrusion detection systems
Requirement	If necessary, an intrusion detection system can be used as an additional risk management control for multi-layer protection.
Overview	The area and the doors leading to it can be equipped with an intrusion detection system (burglary alarm system), if classified information is stored in the area in lockable office furniture and the risk of intrusion is assessed as likely. The area and the routes leading to the area can be equipped with an intrusion detection system (burglary alarm system), if classified information is stored in the area and the risk of intrusion is assessed as likely. When assessing the potential intrusion detection system or a substitute arrangement of the area, the response time estimate processed in connection with the requirement concerning the structures of the area must be taken into account. If the area is controlled by an intrusion detection system, it is recommended that the area be monitored by the system when no work is carried out in the area. The location premises of the intrusion detection system should be located in the security area protected by it.
Implementation example	It is recommended that the equipment and systems included in the multi-layer protection solution comply with European standards and their minimum requirements. Standards that can be used as a reference when assessing an appropriate solution: Intrusion detection systems: SFS-EN 50131 grades 1–4, target level 2; Intrusion alarm transmission: SFS-EN 50136-1 categories DP1–DP4 and SP5–SP6; Security company's alarm receiving centre: SFS-EN 50518
Legislation	TLA 7
References	Katakri: F-05.5
Other additional information	Recommendation on the handling of classified documents 2021:5, page 40

Identifier	FYY-07, C:TL III, I:, A:, DP:
Title	Secured area
Requirement	A secured area must meet the recommendations presented in this section and the risk-based additional specifications so that the objectives of defence in depth are achieved.
Overview	A secured area refers to areas and facilities that are more secure than the administrative area and are intended for the work of an organisation and in which classified information is processed and stored. A secured area may be temporarily established in an administrative area for a classified meeting or other similar purpose. The secured area must meet the recommendations set out in this section. In addition to the recommendations, other risk management measures based on risk assessment and the multi-layer protection principle must be planned, assigned, implemented and maintained so that residual risks to classified information can be accepted and the objectives of defence in depth achieved. In addition, the secured area must take into account all the common recommendations for security areas described in the criterion "Security area".

Implementation example	
Legislation	TLA 7, 9
References	Julkri: FYY-05; Katakri: F-06
Other additional information	Recommendation on the handling of classified documents 2021:5, page 43
Identifier	**FYY-07.1, C:TL III, I:, A:, DP:**
Title	Secured area – boundary and structures of the area
Requirement	The area must have a clearly specified, visible boundary. If the area does not have a storage solution that is deemed sufficient for information storage, the walls, floor, ceiling, windows and doors of the area must provide the level of security required for the storage of information.
Overview	It must be possible to lock or close, with bars or metal grilles, openings in the area which are not used for passage in order to allow reliable control of access to the area. The openings must be monitored by an intrusion detection system if the area is not staffed 24 hours a day or if the premises are not inspected at the end of normal working hours and at occasional times outside working hours. The structures of the area should be reinforced if classified information is stored in the area and the risk of breaking in is assessed as likely. The boundary and structures of the area should be concrete, steel, brick or strong wood. Inadequate structures, such as a normal office structure, must be reinforced. It must not be possible to remove the wall elements as whole elements from outside the space. These reinforcements must be assessed in relation to the other security provided by the facilities surrounding the area and the response time of the security personnel. When inspecting door structures, attention must be paid to the frame structure, the clearance between the door and the frame, and the attachment of the frames to the wall structure. If the area does not have a storage solution that is deemed sufficient for information storage, the walls, floor, ceiling, windows and doors of the area should meet a minimum level of protection equivalent to that of classification RC3 of SFS-EN-1627. Armoured glass should primarily be implemented as part of the normal window structure. Retrofit solutions should be avoided. Emergency escape routes must not pass through a secured area. If it is necessary for an emergency exit route to pass through a secured area, it must be ensured that the emergency exit route is equipped with an intrusion detection system. A secured area through which an emergency exit route passes cannot be accepted, if entering the secured area in practice means immediate access to classified information in the area or if the area does not have a storage solution deemed sufficient for storing the information.
Implementation example	Walls and doors and floor and ceiling structures: SFS-EN 1627, RC1-RC6, target level RC3; Windows (armoured glass): SFS-EN 356, P4A-P5A and P6B-P8B, target level P5A
Legislation	TLA 9(1) item 2
References	Katakri: F-06.1
Other additional information	Recommendation on the handling of classified documents 2021:5, page 43

Identifier	FYY-07.2, C:TL III, I:, A:, DP:
Title	Secured area – physical access monitoring
Requirement	At the border of the area, all entry and exit must be monitored by means of physical access permits or by personally identifying the persons.
Overview	The physical access monitoring may be implemented either electronically or based on personal identification. Two-sided physical access control can be used at the border of the area. It is recommended to use double identification when going in and/or out. Based on the risk assessment, remote connections of the physical access monitoring system and installation of readers must be implemented in a sufficiently secure manner, so that access to the system is possible only from authorised devices and networks, and so that the data connection and interfaces of the physical access monitoring system are protected so that outsiders do not have access to the transmitted data. The location premises of the physical access monitoring system should be located in the security area protected by it.
Implementation example	Recommendation on implementing access control: - The organisation uses photo ID cards or similar visible identifiers. - Access rights to the secured area are granted by a designated person responsible in the organisation - The procedures of the physical access control system have been instructed and documented: -- A document will be drawn up of the access rights granted, and it will be maintained by a designated person in charge. -- A person only has the physical access rights necessary for the performance of their duties. -- The grounds for granting physical access rights are recorded in the document, and only designated persons have a physical access right to the area. -- If necessary, changes in personnel are reflected in the physical access rights. -- Lists of personnel and external persons within the organisation are kept separate. -- Physical access rights are reviewed at regular intervals, for example every 6 months, by a person responsible designated within the organisation. -- The management of the physical access control system may be outsourced if it is well managed. -- Door opening from an end-user workstation to the secured area must be prevented - Only authorised persons have access to the secured area. Access to the area must be verifiable at a later stage. - Access to the space must be verifiable at a later stage. - Tags must use modern and encrypted reading technology or require double identification It is recommended that the equipment and systems included in the multi-layer protection solution comply with European standards and their minimum requirements: Electronic access control systems: SFS-EN 60839-11-1 and 2, categories 1–4. Camera surveillance systems: SFS-EN 62676, Planning in accordance with Finance Finland's K method. The storage time of camera surveillance system recordings is determined on a risk basis in accordance with the organisation's ability to observe deviations, taking into account proactive and reactive procedures. The recommended minimum retention time for recordings is 1 month. In addition, the camera surveillance system can be connected to an intrusion detection system.
Legislation	TLA 9(1) item 2
References	Katakri: F-06.2
Other additional information	Recommendation on the handling of classified documents 2021:5, page 43

Identifier	FYY-07.3, C:TL III, I:, A:, DP:
Title	Secured area – granting of physical access rights
Requirement	An independent right of access to the area may only be granted to a person duly authorised by the organisation, whose reliability has been verified and who is specifically authorised to enter the area.
Overview	Reliability should primarily be ensured by means of a personal security clearance procedure. Access to the area should be based on the need for information. On a case-by-case basis, a special authorisation may also mean the need to work in the area. A person responsible for managing access rights, access tokens and keys must be appointed for the area.
Implementation example	
Legislation	TLA 9(1) item 2
References	Julkri: FYY-05.4; Katakri: F-06.3
Other additional information	Recommendation on the handling of classified documents 2021:5, page 44

Identifier	FYY-07.4, C:TL III, I:, A:, DP:
Title	Secured area – visitors
Requirement	If entering a secured area in practice means immediate access to classified information in the secured area: - the highest level of security of information normally stored in the area must be clearly indicated, and - all visitors must have a special authorisation to enter the area, they must always be escorted, and their reliability must have been properly verified, unless it is ensured that visitors do not have access to classified information.
Overview	The criterion complements the criterion "Security area – Visitors" for all security areas.
Implementation example	
Legislation	TLA 9(1) item 2, 10(1)
References	Julkri: FYY-05.5; Katakri: F-06.4
Other additional information	Recommendation on the handling of classified documents 2021:5, page 44

Identifier	FYY-07.5, C:TL III, I:, A:, DP:
Title	Secured area – security Instructions
Requirement	Instructions on the security procedures to be followed must be drawn up for each secured area.
Overview	The security instructions cover the processes and security areas related to classified information throughout its lifecycle. Compliance with the security instructions is monitored, and the need to amend the instructions is assessed regularly. The timeliness and implementation of the security instructions are verified regularly, at least annually.

Implementation example	Security procedures must be prepared for each secured area, with instructions on: a) the retention and processing of information in the area: a classification level for information that can be processed and stored in the area b) monitoring and protection measures to be applied c) granting of physical access rights to the area: persons with unescorted access to the area on the basis of specific authorisation and verification of reliability d) visitors: where appropriate, procedures for the use of escorts or for the protection of security classified information when other persons are granted access to the area e) other relevant measures and procedures
Legislation	TihL 4(2); TLA 10(1)
References	Julkri: HAL-12; Katakri: F-06.5
Other additional information	Recommendation on the handling of classified documents 2021:5, page 45
Identifier	**FYY-07.6, C:TL III, I:, A:, DP:**
Title	Secured area – intrusion detection systems
Requirement	An area where no personnel are employed 24 hours a day must, if necessary, be inspected at the end of normal working hours and at occasional times outside working hours, unless an intrusion detection system (burglary alarm system) is installed in the area.
Overview	The boundary and structures of the area (walls, doors and windows, floor and ceiling structures) and/or routes leading to the area may be equipped with an intrusion detection system (burglary alarm system), provided that classified information is maintained in the area and the risk of break-in is assessed as likely. When assessing the potential intrusion detection system or a substitute arrangement of the area, the response time estimate processed in connection with the requirement concerning the structures of the area must be taken into account. If the area is controlled by an intrusion detection system, it is recommended that the area be monitored by the system when no work is carried out in the area. Transmission of alarms should be implemented with supervision or with a redundantly secured connection. The alarm transmission device must be used to transmit at least the following information to a security company or other security control room: burglary, on/off, sabotage, fault. The system must be operated using a personal code. Based on the risk assessment, remote connections of the system and installation of management devices must be implemented in a sufficiently secure manner, so that access to the system is possible only from authorised devices and networks, and so that the data connection and interfaces of the intrusion detection system are protected so that outsiders do not have access to the transmitted data. The location premises of the intrusion detection system should be located in the security area protected by it. The management of the area intrusion detection system must be under the control of the organisation. Management may be outsourced based on risk assessment and task separation. Procedures related to system management, alarms and response must be evaluated. The testing of alarm transmission (once a month) and response time (once a year) must be regular and documented. The security personnel must be trained to operate in the area. The skills and tools of the security personnel must be sufficient in relation to the risks in the operating environment. It can be required that two people arrive in the area simultaneously in the event of an alarm, if entering the secured area in practice means immediate access to classified information in the area, or if the area does not have a storage solution deemed sufficient for storing the information.

Implementation example	It is recommended that the equipment and systems included in the multi-layer protection solution comply with European standards and their minimum requirements: Intrusion detection systems: SFS-EN 50131, categories 1–4, target level 3; Alarm transmission of the intrusion detection system: SFS-EN 50136-1, categories DP1–DP4 and SP5–SP6, target level DP3–DP4 (dual path) or SP5–SP6 (single path); Security company's alarm centre: SFS-EN 50518, The company must be competent in accordance with the standard and also maintain a quality management system certified in accordance with SFS-EN ISO 9001, or the company must have been assessed to meet this standard where applicable.
Legislation	TLA 7, 9(1) item 2
References	Katakri: F-06.7
Other additional information	Recommendation on the handling of classified documents 2021:5, page 45
Identifier	**FYY-07.7, C:TL III, I:, A:, DP:**
Title	Secured area – keys and access codes for storage units
Requirement	The keys or access codes of the storage units are held by persons who need to know the information contained in the storage unit. The persons concerned must know the number combinations by heart. The number combinations of the storage units containing classified information must be changed: - factory default codes must be changed when receiving a new secure storage location - whenever there is a change in the personnel who know the number combination - whenever information is compromised or is believed to be compromised - after any of the locks have been serviced or repaired
Overview	
Implementation example	
Legislation	TLA 8, 9(1) item 2, 10(1)
References	Katakri: F-06.10
Other additional information	Recommendation on the handling of classified documents 2021:5, page 46

Identifier	FYY-08, C:Secret, I:, A:, DP:Special category of personal data
Title	Transport of information
Requirement	1. Information must be transported in accordance with the organisation's instructions that take sufficient protection of the data into account. 2. The information must be packaged in such a way that it is protected against unauthorised disclosure. 3. Information may be transported outside security areas by protecting electronic media with sufficiently secure encryption. 4. Unencrypted information can be transported through postal services.
Overview	
Implementation example	
Legislation	TihL 13(1); TLA 13
References	Julkri: TEK-16, FYY-02; Katakri: F-08.1
Other additional information	Recommendation on the handling of classified documents 2021:5, pages 26–28
Identifier	**FYY-08.1, C:TL IV, I:, A:, DP:**
Title	Data transport – TL IV
Requirement	The subcriterion specifies the requirement of the main criterion.
Overview	
Implementation example	The requirement for security classification level IV information can be met by implementing the measures listed below: 1) The information is packaged in a sealed envelope or equivalent. The outer envelope of the packaging must not bear a classification level or otherwise reveal that it contains security classified information (the envelope or equivalent must be opaque). 2) The information is delivered in Finland as ordinary mail, registered mail or in accordance with an approved procedure for the security classification level in question. Delivery abroad by mail only based on separate approval by the authorities. 3) The organisation's internal mail handling chain only includes approved personnel. 4) The organisation has identified requirements and implemented procedures for the transmission of information subject to special protection (e.g. encryption keys).
Legislation	TLA 13
References	Katakri: F-08.1
Other additional information	

Identifier	FYY-08.2, C:TL III, I:, A:, DP:
Title	Data transport – TL III
Requirement	Unencrypted information in security classification level II to III must be appropriately packaged for transport and transported under continuous supervision to the recipient. Such information may also be transported to the recipient by other secure means that ensure the confidentiality and integrity of the information in a manner adequate for the classification level in question.
Overview	
Implementation example	The requirement for security classification level III information can be met by also implementing the measures listed below: 5) The information is packaged in a double sealed envelope or equivalent. The outer envelope of the packaging must not bear a classification level or otherwise reveal that it contains security classified information (envelopes or equivalent must be opaque). 6) The information is delivered to the recipient under continuous supervision by a person in the organisation entitled to the classified information in question. Alternatively, delivery in accordance with the procedure approved for the security classification level in question. 7) The organisation's internal mail handling chain only includes approved, security-cleared personnel.
Legislation	TLA 13
References	Katakri: F-08.1
Other additional information	

Identifier	FYY-08.3, C:TL II, I:, A:, DP:
Title	Data transport – TL II
Requirement	The subcriterion specifies the requirement of the main criterion.
Overview	
Implementation example	The requirement for security classification level II information can be met by also implementing the measures listed below: 8) The information is packaged in a double sealed envelope or equivalent. The outer envelope of the packaging must not bear a classification level or otherwise reveal that it contains security classified information (envelopes or equivalent must be opaque). The inner envelope must be closed with a security seal. The recipient must be instructed to check the integrity of the seal and must provide immediate notice if there is a suspicion that the integrity is compromised.
Legislation	TLA 13
References	Katakri: F-08.1
Other additional information	

Identifier	FYY-09, C:Secret, I:, A:, DP:Special category of personal data
Title	Copying information
Requirement	Copies and translations are subject to the security measures regarding the original information.
Overview	Printers and copiers are interpreted as information systems and must therefore meet the requirements for technical, physical and administrative information security. Technical requirements can be met, for example, by means of a separate device solution.
Implementation example	The requirement can be met by implementing the measures listed below: 1) Copies are processed as original information. 2) A copy can only be handed over to a person who has the right to process the information and the need for the content. 3) A copy/print may only be made with a device that meets the security requirements.
Legislation	TihL 13(1); TLA 2(2)
References	Katakri: F-08.2
Other additional information	Recommendation on the handling of classified documents 2021:5, page 28
Identifier	**FYY-09.1, C:TL II, I:, A:, DP:**
Title	Copying information – TL II
Requirement	Copies of the information and their processors must be listed. Permission of the authority that prepared the data must be obtained for copying the information.
Overview	
Implementation example	The requirement may be met by the following additional measure: 4) Copying and processors are entered in a register/journal or listed using another similar procedure.
Legislation	TLA 14(1) items 3 and 4
References	Katakri: F-08.2
Other additional information	
Identifier	**FYY-10, C:TL III, I:, A:, DP:**
Title	Registration of information
Requirement	Receipt and transmission of information in security classification level III or higher must be registered. The processing of security classification level III and higher information is registered in an electronic log, information system, case management system, case register or in the information itself (for example, as part of a document).
Overview	Register-keeping refers to the application of procedures to register the lifecycle of information, including its distribution and destruction. In the case of an information system, the registration procedures may be carried out through the system's own processes. Practical implementation of information lifecycle registration typically requires, for example, ensuring the traceability of events.

Implementation example	
Legislation	TLA 14(1) items 1 and 2
References	Katakri: F-08.3
Other additional information	Recommendation on the handling of classified documents 2021:5, pages 19–23
Identifier	**FYY-11, C:Secret, I:, A:, DP:Special category of personal data**
Title	Physical destruction of data
Requirement	The destruction of non-electronic data is organised reliably. Methods of destruction are used to prevent any or all of the data from being reassembled.
Overview	Data protection must be ensured until the end of the data life cycle. This must be taken into account especially in situations where a third-party service is used to destroy data. As a practical implementation model, a procedure in which the organisation responsible for the data monitors the data destruction process until the end of the life cycle. It is recommended that the equipment and systems included in the multi-layer protection solution comply with European standards and their minimum requirements. When using approved shredder sizes, shredding waste can be disposed of as normal office waste. Other methods to reliably prevent the assembly of data (e.g., burning of shredded paper) may also be used to replace or support shredding. The destruction of electronic materials is described separately in criterion TEK-21.
Implementation example	
Legislation	TihL 21; TLA 15
References	Julkri: TEK-21; Katakri: F-08.4
Other additional information	Recommendation on the handling of classified documents 2021:5, pages 29–31
Identifier	**FYY-11.1, C:TL IV, I:, A:, DP:**
Title	Physical destruction of data – TL IV
Requirement	The subcriterion specifies the requirement of the main criterion.
Overview	
Implementation example	- The maximum shredding size of the paper is 30 mm2 (DIN 66399/P5 or DIN 32757/DIN 4). - The shredding size of magnetic hard drives is up to 320 mm2 (DIN 66399/H-5). - The shredding size of solid-state drives and USB flash memory is up to 10 mm2 (DIN 66399/E-5). - The shredding size of optical media is up to 10 mm2 (DIN 66399/O-5).
Legislation	TLA 15
References	Katakri: F-08.4
Other additional information	

Identifier	FYY-11.2, C:TL III, I:, A:, DP:
Title	Physical destruction of data – TL III
Requirement	The subcriterion specifies the requirement of the main criterion.
Overview	
Implementation example	- The maximum shredding size of the paper is 30 mm2 (DIN 66399/P5 or DIN 32757/DIN 4). - The shredding size of magnetic hard drives is up to 10 mm2 (DIN 66399/H-6). - The shredding size of solid-state drives and USB flash memory is up to 10 mm2 (DIN 66399/E-5). - The shredding size of optical media is up to 5 mm2 (DIN 66399/O-6).
Legislation	TLA 15
References	Katakri: F-08.4
Other additional information	

Identifier	FYY-11.3, C:TL II, I:, A:, DP:
Title	Physical destruction of data – TL II
Requirement	If the information has been prepared by another authority, the destruction of the information that has become unnecessary must be reported to the authority that has prepared the information, unless it is returned to the authority that has prepared the information. The data may only be destroyed by a person assigned to this task by an authority. Versions of the preparatory phase can be destroyed by the person who created them.
Overview	
Implementation example	- The shredding size of paper material is up to 10 mm2 (DIN 66399/P6). - The shredding size of magnetic hard drives is up to 10 mm2 (DIN 66399/H-6). - The shredding size of solid-state drives and USB flash memory is up to 1 mm2 (DIN 66399/E-6). - The shredding size of optical media is up to 5 mm2 (DIN 66399/O-6).
Legislation	TLA 15
References	Katakri: F-08.4
Other additional information	

4 Technical security

The technical sub-area covers the criteria related to the technical measures, secure operation and operating models of information systems and networks. The objective of the criteria is to ensure that information systems and their use implement the requirements of general technical information security and, if necessary, data protection. It should be noted, however, that implementing the criteria of the technical sub-area alone does not guarantee the security of an individual information system, but the criteria in other areas must also be taken into account.

The assessment may target either an individual information system or a data processing environment or a broader entity of information systems. When assessing an entity consisting of several information systems, the fulfilment of the requirements in all individual systems must be taken into account.

The technical sub-area also takes into account the location of systems in security areas and their remote use outside security areas. More detailed requirements for the administrative area and secured area have been defined in the sub-area of physical security.

With regard to several criteria, the criteria refer to the fact that the encryption solution must be sufficiently secure for the use case in question. For example, approvals granted by the NCSA function of the National Cyber Security Centre to protect international classified information can be considered in the security assessment of the encryption solution. Further information is available on the website of the National Cyber Security Centre.

Identifier	TEK-01, C:Secret, I:, A:, DP:Special category of personal data
Title	Structural security of the network
Requirement	The information processing environment is separated from public information networks and other lower-security environments in a sufficiently secure manner.
Overview	The segregation of information systems is one of the most effective factors in the protection of secret information. The objective of separation is to limit the processing environment of secret information to a manageable entity and, in particular, to limit the processing of secret information to sufficiently secure environments. It is also possible to process lower-class data in a higher-class processing environment, provided that the processing is carried out in its entirety in accordance with the protection of the higher security class. Separation can be implemented, for example, through a firewall solution. The Internet, as well as MPLS networks offered by carriers and, for example, the so-called dark fibre, are interpreted as public networks.
Implementation example	
Legislation	TihL 13(1); TLA 11(1) item 1
References	Katakri: I-01
Other additional information	Traficom: Guide for planning principles and solution models for gateway solutions (2 December 2021); ISO/IEC 27002:2022 8.20, 8.22; Information Management Board: Recommendation on the handling of classified documents (2020:19, chapter 6); PiTuKri TT-01

Identifier	TEK-01.1, C:Secret, I:Critical, A:, DP:Personal data
Title	Structural network security – encryption in public information networks
Requirement	In a public information network, data communication containing secret information is encrypted by means of an encryption solution that does not contain known vulnerabilities and that, according to the information received from the manufacturer, supports modern encryption strengths and settings, or alternatively, by using a secure communication connection or method.
Overview	When selecting the encryption strengths and settings to be used, the strengths and settings of security classification level IV can be used as a rule.
Implementation example	
Legislation	TihL 14; TihL 12 and 11(1) item 7
References	Julkri: FYY-7.1; Katakri: I-01, I-12, I-15
Other additional information	ISO/IEC 27002:2022 8.24

Identifier	TEK-01.2, C:Secret, I:Important, A:, DP:Special category of personal data
Title	Structural security of the network – firewall
Requirement	Connecting the computing environment to other security level environments requires the use of at least a firewall solution.
Overview	
Implementation example	
Legislation	TihL 13(1); TLA 11(1) items 1 and 2
References	Katakri: I-01
Other additional information	PiTuKri TT-01
Identifier	**TEK-01.3, C:TL IV, I:, A:, DP:**
Title	Structural security of the network – segregation of processing environments
Requirement	The computing environment is separated from other environments.
Overview	
Implementation example	Combining the information processing environments for unclassified secret information and also security classification level IV data with different security-class environments can be achieved by means of firewall solutions and by limiting traffic of risk-prone services using a lower security-class environment (web browsing, Internet-routed e-mail and similar) through separate content-filtering proxies. It is possible to connect the processing environments of unclassified secret information and security classification level IV information to the Internet and other untrusted networks, provided that the risks posed by the connection can be sufficiently mitigated by other safeguards. Reducing the risks posed by Internet connectivity to unclassified secret information and security classification level IV requires, in particular, taking care of software updates, access rights in accordance with the principle of least privilege, system hardening and the ability to detect and resolve deviations. A typical use method for an unclassified secret or/and security classification level IV processing environment is a limited partition of the organisation's information processing environment, which may consist of, for example, terminal device services, application services, communication services and arrangements related to their protection.
Legislation	TihL 13(1); TLA 11(1) items 1 and 2
References	Katakri: I-01, I-06, I-08, I-11, I-19
Other additional information	

Identifier	TEK-01.4, C:TL IV, I:, A:, DP:
Title	Structural security of the network – encryption outside secured areas
Requirement	Traffic outside the controlled physical security area is encrypted with a sufficiently secure encryption solution.
Overview	
Implementation example	
Legislation	TihL 14; TLA 11(1) item 7, 12
References	Katakri: I-01
Other additional information	

Identifier	TEK-01.5, C:TL III, I:, A:, DP:
Title	Structural security of the network – gateway solution use
Requirement	Security classification levels III–II: Connecting the computing environment to other security-class environments requires the use of a sufficiently secure gateway solution.
Overview	As a starting point, information processing environments are expected to be untrusted for each other, also in situations where information processing environments managed by different organisations are connected to each other. Processing environments of the same security class can be connected to each other by means of an encryption solution sufficiently secure for the security classification level in question (for example, the interconnection of a specific security class's processing environments at different locations within the organisation over a public network). Note: exceeding the security class for management traffic requires the use of a sufficiently secure gateway solution for the security classification level in question. In practice, management traffic is almost invariably restricted by security class. The protection principles of management traffic are discussed in more detail in TEK-04.

Implementation example	From security classification level III onwards, connection to different security-class environments can be implemented with sufficiently secure gateway solutions. The gateway solution must reliably prevent the transfer of information of a higher security class to a lower security-class environment. The planning principles and general solution models for secure, acceptable gateway solutions are described in more detail in the National Cyber Security Centre's gateway solution guide (www.ncsa.fi > "Guide for planning principles and solution models for gateway solutions"). Security classification level III processing environments are entities isolated logically or physically on multiple layers from untrusted networks/systems. Physical isolation refers to the separation at the level of the OSI model physical layer. As a general rule, no other networks or systems are connected to security classification level III processing environments. If the end-user's tasks require access to the Internet or other systems or networks of other security classes, it is usually most justified to arrange this on a separate computer that is not connected to a security classification level III network. On a case-by-case basis, it is also possible to approve the physical connection of a security classification level III processing environment to a separately inspected and approved network or system. Such separately approved networks or systems are most commonly divided into four operating situations: A. Data transmission systems A security classification level III system/network may be a communication system between two or more physical points. In this case, each connected point should be at an equivalent security level. The network-level interface is usually in the form [physically isolated network/workstation] – [firewall hardware/software] – [encryption device approved for the security class] – [firewall hardware/software] – [Internet] – [firewall hardware/software] – [encryption device approved for the security class] – [firewall hardware/software] – [physically isolated network/workstation]. Equivalent arrangements may also be used to implement a security classification level II solution. B. System services A security classification level III system/network can be, for example, a database service that is used from several physical points. In this case, the network-level interface is corresponding to the one in use situation A. C. Gateway solutions C1. Data may be transferred to a security classification level III data processing environment from a lower security-class environment through a one-way gateway solution (e.g., a data diode). Equivalent arrangements may also be used to implement a security classification level II solution. A content filtering solution based on object identification can also be used for communication between security classes IV and III (see C2 below). C2. Information of a lower security-class can be transferred from a security classification level III information processing environment to a lower security-class environment through a content filtering solution based on object identification. The use of a content filtering solution requires the identification of information in a higher-level environment, and only allowing the transfer of lower-level information from a higher-level environment to a lower-level environment. D. Other processing environments Other security classification level III processing environments are most commonly the organisation's product development networks or other security classification III information processing environments. For example, an update server that only serves that environment can be connected to such systems. Centralised distribution of security updates and malware signatures can be allowed with certain limitations from the update server. The updates and signature databases to be distributed can be brought to the update server over an air gap or, alternatively, through a data diode.
Legislation	TLA 11(1) items 1 and 2
References	Julkri: TEK-04; Katakri: I-01
Other additional information	

Identifier	TEK-01.6, C:TL II, I:, A:, DP:
Title	Structural security of the network – TL II processing
Requirement	As a premise, security classification level II processing environments are physically isolated entities.
Overview	
Implementation example	Traffic exceeding the security class may only be permitted through data diodes or equivalent one-way gateway solutions operating on an OSI model physical layer.
Legislation	TLA 11(1) items 1 and 2
References	Katakri: I-01
Other additional information	

Identifier	TEK-01.7, C:TL I, I:, A:, DP:
Title	Structural security of the network – TL I processing
Requirement	The subcriterion specifies the requirement of the main criterion.
Overview	
Implementation example	As a premise, it is recommended that security classification level I information environments be kept physically separated from all other environments. A typical method of implementation is processing of information, separated physically from all other environments in a physical, secured area, in a radiation-proof space, using a dedicated terminal device. Similarly, the implementation method may also be a computing environment consisting of terminal equipment, a local network connecting the equipment and a dedicated printer physically placed in a secured area in a radiation-proof space and physically separated from other environments. Data transfer to physically differentiated environments must be implemented in such a way that the risk of security classification level I data being transferred to a lower-security environment is minimised. A typical implementation method is the use of single-use optical media in data transfers from a lower security-class environment to a higher security-class environment. If, from the perspective of functional needs, a security classification level I information processing environment must absolutely necessarily be connected to a lower security-class environment, the connection should take place through a gateway solution approved for security classification level I. The availability of gateway solutions accepted for separation of security classification level I computing environments is scarce, typically focusing only on multi-tier data diode solutions that enable one-way communication (TL II > TL I). Gateway solutions are described in more detail in the National Cyber Security Centre's gateway solution guide.
Legislation	TLA 11(1) items 1 and 2
References	Katakri: I-01
Other additional information	

Identifier	TEK-02, C:Secret, I:Important, A:Important, DP:Special category of personal data
Title	Zoning the communications network
Requirement	The zoning of a telecommunications network and the filtering rules must be implemented in accordance with the principle of multi-layer protection.
Overview	Dividing the communications network within a security class into separate network areas (zones and segments) may, for example, mean segregation of workstations and servers appropriate from the perspective of data protection, also covering possible project-specific segregation needs. As a rule, all connected IT systems should be treated as untrusted, and general network attacks should be prepared for. Preparedness for general network attacks includes, for example, keeping only the necessary functionalities on. In other words, there should be a justified functional need for each function that is on. Functionality should be limited to the smallest subset that meets the functional requirements (for example, limiting the visibility of functionalities). Preventing address spoofing and limiting the visibility of networks should also be considered.
Implementation example	The requirement can be met by implementing the measures listed below: 1) The communication network is divided into separate network areas (zones, segments) within a security class. 2) Traffic between network zones is restricted and traffic entering the environment is subject to the default-deny rule. 3) The data processing environment is prepared for general network attacks.
Legislation	TihL 13(1); TLA 11(1) items 1 and 2
References	Katakri: I-02
Other additional information	ISO/IEC 27002:2022 8.20, 8.21, 8.22, 8.23; PiTuKri TT-01, TT-02

Identifier	TEK-02.1, C:TL IV, I:, A:, DP:
Title	Zoning the communications network – principle of least privilege
Requirement	The zoning of the communications network and the filtering rules must be implemented in accordance with the principle of least privilege within the relevant security class.
Overview	The monitoring and restriction of traffic between network zones can be implemented at the external border of a security classification level IV network, for example by preventing all inbound connection attempts and restricting outbound connections to web browsing and e-mail traffic only through a proxy server. Consideration of the principle of least privilege, which needs to be taken into account in the networks of all security classes, typically also requires that, within the security class, only the necessary connections between different network zones are allowed (source–target protocol) and that other connection attempts are detected. Within the environment of a specific class, protection can also be complemented and supported by the so-called zero trust approach, in which the opportunities for action of different actors can be limited and controlled, in particular based on the identification and authentication of operators and activities. However, it should be noted that the zero trust approach does not replace the requirement for sufficiently reliable separation of the computing environments of different protection needs/classes (see TEK-01.3 and TEK-01.5). In the implementation of the zero trust approach, the identification and authentication of actors in the information processing environment (users and devices) and adequate encryption of communication between actors play a key role. The secure operation of connections and configurations must be ensured regularly, see TEK-03. Security classification level IV should also take into account the risk of a denial-of-service attack, if the system is connected to an untrusted network. Filtering should be based on the principle of least privilege, and filtering should only allow specifically approved traffic (default-deny). Filtering should also take into account the functionalities of different protocols (e.g., IPv4, IPv6, GRE, IPSec tunnels, routing protocols, and also higher-level protocols, e.g., HTTP, SSH, FTP and SMTP). Unnecessary protocols should be disabled on all systems (workstations, servers, network devices etc.) where there is no real basis of use for them, and it should be ensured that communication is blocked (network, client and server level) with firewall filtering rules. If, for example, IPv6 functionality is used in workstations, servers, network devices or other similar systems, its effects on traffic filtering (firewall should also cover IPv6 traffic) and routing should be taken into account. The impacts of different protocol consolidation and shared-use solutions (e.g. IPv4 and IPv6 implementations, NAT-64, Teredo) should also be taken into account in overall network/system security design.
Implementation example	For processing environments of security classes IV–II, the requirement can be met by implementing the following measures, in addition to the measures mentioned above: 4) Traffic between network zones is monitored and restricted so that only specifically approved traffic necessary for operation is permitted (default-deny).
Legislation	TLA 11(1) items 1 and 2
References	Julkri: TEK-03; Katakri: I-02
Other additional information	ISO/IEC 27002:2022 8.20, 8.21, 8.22, 8.23; PiTuKri TT-01, TT-02

Identifier	TEK-03, C:Secret, I:Important, A:Important, DP:Special category of personal data
Title	Management of filtering and monitoring systems
Requirement	The appropriate operation of filtering and monitoring systems is ensured throughout the lifecycle of the computing environment.
Overview	Systems that filter and/or monitor traffic typically include firewalls, routers, and IDS and IPS systems, as well as network devices, servers and applications with similar functionalities. The implementation of sufficient documentation usually requires, for example, describing the network structure and its network areas (zones and segments) at the level of detail that the documentation can be used to verify that the network corresponds to a documented, sufficiently secure structure. A solution that is appropriate for ensuring usability and adequate documentation is often backing up the settings of filtering and monitoring systems (configurations, including firewall rules etc.) and storing the backups according to the security class. The frequency of inspections that can be accepted for examining the settings and the desired operation depends in particular on the frequency of changes at the site and the extent of the site. For example, an organisation's security classification level IV information processing environment may have extensive firewall policies that may require frequent changes. In such environments, sufficient inspection frequency may be, for example, quarterly or semi-annual. On the other hand, in smaller environments where there is no need to make changes to the filtering rules, annual inspections may be sufficient. The functionality of filtering or monitoring software may also be subject to changes or new features during regular software updates. It is therefore justified to ensure that the filtering rules and other functionalities are correct also when software updates are installed. The possibilities of using and introducing new features (e.g., finer filtering) should be assessed as part of change management (see I-16).
Implementation example	
Legislation	TihL 13(1); TLA 11(1) item 2
References	Katakri: I-03
Other additional information	ISO/IEC 27002:2022 8.21, 8.23

Identifier	TEK-03.1, C:Secret, I:Important, A:Important, DP:Special category of personal data
Title	Management of filtering and monitoring systems – responsibilities and organisation
Requirement	Responsibility for adding, changing, deleting and monitoring settings for systems that filter or monitor traffic has been assigned and the operations have been organised.
Overview	
Implementation example	
Legislation	TihL 4(2) item 1 TLA 11(1) item 2

References	Katakri: I-03, I-16
Other additional information	ISO/IEC 27002:2022 5.35; PiTuKri MH-01
Identifier	**TEK-03.2, C:Secret, I:Important, A:Important, DP:Special category of personal data**
Title	Management of filtering and monitoring systems – documentation
Requirement	The documentation of the network and related filtering and monitoring systems is maintained during its lifecycle as an integral part of the change and configuration management process.
Overview	
Implementation example	
Legislation	TihL 5(2); TLA 11(1) item 2
References	Julkri: HAL-09; Katakri: I-03
Other additional information	
Identifier	**TEK-03.3, C:Secret, I:Important, A:Important, DP:Special category of personal data**
Title	Management of filtering and monitoring systems – reviews
Requirement	The configuration and desired operation of systems that filter or monitor traffic are periodically checked during the operation and maintenance of the information processing environment and in the event of exceptional situations.
Overview	
Implementation example	
Legislation	TihL 13(1); TLA 11(1) item 2
References	Katakri: I-03
Other additional information	ISO/IEC 27002:2022 8.32

Identifier	TEK-04, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Management connections
Requirement	Management access takes place through limited, managed and controlled points.
Overview	In the implementation examples described below, devices/interfaces refer to systems to which only administrators or equivalent should have administrator access. Typically, these include firewalls, routers, switches, wireless access points, servers, workstations, separate console interfaces (e.g. iLO, iDRAC), and blade chassis management interfaces. When assessing the security of management connections, particular attention should be paid to the extent to which the management connection in question can be used to compromise secret information. Most management methods allow access to secret information either directly (for example, database management can usually access the content of the database if necessary) or indirectly (for example, network device management can usually change firewall rules that protect the information system), making these particularly attractive to malicious actors. Especially in situations where a management connection enables direct or indirect access to classified information, the management connection and the devices used for it should be limited to the same security class as the data processing environment in question. In certain specific cases, management of a lower-level environment may be possible from a higher security-class management environment, provided that there is a sufficiently secure gateway solution at the security class boundaries that prevents the transfer of higher security-class information to a lower security-class environment. Especially due to software vulnerabilities in connection protocols, the management possibilities of lower-level environments are typically limited on a risk-based basis only to the management of lower-level environments from security classification level IV environments. As a general rule, the management of a higher security-class environment is not possible from a lower-level environment because of the security-critical nature of management traffic. In some cases, a sufficiently secure gateway solution for a higher security-class environment can be used to provide (read-only) monitoring access to a lower security-class environment. In the implementation of sufficient traceability, the so-called jump host procedure can be used within the security class in question. This means that all control measures are implemented through the most hardened, system-specific and role-specific jump hosts, while also enabling comprehensive traceability (logging, see TEK-12). Considerations particularly in implementations that use cloud technology: - In cloud service environments, remote management is usually the most typical management procedure for both the cloud service platform itself and the customer's systems. For example, a cloud service provider's maintenance activities that occur from outside a physically secured data centre environment are interpreted as remote management. The maintenance of a cloud service customer's system component that is their responsibility is also interpreted as remote management. When assessing the security of management connections, particular attention should be paid to the extent to which the management connection in question can be used to compromise information in the cloud service. Most management methods allow access to information either directly (for example, database management can usually access the content of the database if necessary) or indirectly (for example, network device management can usually change firewall rules that protect the information system). As a rule, management connections are considered to include all means of communication that can influence the protection of secret information. Management connections typically include web consoles/portals offered to a cloud client and similar remote management connections. Especially in situations where a management connection enables direct or indirect access to secret information, the management connection and the devices used for it must be limited to the same security/protection class as the data processing environment in question. As a rule, the management of the environment used for the processing of security classified information is not possible from less secure environments or terminal equipment due to the security-critical nature of management traffic. The management of a cloud service platform containing classified information must be limited to terminal equipment that meets the requirements of the security class in question. Note that terminal equipment management solutions and other related back-end systems must also meet the requirements of the security class in question, as well as the physical facilities/areas from which management is carried out. - In assessing the part for which the customer is responsible, it is recommended that particular attention be paid to the fact that the corresponding requirements also apply to the customer and possible service providers associated with the customer's part.

Implementation example	Limited access must be implemented, for example, through jump hosts, management portals and similar procedures.
Legislation	TihL 13(1), 14(1); TLA 11(1)
References	Julkri: TEK-12; Katakri: I-04
Other additional information	Traficom: Guide for planning principles and solution models for gateway solutions (2 December 2021); ISO/IEC 27002:2022 8.2, 8.20, 8.21, 8.22; PiTuKri IP-03, TT-01
Identifier	**TEK-04.1, C:Public, I:Minor, A:Minor, DP:Personal data**
Title	Management connections – strong authentication in a public network
Requirement	Strong user authentication based on at least two authentication factors must be required for management access from a public network or other remote management solution to be used.
Overview	Protection of management connections is one of the most critical factors affecting the security of information systems. However, it may be justified to be able to manage non-classified and security classification level IV systems in particular, from outside physically secured security areas. In situations where remote management is considered justified, it is recommended that it be secured by more comprehensive security measures than remote use. For example, security classification level IV system remote management connections can be limited to individual physical and logical points.
Implementation example	For example, management connections from a public network require a VPN connection in which at least the user or device is strongly authenticated.
Legislation	TihL 13(1); TLA 11(1) item 5
References	Katakri: I-04
Other additional information	ISO/IEC 27002:2022 8.2; PiTuKri IP-03
Identifier	**TEK-04.2, C:Public, I:Minor, A:Minor, DP:Personal data**
Title	Management connections – encrypting management connections
Requirement	Management traffic in a public network is encrypted using a method suitable for the use case, favouring validated and standardised encryption solutions/protocols for correct operation.
Overview	
Implementation example	
Legislation	TihL 13(1); TLA 11(1) items 4 and 7
References	Katakri: I-04
Other additional information	ISO/IEC 27002:2022 8.24

Identifier	TEK-04.3, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Management connections – least privilege
Requirement	Management connections are limited according to the principle of least privilege.
Overview	
Implementation example	
Legislation	TihL 16; TLA 11(1) item 3
References	Julkri: HAL-2.1; Katakri: I-04
Other additional information	ISO/IEC 27002:2022 8.20

Identifier	TEK-04.4, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Management connections – personal credentials
Requirement	System and application maintenance credentials are personal.
Overview	
Implementation example	If the use of personal credentials is not technically possible in all systems or applications, agreed and documented management practices for shared credentials are required, and they must enable the unique identification of the user.
Legislation	TihL 13(1), 16; TLA 11(1) items 3 and 5
References	Katakri: I-04
Other additional information	PiTuKri IP-02

Identifier	TEK-04.5, C:TL IV, I:, A:, DP:
Title	Management connections – limiting connections by security category
Requirement	Management connections are limited by security category unless a sufficiently secure gateway solution is used, taking the security class into account.
Overview	
Implementation example	There is no interconnection to the information processing environment for management connections from other security-class environments without a secure gateway solution.
Legislation	TLA 11(1) item 1
References	Julkri: TEK-01; Katakri: I-04
Other additional information	

Identifier	TEK-04.6, C:TL IV, I:, A:, DP:
Title	Management connections – management connections with classified information
Requirement	When management traffic contains classified information and passes through a lower security-class environment, the classified information is encrypted with a sufficiently secure encryption product.
Overview	
Implementation example	The management workstation of the security class in question is connected to the device/interface only through a sufficiently secure encryption solution in situations where management traffic passes through a lower security-class environment.
Legislation	TihL 14; TLA 11(1) item 7, 12
References	Katakri: I-04, I-12
Other additional information	

Identifier	TEK-04.7, C:TL IV, I:, A:, DP:
Title	Management connections – encrypting within a security class
Requirement	When management traffic is conveyed within the security class in question, lower-level encryption or unencrypted transfer can be used based on the results of the risk management process.
Overview	
Implementation example	In situations where management traffic passes within the relevant security class (within an encryption appropriate for the security class in question or/and within a network located inside a security area approved for the storage of information of that security class, physically separated from other environments), a) the management workstation of the security class in question is physically connected to the device/interface (e.g., console cable), or b) the traffic channel of the management connection of the security class in question is otherwise reliably physically protected (e.g., cabling within the secured area), or c) the management workstation of the security class in question is connected to the device/interface with a lower-level encryption (e.g. SSH, HTTPS, SCP) secure connection. 4) management connections to devices/interfaces are allowed in accordance with the principle of least privileges only from approved sources and with specified user rights.
Legislation	TihL 14; TLA 11(1) item 7, 12
References	Katakri: I-04
Other additional information	

Identifier	TEK-04.8, C:TL III, I:, A:, DP:
Title	Management connections – TL III
Requirement	Remote management of security classification level III processing environments must be carried out from a secured area.
Overview	Security classification level III and other critical processing environments require the technical linking of remote management to approved remote management equipment (e.g., device identification).
Implementation example	Remote management using non-approved devices is technically blocked.
Legislation	TLA 10(3) item 1
References	Katakri: I-18
Other additional information	

Identifier	TEK-05, C:Secret, I:, A:, DP:Personal data
Title	Wireless communication
Requirement	In wireless data transmission, communication is encrypted with an encryption solution that has no known vulnerabilities and, according to the manufacturer's information, supports modern encryption strengths and settings.
Overview	The use of a radio interface for wireless communication (e.g., Wi-Fi, Bluetooth) is interpreted as leaving a physically protected area. In other words, the use of a radio interface is treated as traffic over the public network, which should be taken into account especially in traffic encryption and physical security. Several wireless interfaces also involve shortcomings in protocol and software implementations, which can be exploited by outsiders. The same security principle applies to wireless peripherals (for example, mice, keyboards, headphones, and video transfer systems). An exception is a situation in which the risks associated with the use of the wireless interface can be reliably reduced by means of physical security procedures (for example, the use of a wireless mouse within a secured area in a room where access to its proximity is restricted only to persons authorised for the information being processed). In addition, smartphones and corresponding lower security-class wireless devices should be taken into account, as these must not be connected to the information processing environment, for example, to charge the battery. The products and algorithms used must not contain known non-remedied vulnerabilities and weaknesses that compromise information security. In addition, the manufacturer of the products used must provide security updates for the products.
Implementation example	1) Wireless transmission having coverage outside the physically protected area is encrypted as required. 2) Wireless communication within a physically secured area, using security lower than the requirements (e.g. wireless peripherals) can be accepted if it can be ensured that the confidentiality of the data is not compromised through these connections. 3) Lower security-level devices with wireless connections are not connected to the environment.
Legislation	TihL 14; TLA 11(1) item 7, 12
References	Katakri: I-05, I-08, I-09, I-12, I-15, I-16
Other additional information	PiTuKri SA-01; ISO/IEC 27002:2022 8.22

Identifier	TEK-05.1, C:TL IV, I:, A:, DP:
Title	Wireless communication – encryption
Requirement	In wireless data transmission, communication is encrypted using an encryption solution that is sufficiently secure for the security class in question.
Overview	
Implementation example	At the TL IV level, the requirement can be implemented, for example, by tunnelling traffic with a sufficiently secure VPN solution or by using an approved application-level encryption solution.
Legislation	TihL 14; TLA 11(1) item 7, 12
References	Katakri: I-05
Other additional information	ISO/IEC 27002:2022 8.24; PiTuKri SA-01

Identifier	TEK-06, C:Secret, I:, A:, DP:Personal data
Title	Cascade effect
Requirement	The cascade effect has been taken into account in the protection of the information processing environment.
Overview	When the security class of the site's central data repository is deemed to be higher than the class of individual data elements due to the cascade effect, the specified protection methods of the data repository must be implemented in accordance with the requirements of the higher level. Specified protection methods refer to methods that limit access only to the individual or limited part of the data content required for the task and with which attempts to gain unauthorised access to a larger part of the data content are detected. When using Julkri as the evaluation tool, the cascade effect should be interpreted so that the higher-level data repository protection required includes physical security and TEK-14 (security of the application layer), TEK-12 and TEK-13 (traceability and observability), HAL-02.1 (separation of duties and responsibilities) and TEK-07 (management of access rights). It should be noted that the security class of the data repository that has risen by one class as a result of the cascade effect does not require an acceptable gateway solution between the data repository (e.g., TL III) and terminal devices (e.g., TL IV). As a result of the cascade effect, it must also be particularly taken into account with security classification level III data warehouse management solutions that the devices used for management are reliably separated from Internet-connected networks.
Implementation example	
Legislation	TihL 15(2), 13(1)
References	Julkri: HAL-04.3
Other additional information	ISO/IEC 27002:2022 5.3, 5.15, 5.16, 5.17, 5.18, 8.2; PiTuKri IP-01

Identifier	TEK-07, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Access rights management
Requirement	Access rights to information systems have been specified.
Overview	The key objective of access rights management is to ensure that only authorised users have access to the information processing environment and the information to be protected that it contains.
Implementation example	1) At least one person responsible for the access rights management of the systems has been designated. 2) A list of system users exists.
Legislation	TihL 16; TLA 8, 11(1) item 3
References	Julkri: HAL-14, HAL-14.1, HAL-19; Katakri: I-06
Other additional information	ISO/IEC 27002:2022 5.3, 5.15, 5.16, 5.17, 5.18, 8.2; PiTuKri IP-01

Identifier	TEK-07.1, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Access rights management – granting of access rights
Requirement	Access to information systems can only be granted to persons whose needs for use have been verified.
Overview	It is recommended that access rights be based on an agreement or other documented basis that can be verified (e.g., employment relationship, agreement on work to be carried out in the environment).
Implementation example	3) When granting an access right, it is verified that the recipient is a member of personnel or otherwise entitled. 4) The processing and granting of access rights have been instructed. 5) A document (paper or electronic) remains for each access right granted.
Legislation	TihL 16; TLA 8, 11(1) item 3
References	Julkri: HAL-14, HAL-10.1; Katakri: I-06
Other additional information	ISO/IEC 27002:2022 5.3, 5.15, 5.16, 5.17, 5.18, 8.2; PiTuKri IP-01

Identifier	TEK-07.2, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Access rights management – restriction of access rights
Requirement	Users of a computing environment and automated processes are given only the information, rights or authorisations necessary for the performance of their tasks.
Overview	The access rights must be limited only to the subset required for operational needs. Unnecessarily extensive rights provide the user or process, or an attacker gaining the rights of the above, with unnecessarily extensive operating possibilities. Limiting access rights according to the principle of least privilege can reduce the risks of both intentional and unintentional acts and, for example, malware. In particular, it should be noted that maintenance rights are only used for maintenance activities. A user account with maintenance access must not be used, for example, to browse the web or use e-mail. Owners of security classified information often reserve the right of audit to all networks/systems where information that they own is processed. Audits often require physical and logical access to the object to be inspected, which means that auditors often have technical access to information processed at the site. Especially in multi-project networks and other similar environments where there is a need to process the information of several different owners, it should be ensured that the structure of the network/system enables audits so that the owners of the information cannot access each other's data in connection with the audit. Note: The separation requirement for security classification level IV information does not apply to workstations or other similar limited data repositories, provided that methods deemed reliable are in place to prevent cascade effects. It is also not required to separate the information of owners who reserve the right of audit in situations where separate written approval has been received from all owners of information, accepting the risks brought about by the right of audit, or if the information owners undertake not to use the technical right of audit to the information processing environment in question. The information separation methods for different owners are divided into three main categories. a) Methods based on logical-level separation (e.g., server virtualisation and network disk folders restricted by access rights) are appropriate for security classification level IV data. b) Methods based on reliable logical separation (e.g., acceptably encrypted virtual machines on designated, customer-specific physical disks in the array, and accepted encryption of data/communications with shared network devices) are suitable for security classes IV and III for internal separation of the same security class. c) Methods based on physical separation (physical devices designated by data owner) are appropriate for security classes IV, III, II and I. Considerations particularly in implementations that use cloud technology: - When applying the requirement, the division of responsibilities between the cloud service provider and the customer must be taken into account. Typically, the cloud service provider is responsible for the access rights management of the system entity related to the provision of the cloud service, and the customer's responsibility concerns the access rights management of the part built on the service entity of the service provider (IaaS, PaaS or SaaS). In assessing the part for which the customer is responsible, it is recommended that particular attention be paid to the fact that the corresponding requirements also apply to the customer and possible service providers associated with the customer's part. - Implementation of separation using cloud technology, notes: -- The separation of secret information must be carried out with sufficient reliability, by logical or/and physical separation methods. Encryption is a common method of separation for shared network devices and storage systems, for example. Data in-transit and data at-rest encryption implemented with customer-specific keys can also be used to support other security objectives, such as the safe disposal of equipment. -- If the same equipment is used to process multiple customers' data simultaneously, it must be ensured that the physical and logical separation of data is sufficiently secure. If there is insufficient certainty, separate physical devices must be used for processing the data. For example, classified information can be stored on a physically separate virtualisation platform where, for example, interfaces related to potential processor vulnerabilities are limited to only users authorised for classified information. -- If the same hardware is used to process information from several different customers but not at the same time, it must also be ensured that the data from the previous customer has been removed sufficiently securely from the hardware (including all components, BIOS, caches of different other devices). If there is insufficient certainty, separate physical devices must be used for processing the data. Cf. PiTuKri/SI-02 (Destruction of data). -- Owners of classified secret information can reserve the right of audit to all networks/systems where information they own is processed. Audits often require physical and logical access to the object to be inspected, which means that auditors often have technical access to information processed at the site. Especially in environments where there is a need to process the information of several different owners, it must be ensured that the implementation of the network/system enables audits so that the owners of the information cannot access each other's data in connection with the audit. Especially with the IaaS and PaaS service models, the segregation of security classified information must be ensured with physically separate networks or encrypted virtual or software-based local networks. Cf. PiTuKri/SA-03 (Encryption within a physically protected security area).

Implementation example	6) In information systems, classified information is separated according to the principle of least privilege by access specifications and system processing rules or by some similar procedure. 7) In information systems, the information of owners that reserve the right of audit is stored separately from other information, separated by a method that is sufficiently secure for the security class in question.
Legislation	TihL 13(1), 15(1) item 1, 16; TLA 8, 11(1) items 3 and 4
References	Katakri: I-06
Other additional information	ISO/IEC 27002:2022 5.3, 5.15, 5.16, 5.17, 5.18, 8.2; PiTuKri IP-01, SA-03, KT-03
Identifier	**TEK-07.3, C:Public, I:Minor, A:Minor, DP:Personal data**
Title	Access rights management – timeliness of access rights
Requirement	Access rights must be kept up to date.
Overview	
Implementation example	8) There is a clear and effective way of immediately notifying the appropriate parties of changes in the personnel and an effective way of making the necessary changes. 9) Permissions and access rights are reviewed regularly.
Legislation	TihL 16
References	Julkri: HAL-14.1; Katakri: I-06
Other additional information	ISO/IEC 27002:2022 5.3, 5.15, 5.16, 5.17, 5.18, 8.2; PiTuKri IP-01
Identifier	**TEK-07.4, C:TL IV, I:, A:, DP:**
Title	Access rights management – segregation of security classified information
Requirement	The subcriterion specifies the requirement of the main criterion.
Overview	
Implementation example	1) The information of each security class is kept separate from public information and information of other security classes, or information at different levels is processed according to the highest classification level. 2) In servers, workstations and other storage media, classified information is stored in a format encrypted by a sufficiently secure method, if encryption is used to separate the information of different data owners who reserve the right of audit, or/and if storage media are, during their lifecycle, taken outside of the security area approved for their storage.
Legislation	TLA 11(1) item 1
References	Katakri: I-06
Other additional information	

Identifier	TEK-07.5, C:TL III, I:, A:, DP:
Title	Access rights management – TL III
Requirement	The subcriterion specifies the requirement of the main criterion.
Overview	The sufficient implementation of the separation of duties depends significantly on the use cases of the system in question. In most systems, sufficient separation of duties can be achieved by separating system maintenance roles (and persons) and log-monitoring roles (and persons) from each other. An often used control mechanism is also that critical maintenance and similar activities require the approval of two or more persons.
Implementation example	Tasks and responsibilities are differentiated, where possible, in order to reduce the risk of unauthorised or unintentional modification or misuse of the assets to be protected. If dangerous work combinations arise, there must be a control mechanism for them.
Legislation	TihL 13(1); TLA 11(1) item 3
References	Julkri: HAL-2.1; Katakri: I-06, I-12
Other additional information	

Identifier	TEK-08, C:Secret, I:Normal, A:, DP:Personal data
Title	Identification of actors in the computing environment
Requirement	Persons, devices and information systems using the information processing environment are identified with sufficient reliability.
Overview	

Implementation example	The requirement can be met by implementing the measures listed below: Identification of persons: 1) Unique user identifiers are used. 2) All users are identified and authenticated. 3) Identification and authentication use a technology that is known and considered secure, or are otherwise reliably organised. 4) Identification failure too many times in a row causes the ID to lock. 5) System and application maintenance credentials are personal. If this is not technically possible in all systems or applications, agreed and documented management practices for shared credentials are required, and they must enable the unique identification of the user. 6) Authentication is done using at least a password. If password authentication is used, a) users have been instructed on good security practice when selecting and using a password, b) the software that monitors the use of the password imposes certain minimum security requirements and forces a password change at appropriate intervals. The appropriate interval for changing the password must be proportionate to the organisation's operating environment and the classification of the classified information processed and stored in the device, taking into account the other security solutions in place. Identification of information systems: 7) Information systems exchanging information are identified by methods appropriate for the use case, such as passwords, keys (e.g., API key), tokens (e.g., oAuth) or similar methods. Identification is carried out through encrypted connections. Notes The reliable organisation of identification and authentication includes seeing to it that at least: i) the authentication method is protected against man-in-the-middle attacks; ii) when logging in, before authentication, no unnecessary information is disclosed; iii) authentication credentials are always in encrypted form if they are sent over a network; iv) the authentication method is protected against retransmission attacks; v) the authentication method is protected against brute force attacks. Considerations particularly in implementations that use cloud technology: - In cloud services that can be accessed over a public network, the method of use can be interpreted as remote use and thus, for example, the requirements for strong authentication based on several authentication factors must be taken into account. - In situations where federated identity management or/and identity and access management systems (the organisation's own or, for example, the cloud service provider's) are used in authentication for a cloud service, particular attention must be paid in assessing the reliability of the identification service and the transmission chain of attributes. Only identification services that offer an identity based on strong initial identification and whose attribute transmission chain can be implemented sufficiently securely up to the service that relies on identification are suitable for the processing of confidential information. - Because the protection of secret information is usually directly dependent on the reliability of the identification service, verifying the security of the identification service is almost without exception part of the assessment of cloud security. For example, it is typically justified to assess the cryptographic security of the attribute transmission in the same way as the key exchange of the encryption solution used to protect the information type in question. - Of the identity management models, organisation-centric identity management is usually better suited than user-centric management for the protection needs of secret information, which must also take into account the user's connection to a specific organisation and ensuring the reliability of the security implementation. - In assessing the part for which the customer is responsible, it is recommended that particular attention be paid to the fact that the corresponding requirements also apply to the customer and possible service providers associated with the customer's part.
Legislation	TihL 14; TLA 11(1) item 5
References	Julkri: HAL-19; Katakri: I-07
Other additional information	ISO/IEC 27002:2022 5.15, 5.17, 8.3, 8.5; NIST Special Publication 800-63B; PiTuKri IP-02, SA-01, SA-02 and SA-03.

Identifier	TEK-08.1, C:Secret, I:Normal, A:, DP:Personal data
Title	Identification of actors in the computing environment
Requirement	All users are identified and authenticated with unique personal credentials.
Overview	
Implementation example	
Legislation	TihL 13(1), 16; TLA 11(1) items 3 and 5
References	Katakri: I-07
Other additional information	PiTuKri IP-02
Identifier	**TEK-08.2, C:Secret, I:Normal, A:, DP:Personal data**
Title	Identification of actors in the computing environment
Requirement	Identification and authentication use a technology that is known and considered secure, or these must be otherwise reliably organised.
Overview	
Implementation example	
Legislation	TihL 13(1), 14, 16 TLA 11(1) items 3 and 5
References	Katakri: I-07
Other additional information	ISO/IEC 27002:2022 8.5; PiTuKri IP-02
Identifier	**TEK-08.3, C:Secret, I:Normal, A:, DP:Personal data**
Title	Identification of actors in the computing environment
Requirement	User credentials are locked when authentication fails too many times in succession.
Overview	
Implementation example	
Legislation	TihL 13(1); TLA 7
References	Katakri: I-07
Other additional information	ISO/IEC 27002:2022 8.5; PiTuKri IP-02

Identifier	TEK-08.4, C:TL IV, I:Critical, A:, DP:
Title	Identification of actors in the computing environment – TL IV
Requirement	The subcriterion specifies the requirement of the main criterion.
Overview	
Implementation example	Device identification: Only terminal equipment provided and managed by the organisation and approved for the security class in question are used to process classified information. The connection of any other devices to the processing environment of security classified information is unequivocally prohibited. The personnel are instructed and obliged to act in accordance with the instructions. Identification of information systems: Information systems exchanging information are identified by methods appropriate for the use case, such as passwords, keys (e.g., API key), tokens (e.g., oAuth) or similar methods. Identification is carried out through encrypted connections. Notes: In security classification level IV processing environments where a threat of effecting a denial-of-service attack (locking of credentials, e.g., in Internet-connected authentication services) is assessed as significant, locking of the credentials can be replaced with some mitigating process (e.g., procedures based on slow response, filtering or temporary locking). Security classification level IV processing environments do not usually require technical identification of terminal equipment if users are identified.
Legislation	TLA 11(1) item 5
References	Katakri: I-07
Other additional information	ISO/IEC 27002:2022 5.15, 5.17, 8.3, 8.5; NIST Special Publication 800-63B; PiTuKri IP-02

Identifier	TEK-08.5, C:TL III, I:Critical, A:, DP:
Title	Identification of actors in the computing environment – TL III
Requirement	The subcriterion specifies the requirement of the main criterion.
Overview	
Implementation example	Security classification levels III–II are also subject to the following measures: 1) Strong user authentication based on at least two factors is required. 2) Terminal devices are technically identified (device identification, 802.1X, or similar procedure) before allowing access to the network or service, unless connection to the network is limited by physical security methods (e.g., placing the server in a locked cabinet within a secured area). Notes In some cases, the methods used in security classification level III and II processing environments for strong user identification and terminal device identification can be implemented in such a way that it is only possible to access the information system from a strictly limited, physically protected area (usually a secured area, a locked hardware cabinet or similar), whose access control uses strong identification based on at least two factors. In this case, user identification in the information system can be arranged with username–password pairs. In situations where user identification relies on physical security procedures, the physical security procedures must also meet the requirements for traceability, especially with regard to log data and the storage periods of corresponding records.
Legislation	TLA 11(1) item 5
References	Katakri: I-07
Other additional information	

Identifier	TEK-09, C:Secret, I:Critical, A:, DP:Special category of personal data
Title	Physical security of information systems
Requirement	Data material must be processed and stored in premises that are sufficiently secure for implementing the requirements related to the confidentiality, integrity, and availability of data.
Overview	The requirements set for an administrative area, secured areas and, for example, storage units are described in the physical security section. Use outside the security area is remote access subject to the requirements of the corresponding section. In situations where information is temporarily processed in a space of a lower level than the class, attention must also be paid to, for example, activities during breaks in work (e.g., information to be taken into the safe of a secured area for the break), limiting visibility to the space (e.g., covering windows, if any) and limiting access to the processing space to approved persons only. It must be possible to ensure the integrity of the terminal device at a sufficient level so that the confidentiality of the information is not compromised as a result of the loss of the integrity of the device. The most typical way of ensuring the integrity of an information system is to protect it by means of physical access management procedures of security areas, including, for example, all physical servers, network devices, terminal devices and cabling related to the information system.
Implementation example	
Legislation	TihL 15(2); TLA 10
References	Julkri: FYY-7.1, HAL-19; Katakri: I-17
Other additional information	ISO/IEC 27002:2022 7.1, 7.3, 7.6, 7.8; Information Management Board: Recommendation on the handling of classified documents 2020:19, chapter 5; PiTuKri FT-02; CPNI: Physical Security Advice
Identifier	**TEK-10, C:Secret, I:Important, A:, DP:Special category of personal data**
Title	System hardening
Requirement	A procedure is in place to systematically install systems in such a way that the end result is a hardened installation.

Overview

Systems often have many features that are usually on by default and easy to enable. The default settings of the features are often not safe enough. If unnecessary features are not disabled, these are also available to a malicious actor. If the risk-prone default settings of essential services are not changed, these are also available to a malicious actor. For example, systems often use predefined default maintenance passwords, preinstalled unnecessary software and unnecessary user accounts.

In general, hardening refers to changing the system settings to reduce the system's attack surface. In order to mitigate risks, the systems must generally use only features, equipment and services that are essential to the requirements for use, and the visibility of services, for example, must be limited to the minimum possible. Similarly, for example, automated processes must only be provided with the information, rights or authorisations necessary to carry out their tasks, in order to limit possible damage caused by accidents, errors or unauthorised use of system resources. Any unsafe default system settings and, for example, unnecessary default user accounts must be changed or deleted.

Systems refer to active devices, servers, workstations, mobile devices, printers, peripherals and other devices that are considered an information system. Sufficient hardening of servers, workstations and similar can be achieved, for example, adapting DISA STIG, CIS or similar levels. If network printers, voice systems or similar are used to process classified information, the aforementioned principles should also apply to these systems. Configuration management tools can often be used for hardening and maintaining hardened installations.

Essential for hardening
1) Default passwords have been changed to complex passwords in accordance with the organisation's password policy. Passwords are stored so that passwords are protected and available.
2) Extraneous services, applications, connections (including at the BIOS level) and devices have been removed.
3) Users, interfaces and devices are identified (see I-07).
4) The necessary services are accessible only for the necessary networks, devices and user accounts.
5) Software (e.g., firmware, applications) is kept up to date (see I-19).
6) The site's connections, including management connections, are limited, hardened, user-identified, and time-limited (session timeout).
7) The applications, interfaces and similar in use have been hardened and limited, and features have been set in accordance with the principle of least privilege.
8) Software, such as operating systems, applications and firmware, is set up to collect the necessary log data to detect misconduct (see I-10).
9) Booting the information system from an unknown (non-primary) device is prevented.

Substitute methods
For example, if the management of a network device is not technically possible with a user ID that uniquely identifies a user, the user's unique identification can be arranged by operating rules, for example, so that access to the password requires the participation of two persons. If the environment is larger, it is recommended to use duplicate AAA servers (especially TACACS+, RADIUS or Kerberos) to organise authentication.

Considerations particularly in implementations that use cloud technology:
In assessing the part for which the customer is responsible, it is recommended that particular attention be paid to the fact that the corresponding requirements also apply to the customer and possible service providers associated with the customer's part.

Implementation example	1) The objects to be hardened have been identified. 2) Implementation of the hardening has been specified. 3) Objects are hardened according to specifications. 4) The activeness of the hardening is verified regularly, especially after updates, throughout the lifecycle of the information system. Special considerations: a) Hardening is targeted at all devices in the computing environment, including active network devices, servers, workstations, mobile devices, printers, peripherals and other devices that are considered an information system. b) In order to limit the attack surface, the equipment has only the necessary services, interfaces, connections and routes on, and these operate on the principle of least privilege. c) The firmware (firmware, BIOS, and similar), operating system, applications and other similar components of the device are hardened at least in accordance with the manufacturer's hardening recommendation and/or using a commonly known hardening guide. In addition, hardening is tailored for each system based on its intended use and risks. If no hardening guide exists for the component used, the guide for a corresponding product is used.
Legislation	TihL 13(1) and (4); TLA 11(1) item 6
References	Katakri: I-08
Other additional information	ISO/IEC 27002:2022 8.27; The United States Government Configuration Baseline (USGCB); DISA Security Technical Implementation Guides (STIGs); NIST - National Checklist Program Repository; Microsoft DSC Environment Analyzer; Microsoft Baseline Management; CIS benchmarks; PiTuKri JT-02
Identifier	**TEK-10.1, C:Secret, I:Important, A:, DP:Special category of personal data**
Title	System hardening – minimising the number of services used
Requirement	Only the functions, equipment and services that are essential for fulfilling the requirements and data processing have been enabled.
Overview	Hardened installation includes only the components, services and user and process rights that are necessary for meeting operational requirements and ensuring safety.
Implementation example	
Legislation	TihL 13(1); TLA 11(1) item 6
References	Katakri: I-08
Other additional information	

Identifier	TEK-10.2, C:Secret, I:Important, A:, DP:Special category of personal data
Title	System hardening – ensuring hardening throughout the lifecycle
Requirement	The validity and effectiveness of the hardening is ensured throughout the lifecycle of the information system.
Overview	
Implementation example	
Legislation	TihL 13(1) and (4); TLA 11(1) item 6
References	Katakri: I-08
Other additional information	

Identifier	TEK-10.3, C:TL III, I:Critical, A:, DP:
Title	System hardening – classified environments
Requirement	The subcriterion specifies the requirement of the main criterion.
Overview	In particular, in environments of the highest security classes, it is often justified to implement the prevention of the use of unwanted components (e.g., wireless network cards, cameras, microphones) by physically removing them from the device. In situations where a component cannot be physically removed, protection can in some cases include, for example, taping cameras, decommissioning the hardware by software, and the user setting, operating system and firmware levels. In some operating systems, protection can also be supplemented by removing kernel modules related to the use of the device in question. In the processing environments of security classes III–II, possible levels contained in the hardening instructions and the use of several different hardening guides must be taken into account, such as the manufacturer's specific instructions, CIS Benchmark and DISA Stig, to ensure the coverage of hardening.
Implementation example	In the processing environments of security classes III–II, the requirement can be implemented by using several hardening instructions for hardening in addition to items 1–4 and increasing the strictness of the hardening instructions.
Legislation	TihL 13(1) and (4); TLA 11(1) item 6
References	Katakri: I-08
Other additional information	

Identifier	TEK-11, C:Secret, I:Normal, A:Normal, DP:Special category of personal data
Title	Protection from malware
Requirement	Reliable methods for preventing, blocking, detecting, resisting and remedying malware threats are implemented in the data processing environment.
Overview	Protection against malware risks can be provided by, for example, hardening of systems, restriction of user rights, maintaining systems at the level of security updates, the ability to detect deviations, ensuring personnel safety awareness and also using anti-malware software. Risks can also be mitigated by separating high-risk environments from production environments and, for example, by limiting the use of removable media (e.g., USB memory). Prevention software may be left uninstalled in environments where access of malicious software is otherwise blocked (e.g., systems that do not have any data import/export interfaces, or where well-specified interfaces provide reliable validation/sanitation of the data being transferred).
Implementation example	The requirement can be met by implementing the measures listed below: 1) The system access rights are limited according to the principle of least privilege. 2) The systems are kept up to date with security updates. 3) The systems are hardened so that only essential functionalities and software components are used. 4) Personnel security awareness is ensured. Users have been instructed on malware threats and how to act in accordance with the organisation's information security principles. 5) Anti-malware software is installed on all systems that are vulnerable to malware infection. These typically include public network gateways (e.g., e-mail and web traffic) and terminal devices connected to external interfaces (other networks, USB media, etc.). 6) The protection software is operational and running. 7) The protection software produces log data and alarms from its observations. 8) Malware signatures (and similar) are updated regularly. 9) Malware observations and alarms are monitored regularly and reacted to.
Legislation	TihL 13(1), 15(1); TLA 11(1) items 2 and 3
References	Katakri: I-09
Other additional information	ISO/IEC 27002:2022 8.7; PiTuKri JT-04

Identifier	TEK-11.1, C:TL IV, I:, A:, DP:
Title	Protection against malware – TL IV
Requirement	The subcriterion specifies the requirement of the main criterion.
Overview	
Implementation example	For processing environments of security classification level IV, the requirement can be met by additionally implementing the following measures: 1) Systems have been identified where additional protection can be obtained with anti-malware software.
Legislation	TLA 11(1) item 2
References	Katakri: I-09
Other additional information	ISO/IEC 27002:2022 8.7; PiTuKri JT-04

Identifier	TEK-11.2, C:TL III, I:, A:, DP:
Title	Protection against malware – TL III
Requirement	The subcriterion specifies the requirement of the main criterion.
Overview	Environments isolated from public networks On systems that are not connected to a public network, the update of malware signatures can be organised, for example, by using a managed, secure update retrieval server whose signature database is manually updated from a separate Internet-connected system (e.g., 1–3 times a week) or importing the signatures through an approved gateway solution. In the risk assessment, the assessment of the adequacy of the updating frequency of signatures should be proportionate to the characteristics of the environment in question, especially taking into account the frequency of other data transfers of the environment. Note: There should be a procedure for ensuring the integrity of updates (source, checksums, signatures etc.). The case-by-case conditions for using USB ports and similar interfaces may include, for example, that only separately configured, trusted flash drives (and similar) that are not connected to any other system can be connected to the system. Case-by-case conditions may include, for example, an arrangement whereby only storage media distributed by the organisation's information management (or equivalent) can be connected to the organisation's systems, and that the connection of all other storage media is prohibited and/or technically blocked. In situations where there is a need to import data from untrusted systems using a storage medium, case-by-case conditions often also include specifications of the methods used to reduce the risk from this arrangement. For example, the method may be to connect storage media from an untrusted source to an isolated inspection system to which the transferred data is transferred and from which the information is further taken to the trusted system using a separate storage medium.
Implementation example	The requirement for security classification levels III–II processing environments can be met by also implementing the measures listed below: All data import and export use cases have been identified. Secure operating methods have been specified, instructed and supervised. Secure procedures include an assessment of the need for using USB ports and similar interfaces in systems. a) In situations where there is no sustainable basis that withstands critical consideration for the use of interfaces, the interfaces are disabled. b) In situations where there is a sustainable basis that withstands critical consideration for the use of interfaces, it is assessed on a case-by-case basis what prerequisites and terms apply for connecting to devices and tools (e.g., USB storage media) to the system. In situations where there is a need to import data from untrusted systems using a storage medium, the inspection of at least the memory area is usually taken into account in security classification level III.
Legislation	TLA 11(1) item 2
References	Katakri: I-09
Other additional information	

Identifier	TEK-11.3, C:TL II, I:, A:, DP:
Title	Protection against malware – TL II
Requirement	The subcriterion specifies the requirement of the main criterion.
Overview	
Implementation example	In addition, in situations where there is a need to import data from untrusted systems using a storage medium, the threats of controller-level customisations of the storage medium are usually taken into account from security classification level II onward.
Legislation	TLA 11(1) items 2 and 5
References	Katakri: I-09
Other additional information	

Identifier	TEK-12, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Traceability of security-related events
Requirement	In order to detect unauthorised modification of data and other unauthorised or inappropriate processing of information, reliable methods are implemented in the information processing environment to ensure the traceability of security-related events.

Overview

Traceability refers to logging events in the system environment in such a way that in the event of a deviation, it is possible to determine what actions have been taken in the environment, by whom and what impacts the actions have had. Key recordings typically include not only login information but also the log information of essential network devices and servers. For example, log data from workstations and similar is also very often included here.

It can often be used in implementing the coverage requirement that it is ensured that at least workstations, servers, network devices (especially firewalls, including workstation software firewalls) and similar logs are enabled. It should also be possible to use network device logs afterwards to determine what management measures have been taken, when and by whom. Event logs should be collected on the operation of the system, user activities, information security events and exceptions.

One of the recommended ways to secure logs is to direct the essential log data to a centralised, highly secure log server that is backed up daily in a separate environment of at least the same security class. An effort should be made to collect and store log data so that deleting or changing log data can also be detected in situations where, for example, the network connection between the log source and the log collector is not available. Correspondingly, for example, log collection from workstations permanently disconnected from the network and backing up the collected log data require a regular process. It is recommended for both the legal protection of administrators and the investigation of suspected data breaches that tasks be separated so that the maintenance of log data is separated from other maintenance personnel. In addition, in the implementation of traceability, situations must also be taken into account in which a person logged in to the system has the opportunity to perform functions using another account (user impersonation). The functionality of the log data storage and monitoring software must also be monitored, and any disruptions must be detected with a short time delay (e.g., within one day after the log source has stopped delivering logs).

The needs of the use case in question must be taken into account in the retention periods of log data. For example, it may be justified to require different retention periods for the processing and disclosure logs of some data than for log data collected for the investigation of deviations. For example, in official activities, criminal statute periods can typically lead to a minimum of five years of storage time. A frequently used practice is that historical logs of 6 months are available in real time, and longer-term logs are available, if necessary, with a delay of a few working days. Various use cases of log data are also discussed in the recommendation of the Information Management Board (2020:21, chapter 7).

The implementation often also requires taking account of the fact that the storage space and time of logs are increased to be sufficient. Recommendation: an amount assessed as sufficient in the environment will be reserved for logs. The determination of sufficient time may, for example, be made by estimating a sufficient space for the required retention period on the basis of one month's log accumulation. Note: a generous amount of "buffer" should be reserved, because abnormal situations and certain types of attacks also significantly increase log volumes.

Implementation example	The requirement can be met by implementing the measures listed below: 1) A written policy/guide for log collection and disclosure, alerting and monitoring has been effectively implemented, and it has been formulated taking into account the requirements of the operations. 2) Records are sufficiently comprehensive for ex-post verification of data breaches or attempts. 3) Key records are retained for at least 6 months, unless the legislation or agreements require a longer retention period. Processing logs and records that are subject to, for example, criminal statute periods for official activities are kept for at least 5 years. 4) Log data and related recording services are protected from unauthorised access (access rights management, logical access control).
Legislation	TihL 17, 15; TLA 7, 14
References	Julkri: HAL-7.1; Katakri: I-10
Other additional information	The United States Government Configuration Baseline (USGCB); ISO/IEC 27002:2022 5.33, 8.15, 8.17; Information Management Board: Collection of recommendations on the application of certain information security regulations (2020:21, chapter 7); PiTuKri JT-01
Identifier	**TEK-12.1, C:Public, I:Minor, A:Minor, DP:Personal data**
Title	Traceability of security-related events – data disclosure
Requirement	The necessary log data are collected on the use of information systems and disclosures from them, if the use of the information system requires identification or other logging in.
Overview	The purpose of the log data is to monitor the use and disclosure of data in information systems and to investigate technical errors in the information system.
Implementation example	
Legislation	TihL 17, 15; TLA 7, 14
References	Julkri: HAL-07.1, TSU-18; Katakri: I-10
Other additional information	
Identifier	**TEK-12.2, C:TL III, I:, A:, DP:**
Title	Traceability of security-related events – TL III
Requirement	The processing of security classification levels II–III information must be registered in an electronic log, information system, case register or the information itself (e.g., as part of a document).
Overview	A Ministry of Finance recommendation on the storage of log data related to the processing of classified documents has been issued, VM 2021:5: "Recommendation on the handling of classified documents."

Implementation example	The requirement for security classification levels III–II processing environments can be met by implementing items 1–4 and additionally the measures listed below: 5) Key records are retained for at least 5 years, unless the legislation or agreements require a longer retention period. Records that, for example, have very minor significance for the investigation of deviations or in the criminal-law aspect of official activities can be kept for a shorter period, such as 2–5 years. 6) Log data are backed up regularly. 7) The clocks of essential information processing systems in the same security area are synchronised with an agreed time source. 8) There is a method for ensuring log integrity (non-alteration). 9) The use and processing of the generated log data are recorded.
Legislation	TihL 17, 15; TLA 7, 14
References	Katakri: I-10
Other additional information	Ministry of Finance: Recommendation on the handling of classified documents (2021:5) 7.9.
Identifier	**TEK-12.3, C:TL I, I:, A:, DP:**
Title	Traceability of security-related events – TL I
Requirement	The subcriterion specifies the requirement of the main criterion.
Overview	
Implementation example	In the processing of security classification level I information, storage periods longer than with security classification level II are recommended on a risk basis (for example, at least 10 years). Security classification level I information-processing environments are typically limited, for example consisting of terminal devices permanently disconnected from all networks. On the other hand, the retention of a 10-year log accumulation, for example, is challenging to implement credibly on terminal equipment only, whereby the collection of logs of such terminal devices and the backups of the collected log data usually require a planned, regular process. The practical implementation method may include, for example, the regular collection of log data on removable media, which are processed and stored during their lifecycle as security classification level I information. In addition, it must be noted that if the access management of the information system or, for example, the traceability of operations is based on physical security procedures, it may also be justified to store and manage the records resulting from these using security classification level I procedures.
Legislation	TihL 17, 15; TLA 7, 14
References	Katakri: I-10
Other additional information	

Identifier	TEK-13, C:Secret, I:Important, A:Important, DP:Special category of personal data
Title	Ability to detect incidents and recovery from them
Requirement	Reliable methods are implemented in the information processing environment that aim at detecting an attack on the information processing environment, limiting the impact of the attack to a minimum part of the information or resources in the information processing environment, and preventing other damage, and restoring the secured state of the information processing environment without delay.
Overview	A technical incident detection capability is usually based on three sources: 1) Events manifested in network traffic, 2) records (logs) collected and 3) events manifested in the targets (hosts). Sufficient technical observation capability can usually be achieved by combining the above-mentioned observation sources. The more accurately the information processing environment and its normal operation are known, the more possible it also is to observe events that differ from normal operation. Observation of events that differ from normal operation also supports detection of attacks for which indicators of compromise (IoC) are not available. The normal operation of the information processing environment should be known throughout the lifecycle, from the beginning to decommissioning. Change management (TEK-17) also supports the ability to detect deviations, including by regularly reviewing hardware and software configuration changes. There are several suitable implementation possibilities for monitoring and limiting the impact of a detected attack, ranging from monitoring at the level of key network nodes to workstation/server-specific sensors, and combinations of these. Regardless of the network devices and suppliers used, a practical implementation of network-level observation capability typically requires knowledge of the normal state of network traffic. For security classification level IV processing environments, network-traffic-level detection capability should cover, in particular, the external border of the network/target, and, from class III onwards, the gateway solution of the external border and the traffic within the network/target. In practice, detection of an attack/abuse attempt requires the use of automated detection and alarm systems in most environments. In some situations, manual processing of log data is also possible and even necessary if, for example, no deviation has been detected by automatic means and the deviation situation requires more detailed investigation. It should also be remembered that only information necessary for information security measures may be collected in logs, and when measures are taken, the freedom of expression or the protection of confidential messages or privacy may not be restricted. In general, it should be noted that the observation capability requires knowledge of the characteristics of each information processing environment and, among other things, the specification and tailoring of critical targets and events to be monitored in accordance with the information processing environment in question, as well as continuous maintenance of the observation capability. Restoring the information environment to a secured state within a reasonable time usually requires planned, described, trained and practised processes and technical methods. The role of all personnel must also be taken into account when developing and maintaining the ability to observe deviations. For example, observations reported by end users can produce valuable information for detecting attacks or attempted attacks.
Implementation example	The normal state of network traffic (traffic volumes, protocols and connections) is known. There is a procedure for attempting to detect events that differ from the normal state of network traffic (for example, abnormal connections or attempts to make them).
Legislation	TihL 13(1), 15(1), 17; TLA 7, 11(1) item 2

References	Julkri: TEK-17; Katakri: I-11, T-07, T-12
Other additional information	ISO/IEC 27002:2022 5.25, 5.26, 8.15, 8.16; PiTuKri TT-02, JT-01, TJ-05
Identifier	**TEK-13.1, C:Secret, I:Important, A:, DP:Special category of personal data**
Title	Ability to detect incidents and recovery from them – observation of incidents using log data
Requirement	The subcriterion specifies the requirement of the main criterion.
Overview	
Implementation example	It is recommended to implement a procedure for detecting incidents using collected records and situational information (e.g., changes in logs) (in particular, it must be possible to detect an unauthorised attempt to access an information system).
Legislation	TihL 13(1), 15(1), 17; TLA 7, 11(1) item 2
References	Katakri: I-11
Other additional information	ISO/IEC 27002:2022 8.15, 8.16; PiTuKri JT-01, TJ-05
Identifier	**TEK-13.2, C:TL IV, I:Important, A:, DP:**
Title	Ability to detect incidents and recovery from them – TL IV
Requirement	The subcriterion specifies the requirement of the main criterion.
Overview	
Implementation example	1) A procedure is in place for detecting incidents using collected records and situational information (e.g., changes in logs) (in particular, it must be possible to detect an unauthorised attempt to access an information system). 2) A procedure is in place for detecting deviations in objects in the computing environment (hosts, such as workstations and servers). 3) A procedure is in place for recovering from observed deviations.
Legislation	TihL 13(1), 15(1), 17; TLA 7, 11(1) item 2
References	Katakri: I-11
Other additional information	ISO/IEC 27002:2022 8.15, 8.16; PiTuKri JT-01, TJ-05

Identifier	TEK-13.3, C:TL I, I:, A:, DP:
Title	Ability to detect incidents and recovery from them – TL I
Requirement	The activities of users and administrators are monitored to detect exceptional activities.
Overview	
Implementation example	In the processing of security classification level I data, enhanced incident-detection capabilities are recommended, with emphasis on monitoring the activities of users and administrators of the information processing environment.
Legislation	TihL 13(1), 15(1), 17; TLA 7, 11(1) item 2
References	Katakri: I-11
Other additional information	ISO/IEC 27002:2022 8.16; PiTuKri JT-01, TJ-05

Identifier	TEK-14, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Ensuring software security
Requirement	Applications and application programming interfaces (APIs) are designed, developed, tested and deployed in accordance with the industry's best security practices. Applications and interfaces must be able to withstand common attack methods available for them without compromising the confidentiality, integrity or availability of the information processed.

Overview

Software and its uses in different information processing environments vary greatly. Similarly, the needs for the secure implementation and deployment of software differ significantly in different information processing environments and uses. For example, the security needs of office software used on a physically isolated workstation differ from the needs of a case management system accessible by multiple users.

The risks and security needs associated with software can be assessed, for example, by means of the purpose of the software and its role, the attack surface, and the nature and security classification of the data to be processed. If the intended use and role of the software are to act as an access-limiting mechanism in the processing of security classified information, it should be possible to ensure the reliable operation of the software. The attack surface of the software can have a significant impact on the security needs on the software. Typically, security classification level IV services, for example, can be accessed more extensively and by a more heterogeneous group than, for example, security classification levels III–II services. The security requirements set for software may in some respects be more stringent in security classification level IV systems than, for example, in strictly insulated and narrow, higher-security systems where each user has a need to know all the information processed in the system. The security class of the information being processed, and the expected interest of external actors may affect the risk and security needs of the software. For example, politically high-interest information, or information classified with high security, can have a significant impact on software risks and security needs, including in preparing for the most advanced attacks.

When commissioning standard software or ordering customised or self-produced software, attention must be paid to the secure development of the software and the peripheral components used by the software already in the design phase. Attention should also be paid to other aspects of the entire software lifecycle. These factors include requirements during deployment, contract technology, update practices and change management. Software that significantly affects the protection of security classified information must be implemented based on secure software-development practices, covering both the quality of the software code and the software development processes.

The requirements derived from legislation must be taken into account in the requirement specification of the software already at the procurement stage. In particular, entities related to encryption (I-12), management interfaces (I-04), user management and identification (I-06, I-07), hardening (I-08) and traceability (logging, I-10) must also be taken into account in software implementation. Software implementations must not jeopardise the fulfilment of the need to know or provide external actors with access to the information processing environment or its sub-entities to be protected. In the lifecycle stages, responsibility for producing software patches must be ensured, and the security of the software must also be maintained against new attack techniques. An effort can also be made to ensure that standard software is of sufficient quality in accordance with similar principles.

Sometimes there may be a need to use services with low or even non-existent visibility of the program code and its development practices. Evidence of the reliability of such software can be sought, for example, by examining update frequencies, documentation and possible other visibility, such as existing test reports. In such situations, substitute protection can be used in addition to secure configuration. With certain limitations, secure configuration and substitute protection can rely on, for example, enhanced detection capability, hardening, code run-time restrictions (e.g. AppLocker, SELinux, AppArmor), application firewalls (WAF) and logical isolating of the entire software, for example using virtualisation.

More detailed industry instructions and standards must be used to ensure the security of software. These include the VAHTI Application development information security guide (VAHTI 1/2013), OWASP Application Security Verification Standard (ASVS) and the Cyber Security Centre's guide "Secure development – towards approval".

Implementation example	1) The intended purposes of the software (applications, services, systems) and the roles that may implement software security have been identified. 2) The security needs of the software (applications, services, systems) have been assessed, taking into account in particular the intended use of the software and its role, the attack surface, and the nature and security class of the information to be processed. 3) The dependencies and interfaces of the software (applications, services, systems) have been identified. Dependencies and interfaces are subject to the requirements corresponding to the software, taking into account, for example, the libraries used, interfaces (APIs) and hardware requirements. The requirements take into account both server- and client-side aspects. 4) Critical software (applications, services, systems) is implemented or the implementation is audited, as far as possible, against a reliable standard or/and using a secure programming guide. 5) It has been verified that the maintenance, development and change management of the software (applications, services, systems) meets the needs throughout the lifecycle. 6) It has been verified that the software (applications, services, systems) meets regulatory requirements. Special attention must be paid to encryption, management interface, user management and identification, hardening and traceability sections.
Legislation	TihL 13(1), 15 (1); TLA 11(1) items 2, 3, 4, 5 and 6
References	Julkri: HAL-16; Katakri: I-13
Other additional information	OWASP Application Security Verification Standard (ASVS); CWE TOP 25 Most Dangerous Software Errors; The Building Security In Maturity Model; Software Assurance Maturity Model; ISO/IEC 27002:2022 5.8, 8.26, 8.27, 8.28, 8.29; Traficom: Secure development – towards approval; PiTuKri MH-02
Identifier	**TEK-15, C:TL III, I:, A:, DP:**
Title	Electromagnetic emanations (TEMPEST) and electronic intelligence
Requirement	Security measures are implemented in an information processing environment related to classified information using sufficiently secure methods so that the information is not compromised by unintended electromagnetic leaks (TEMPEST security measures). These security measures must be proportionate to the risk and security class of data exploitation. When processing security classification level III or II information electronically, it must be ensured that risks associated with electronic intelligence are adequately mitigated.
Overview	In processing environments of security classification levels III–II, protection against electromagnetic emanations exceeding the limit values is carried out with procedures that are sufficiently secure for the security class in question. With regard to security classification level III information, there is greater room to adopt compensatory procedures to achieve adequate protection.
Implementation example	1) Risks associated with electromagnetic emanations have been identified and assessed. 2) Security measures or compensatory procedures are dimensioned for risks, the security class of the information and acceptable residual risk level.
Legislation	TLA 11(2)
References	Julkri: FYY-5.6; Katakri: I-14
Other additional information	Traficom: Principles for preventing the information security risks of electromagnetic emanations; ISO/IEC 27002:2022 7.12

Identifier	TEK-15.1, C:TL II, I:, A:, DP:
Title	Electromagnetic emanations (TEMPEST) and electronic intelligence – TL II
Requirement	The subcriterion specifies the requirement of the main criterion.
Overview	
Implementation example	Security measures have been implemented, dimensioned for the risks and information security class. The adequacy of the target's countermeasures to electromagnetic emanations can be verified by zone measurement or protected-space measurement.
Legislation	TLA 11(2)
References	Katakri: I-14
Other additional information	

Identifier	TEK-15.2, C:TL I, I:, A:, DP:
Title	Electromagnetic emanations (TEMPEST) and electronic intelligence – TL I
Requirement	The subcriterion specifies the requirement of the main criterion.
Overview	
Implementation example	When protecting security classification level I information, risks different from security classification level II information must be taken into account and made proportionate to the security measures to be taken. Electromagnetic emanations and the principles of protecting against them are described in more detail in the National Cyber Security Centre's guide on protecting against electromagnetic emanations.
Legislation	TLA 11(2)
References	Katakri: I-14
Other additional information	

Identifier	TEK-16, C:Secret, I:Important, A:, DP:Special category of personal data
Title	Encryption of information
Requirement	When secret information is transferred over a public network, the information is encrypted with an encryption solution that has no known vulnerabilities and, according to the manufacturer's information, supports modern encryption strengths and settings. In addition, the information transfer must be arranged in such a way that the recipient is verified or identified in a sufficiently secure manner before the recipient can process the transferred, non-classified secret data.

Overview	There are several risks associated with the electronic transmission of secret information. Reducing the risks to an acceptable level requires consideration of factors related to both personnel and the technical implementation. In situations where there is a need to transmit secret information between, for example, two organisations over a public network, secure transmission requires secure encryption solutions and key management practices as well as personnel trained in their use. In situations where the use of an encryption solution requires action by the personnel (for example, the transmission of a secret document to another organisation as an encrypted attachment to an e-mail), particular attention must be paid to the real-life adoption of the secure use of the encryption solution by the personnel. A technically secure encryption solution does not provide sufficient protection for secret information, for example in situations where key management practices are inadequate or where the personnel do not use the encryption solution in accordance with the related principles of secure use. The sufficiently reliable verification of the recipient depends significantly on the encryption solution used. For example, the use policies of encryption solutions approved by the National Cyber Security Centre for the protection of security classified information often also address user identification when the encryption solution in question is used, for example, for communications to a person in another organisation. On the other hand, in a number of encryption solutions, counterparty authentication relies on key management reliability (for example, encryption between sites in an organisation or between networks in two organisations (LAN-2-LAN), or file encryption based on a shared secret). When selecting the encryption strengths and settings to be used, the strengths and settings of security classification level IV can be used as a rule. The Internet, as well as MPLS networks offered by carriers and, for example, so-called dark fibre, are interpreted as public networks. This includes telephony, fax, e-mail, instant messengers and other similar communication methods over a network.
Implementation example	1) When transferring secret information over a network outside the physically protected areas approved for the information in question, the role of encryption as an essential security measure must be taken into account. a) The personnel have tools and methods in place to protect unclassified secret information with an encryption solution that does not contain known vulnerabilities and that, according to the manufacturer's information, supports modern encryption strengths and settings. b) The personnel's competence in the secure use of the encryption solution has been ensured (e.g., instructions, training and supervision). 2) Secret keys are only used by authorised users and processes. Encryption key management processes and practices are documented and appropriately implemented. The processes require at least a) cryptographically strong keys, b) secure key distribution, c) secure key storage, d) regular key replacement, e) replacement of old or exposed keys, f) prevention of unauthorised key replacement. 3) The security of the encryption solution's supply chain has been verified at an adequate level. In particular, the supply chain of the encryption solution from a reliable manufacturer to the target's information processing environment has been secured.
Legislation	TihL 13(1), 14; TLA 11(1) item 7, 12
References	Julkri: TEK-01; Katakri: I-01, I-12, I-15, I-18
Other additional information	Traficom: Cryptography solutions approved by Traficom's NCSA-FI; Traficom: Cryptographic requirements for confidentiality – national protection levels; Traficom: Secure development – towards approval; Information Management Board: Recommendation on the handling of classified documents (2020:19, chapter 7); ISO/IEC 27002:2022 5.14, 5.31, 8.24; PiTuKri JT-05, SA-01, SA-02, SA-03

Identifier	TEK-16.1, C:Secret, I:Important, A:, DP:Special category of personal data
Title	Encryption of information – encryption within a security area
Requirement	When secret information is transferred within an authority's internal network, lower-level encryption or unencrypted communication can be used based on the results of the risk management process.
Overview	
Implementation example	
Legislation	TihL 13(1), 14; TLA 11(1) item 7, 12
References	Julkri: FYY-7.1; Katakri: I-15
Other additional information	ISO/IEC 27002:2022 5.14, 8.24; PiTuKri JT-05, SA-02, SA-03

Identifier	TEK-16.2, C:TL IV, I:, A:, DP:
Title	Encryption of information – transfer of security classified information outside security areas
Requirement	When classified information is transferred outside approved physically protected security areas, the information/communication is encrypted with a sufficiently secure method. In addition, the information transfer must be arranged in such a way that the recipient is verified or identified in a sufficiently secure manner before the recipient can process the transferred, classified data.
Overview	In particular, the need to use encryption solutions with reliable evidence of sufficient security is emphasised in the protection of security classified information. Several factors are taken into account in the assessment of encryption solutions. In addition to ensuring the correct functioning of the encryption strength and encryption solution, the threat level of the encryption solution's operating environment is also taken into account. For example, when communicating over the Internet, the threat level differs significantly from a situation where encryption is used for communication within a controlled, physically protected area (for example, traffic between two secured areas via an administrative area). Other factors to be taken into account in the assessment of encryption solutions include the requirements of the use case in question for the secrecy period and cryptographic integrity of the data. Purely software-based encryption solutions are typically acceptable under security classification level IV and, in some situations, also under special conditions for security classification level III. Security classification level II and, most often, security classification level III typically require more of the platform reliability. The approval process for encryption solutions is described in more detail in the National Cyber Security Centre's guide on encryption product assessments and approvals. The minimum requirements for encryption solutions are also discussed in the encryption strength description maintained by the National Cyber Security Centre and in the guide on secure product development.

Implementation example	1) The organisation has identified use cases where encryption solutions are needed to protect classified information. The identified use cases cover all situations where the protection of security classified information relies entirely or partially on an encryption solution. In particular, traffic over a public or lower-security-class network, communication of information to another organisation, and terminal equipment taken outside security areas have been taken into account. 2) a) Encryption solutions approved by the authorized authority, used in accordance with the use policy and regulations specified at the time of approval, or b) case-by-case approvals and user policies/regulations granted by the authorized authority for encryption solutions that did not already have a valid approval, have been acquired for the security class in question. 3) When transferring classified information over a network outside the physically protected security areas approved for the security class in question, the role of encryption as an essential security measure must be taken into account. a) The personnel have tools and procedures in place to protect classified information with an encryption solution approved by the authorized authority. b) The personnel's competence in the secure use of a sufficiently secure encryption solution has been ensured (e.g., instructions, training and supervision).
Legislation	TihL 14; TLA 11(1) item 7, 12
References	Julkri: FYY-7.1; Katakri: I-01, I-12, I-15, I-18, F-08.1
Other additional information	ISO/IEC 27002:2022 5.14, 8.24; PiTuKri JT-05, SA-02, SA-03
Identifier	**TEK-16.3, C:TL IV, I:, A:, DP:**
Title	Encryption of information – transfer of security classified information within security areas
Requirement	When transmitting classified information within physically protected security areas, lower-level encryption or unencrypted transfer can be used based on the results of the risk management process and on the separate approval of the competent authority.
Overview	
Implementation example	2) In situations where classified information is transferred within physically protected security areas: a) the security class's transmission channel in question is physically protected (for example, cabling that runs in its entirety within a narrow, for example covering only one room, physically protected security area approved for the storage of information of that security class), or b) the data is protected by sufficiently secure lower-level encryption (e.g. HTTPS in the internal traffic of the security class's network in question).
Legislation	TihL 14; TLA 11(1) item 7, 12
References	Julkri: FYY-7.1; Katakri: I-15
Other additional information	

Identifier	TEK-16.4, C:TL III, I:, A:, DP:
Title	Encryption of information – TL III
Requirement	Storage of only security classification level III electronic information in a terminal device of that security class outside the secured area is possible, provided that a) the information is protected by an encryption solution that is sufficiently secure for the security class in question, and b) the information security of the terminal device, in particular the confidentiality and integrity required for the security class in question, has been ensured by adequate procedures.
Overview	
Implementation example	
Legislation	TLA 10
References	Julkri: FYY-7.1; Katakri: F-04, I-12, I-17, I-18
Other additional information	
Identifier	**TEK-16.5, C:TL I, I:, A:, DP:**
Title	Encryption of information – TL I
Requirement	The subcriterion specifies the requirement of the main criterion.
Overview	In other situations where encryption solutions are used to protect security classification level I data, such as the encryption of hard drives of terminal equipment or the segregation of information of different information owners, it is recommended that account be taken of the highly limited availability of encryption solutions that are sufficiently reliable and approved for protecting security classification level I information. In such situations, encryption solutions are in principle only in a role supportive of other security, especially physical access management.
Implementation example	Particular attention should be paid to the very limited availability of reliable encryption solutions approved for protecting security classification level I information. This typically involves transferring security classification level I information by means of a courier procedure approved for security classification level I in situations where there is a need to transfer security classification level I information between physical, secured areas.
Legislation	TihL 14; TLA 11(1) item 7, 12
References	Katakri: I-15
Other additional information	
Identifier	**TEK-17, C:Public, I:Minor, A:Minor, DP:Personal data**
Title	Change management procedures
Requirement	A change management procedure that takes security into account is in place for changes to the information processing environment.

Overview	Reliable management of information security and changes of the information processing environment requires that the technical structure of the environment and, for example, all hardware and software included in it are known. Changes in the settings and operation of information systems must be monitored, and any observed changes must lead to verification of their correctness. With up-to-date accounting, changes can be allocated accurately throughout the lifecycle, the impacts of the changes can be predicted more easily and it is possible to examine the security of the environment. For example, network diagrams, lists of hardware and software components, and configuration databases can be used in accounting. It must be possible to verify the information security of the information processing environment throughout the entire lifecycle. This requires continuous monitoring of change needs and regular changes. Change needs can result, for example, from the end of the lifecycle of systems in the information environment or from the inability of existing protection measures to respond to new attack methods. For example, software updates can have unexpected consequences, such as changes in security settings and access rights, or the introduction of new, insecure services into the information processing environment. Efforts can be made to prevent harmful consequences, for example through comprehensive testing and examination of change logs (typically changelog, readme, etc.). Attempts can be made to observe harmful consequences, for example, by reviewing the configurations after updates (installed in a test environment) and by automated scans and configuration comparisons. The following, among others, can be used in hardware protection to protect against connection of unauthorised devices: a) placement of hardware in a sealed and/or alarm-equipped security chassis or equivalent, b) using tamper-proof devices, or c) a similar procedure (e.g., sealing of hardware used). When using a sealing method, there should be a regular process for checking the integrity of the seals. The frequency of inspections acceptable for the examination of unauthorised changes or equipment depends on the methods implemented at the site in question to restrict and monitor access to the object (information system, physical space). In most environments, inspections may be sufficient, for example, semi-annually or annually. Personnel instruction must also be taken into account when protecting against the connection of unauthorised equipment. It must be taken into account that no peripheral devices (e.g., display, keyboard, mouse) and media (e.g. only USB memory approved for that environment) other than those approved for the information processing environment of the security class in question may be connected to terminal equipment. Especially in situations where the terminal equipment is used in a lower-security-class physical space, it is usually not possible to use peripheral devices or media stored in that space.
Implementation example	1) Up-to-date accounting of the configuration of the information processing environment exists. Accounting refers to hardware and software accounting, as well as information about configurations and procedures that affect safety. 2) A change management procedure is in place for changes related to information processing and the information processing environment. Changes are traceable. 3) Procedures are in place to ensure that the security level of the information processing environment is maintained in the event of changes.
Legislation	TihL 13, 15
References	Katakri: I-03, I-05, I-16, I-17, I-18, T-04, T-12
Other additional information	ISO/IEC 27002:2022 5.9, 5.36, 5.37, 8.19, 8.29, 8.32; Information Management Board: Collection of recommendations on the application of certain information security regulations (2020:21, chapter 5); PiTuKri MH-01

Identifier	TEK-17.1, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Change management procedures – reassessment
Requirement	Information security audits and reassessments are carried out periodically during the operation and maintenance of the information processing environment and in the event of exceptional situations.
Overview	
Implementation example	
Legislation	TihL 13(1)
References	Katakri: I-16
Other additional information	

Identifier	TEK-17.2, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Change management procedures – documentation
Requirement	Security documents for the information processing environment will be developed during its life cycle as an integral part of the change and configuration management process.
Overview	
Implementation example	
Legislation	TihL 5(2)
References	Katakri: I-16
Other additional information	ISO/IEC 27002:2022 8.9, 8.32

Identifier	TEK-17.3, C:TL IV, I:Important, A:Important, DP:
Title	Change management procedures – TL IV
Requirement	The subcriterion specifies the requirement of the main criterion.
Overview	
Implementation example	1) The information processing environment is documented at such a level that it is possible to use it to determine the hardware and software used in the information processing environment, including version information (hardware, operating system and application software), and it also supports vulnerability management. 2) The information processing environments are monitored to detect unauthorised changes or hardware. The accounting of the information processing environment is kept up to date throughout the lifecycle. 3) The classification and protection needs of the material related to the implementation of the security of the information processing environment (documentation, electronic accounting and equivalent) have been identified.

Legislation	TihL 5(2), 13(1)
References	Katakri: I-16
Other additional information	ISO/IEC 27002:2022 5.9, 8.8
Identifier	**TEK-17.4, C:TL II, I:Critical, A:Critical, DP:**
Title	Change management procedures – TL II
Requirement	The subcriterion specifies the requirement of the main criterion.
Overview	
Implementation example	1) Hardware is protected against the connection of unauthorised devices (keyloggers, wireless transmitters including mobile devices and similar devices).
Legislation	TLA 11(1) items 2 and 5
References	Katakri: I-16
Other additional information	
Identifier	**TEK-18, C:Secret, I:Normal, A:, DP:Personal data**
Title	Remote access
Requirement	In remote access, users have been instructed and are identified in a sufficiently reliable manner.
Overview	In traditional terms, remote access and management refer to the use/management of information systems from outside the organisation's premises with a terminal device obtained for this purpose. Normally, the terminal device is a portable computer provided to an individual by the organisation. For classified information, remote access in its traditional sense is suitable only for information of security classification level IV. In personnel training and instruction, particular attention must be paid to protecting secret information from third parties. Protection from third parties includes, for example, the selection of possible processing places and restrictions related to the places on processing (prevention of secret viewing and listening), protection of terminal equipment and other work equipment against theft and tampering (storage only in locked space and encryption of memory areas always activated, including the use of protective packaging and cases), and other procedures for the secure use of such equipment and other work equipment.
Implementation example	1) Users are reliably identified in remote access. 2) Remote access is instructed and monitored.
Legislation	TihL 4(2), 13(1); TLA 10(1)
References	Julkri: HAL-12, HAL-13, HAL-19; Katakri: I-17, I-18
Other additional information	CPNI: Personnel Security in Remote Working; CPNI: Configuring and managing Remote Access for Industrial Control Systems; CPNI: Physical Security Advice; ISO/IEC 27002:2022 5.10, 5.37, 6.3, 6.7, 7.1, 7.8, 7.9, 7.10, 8.1; PiTuKri IP-03, JT-05, SA-02

Identifier	TEK-18.1, C:Secret, I:Important, A:, DP:Special category of personal data
Title	Remote access – encrypting information and communications
Requirement	Terminal devices, storage devices and data connections used in remote access outside a security area are protected using encryption solutions that do not contain known vulnerabilities and that, according to information received from manufacturers, support modern encryption strengths and settings.
Overview	For removable media (hard drives, USB memory, and similar), unencrypted devices may be allowed in the event that the media is never left unattended outside the approved security area.
Implementation example	1) The terminal device must have the information encrypted with an encryption solution that has no known vulnerabilities and, according to the manufacturer's information, supports modern encryption strengths and settings. 2) The remote access of the systems requires a data communication encryption solution that has no known vulnerabilities and, according to the manufacturer's information, supports modern encryption strengths and settings. 3) Storage media must not be left unattended unless the storage media (hard drives, USB memory and similar) taken outside security areas is encrypted with a solution that does not have known vulnerabilities and that, according to the manufacturer's information, supports modern encryption strengths and settings.
Legislation	TihL 13(1), 15(2); TLA 10, 11, 12, 13
References	Julkri: FYY-7.1; Katakri: I-18
Other additional information	ISO/IEC 27002:2022 7.9, 7.10, 8.1

Identifier	TEK-18.2, C:TL IV, I:, A:, DP:
Title	Remote access – encrypting classified information and communications
Requirement	Terminal devices, storage devices and data connections used in remote access outside a security area are protected using sufficiently secure encryption solutions, taking into account the security class in question.
Overview	For removable media (hard drives, USB memory, and similar), unencrypted devices may be allowed in the event that the media is never left unattended outside the approved secured area.
Implementation example	1) The data in the terminal device must be protected with an encryption solution that is sufficiently secure for the security class in question, and sufficient integrity of the terminal device for the security class in question must be ensured. 2) Remote access of the systems requires traffic encryption sufficiently secure to protect the information of the security class in question. 3) If the storage media containing classified information (hard drives, USB memory and similar) taken outside security areas are not encrypted by a method sufficiently secure for the security class in question, the data media will not be left unmonitored.
Legislation	TihL 13(1), 15(2); TLA 10, 11, 12, 13
References	Julkri: FYY-7.1; Katakri: I-18
Other additional information	ISO/IEC 27002:2022 7.9, 7.10, 8.1

Identifier	TEK-18.3, C:TL IV, I:Important, A:, DP:
Title	Remote access – strong user identification
Requirement	In remote access, users of systems are identified using strong user identification based on at least two authentication factors.
Overview	
Implementation example	
Legislation	TLA 10, 11(1) item 5
References	Katakri: F-04, I-18
Other additional information	

Identifier	TEK-18.4, C:TL IV, I:Critical, A:, DP:
Title	Remote access – approved devices
Requirement	Only devices approved and identified for the operating environment are used in remote access.
Overview	
Implementation example	Only devices and remote connections approved for the operating environment are used.
Legislation	TLA 10, 11(1) item 5
References	Katakri: F-04, I-18
Other additional information	

Identifier	TEK-18.5, C:TL III, I:, A:, DP:
Title	Remote access – use of security classified information in a public place
Requirement	Classified information is not read or otherwise processed during travel or in public places.
Overview	
Implementation example	
Legislation	TLA 10(1), 13
References	Julkri: FYY-7.1; Katakri: I-18
Other additional information	

Identifier	TEK-18.6, C:TL III, I:Critical, A:, DP:
Title	Remote access – device identification
Requirement	The subcriterion specifies the requirement of the main criterion.
Overview	In security classification levels III and II processing environments and other critical processing environments, the technical linking of use to approved remote access equipment (e.g., device identification) is required.
Implementation example	Remote access using non-approved devices is technically blocked.
Legislation	TLA 10, 11(1) item 5
References	Katakri: I-18
Other additional information	

Identifier	TEK-18.7, C:TL III, I:Critical, A:, DP:
Title	Remote access – TL III
Requirement	The remote use (processing) and storage of security classification III electronic information in a terminal device of that security class outside secured areas is possible, provided that a) the information is protected by an encryption solution that is sufficiently secure for the security class in question, and b) the information security of the terminal device, in particular the confidentiality and integrity required for the security class in question, has been ensured by adequate procedures.
Overview	
Implementation example	
Legislation	TLA 10 (TL III)
References	Katakri: I-18
Other additional information	

Identifier	TEK-18.8, C:TL II, I:, A:, DP:
Title	Remote access – remote access in a security area
Requirement	Remote access of systems is limited to a security area approved by a authorized authority.
Overview	Information processing requires a physically protected security area or substitute procedures to achieve equivalent physical security conditions.
Implementation example	
Legislation	TLA 10 (TL II)
References	Katakri: I-18
Other additional information	

Identifier	TEK-18.9, C:TL I, I:, A:, DP:
Title	Remote access – TL I
Requirement	The subcriterion specifies the requirement of the main criterion.
Overview	Security classification level I information may be stored or otherwise processed only in secured areas (TLA 10), which also imposes restrictions on the possibilities of remote access.
Implementation example	
Legislation	TLA 10 (TL I)
References	Katakri: I-18
Other additional information	

Identifier	TEK-19, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Software vulnerability management
Requirement	Reliable procedures for managing software vulnerabilities are implemented throughout the lifecycle of the information processing environment.

Overview	Software vulnerabilities are exploited in several types of attacks at some point. It should be noted that vulnerable source code exists in operating system software, server applications, and end user applications, as well as in firmware applications and drivers, BIOS, and separate management interfaces (e.g., iLO, iDRAC). In addition to software errors, vulnerabilities are caused by configuration errors and old practices, such as the use of outdated encryption algorithms. Responsible suppliers fix vulnerabilities found in their software. Risks can be reduced by installing patches. When implementing vulnerability management, it is important to ensure that the vulnerability scanner, CMDB and other systems are up to date and secure. Vulnerability management should aim at creating an accurate situational picture that involves continuous monitoring and development of the software and system environment. As part of the maintenance of the situational picture, the risk caused by identified shortcomings and vulnerabilities should be assessed in relation to the operating environment, and corrective measures should be taken based on the criticality of this assessment. Corrective actions include vulnerability fixes and updates from software vendors, and configuration changes that aim to eliminate or limit the risk. In addition, support for the software versions used should be monitored from their supplier. Updates to outdated software versions are not actively released, which can make it impossible to fix security vulnerabilities. Efficient, process-like vulnerability management requires an organised operating model with designated responsibilities, and usually also cooperation between internal and external stakeholders in the organisation. Considerations particularly in implementations that use cloud technology: - In the installation of security updates, a procedure can also be used, for example, where a trusted, golden image of virtual machines is maintained with up-to-date security patches, and any virtual machines in use are regularly replaced with this up-to-date image. In this solution model, special diligence should be exercised in procedures aimed at ensuring image integrity. - In assessing the part for which the customer is responsible, it is recommended that particular attention be paid to the fact that the corresponding requirements also apply to the customer and possible service providers associated with the customer's part.
Implementation example	The requirement can be implemented with a process for vulnerability management that includes at least the following measures: 1) The information security bulletins of authorities, hardware and software manufacturers and other similar parties are actively monitored, and security updates deemed necessary are installed in a managed manner. 2) The installation success of updates is reviewed regularly, at least monthly. 3) The network and its services, servers, and networked workstations, laptops, printers, mobile devices and similar are thoroughly inspected at least annually (vulnerability scanning), and always after significant changes, in order to find repair objects for the upgrade procedures. 4) The processing of discovered vulnerabilities and shortcomings in updating procedures has been arranged in such a way that weaknesses that significantly affect the protection of the information processing environment are eliminated, corrected or otherwise restricted, so that the processing of security classified information is not unduly compromised.
Legislation	TihL 13; TLA 11(1) item 2
References	Julkri: HAL-16, HAL-16.1; Katakri: I-19
Other additional information	ISO/IEC 27002:2022 8.8; Recommendation of the Information Management Board (2020:21, chapter 5); PiTuKri KT-04

Identifier	TEK-19.1, C:TL IV, I:Important, A:Important, DP:
Title	Software vulnerability management – TL IV
Requirement	The devices in the information processing environment are scanned comprehensively for software vulnerabilities at least annually and in connection with significant changes.
Overview	
Implementation example	1) The network and its services, servers, and networked workstations, laptops, printers, mobile devices and similar are thoroughly inspected at least annually (vulnerability scanning, CMDB, etc.), and always after significant changes, in order to find repair objects for the upgrade procedures. 2) The timeliness and information security of hardware and software accounting (incl. CMDB) and the scanning software have been ensured.
Legislation	TihL 13; TLA 11(1) item 2
References	Katakri: I-19
Other additional information	ISO/IEC 27002:2022 8.8; Recommendation of the Information Management Board (2020:21, chapter 5); PiTuKri KT-04
Identifier	**TEK-19.2, C:TL III, I:Critical, A:Critical, DP:**
Title	Software vulnerability management – TL III
Requirement	The devices in the information processing environment are scanned comprehensively for software vulnerabilities at least semi-annually and in connection with significant changes.
Overview	
Implementation example	The network and its services, servers, and networked workstations, laptops, printers, mobile devices and similar are thoroughly inspected at least semi-annually (vulnerability scanning, CMDB, etc.), and always after significant changes, in order to find repair objects for the upgrade procedures. “Significant changes” can include changes in network topology, deployments of new systems and/or service-pack-level updates of existing systems, significant changes in firewall and corresponding filtering rules, etc.
Legislation	TihL 13; TLA 11(1) item 2
References	Katakri: I-19
Other additional information	
Identifier	**TEK-20, C:Public, I:Minor, A:Minor, DP:Personal data**
Title	Backup
Requirement	The backup and recovery processes have been designed, implemented, tested and described to meet the requirements of legislation and operations.

Overview	It is recommended that backup always be scaled to operational requirements. At least the following should be taken into account with backups that are adequate for the operational requirements: 1) The frequency of backups is sufficient in relation to the criticality of the information to be backed up. Requires an investigation of how much information can be lost (recovery point objective, RPO). 2) Backups cover all information relevant to the continuity of system operation. 3) The speed of the recovery process is sufficient in relation to the operational requirements. Requires an investigation of how long recovery may take (recovery time objective, RTO). 4) The backup and restore processes are tested regularly. 5) The documentation of the recovery process is at an adequate level. 6) The physical location of the backups is sufficiently separated from the actual system (different collapse/fire partition, distance between backup and actual space, etc.). Note: Backups should be protected by physical and logical access control methods at least in accordance with the security class of the information (possibly increased by the cascade effect).
Implementation example	The requirement can be met by implementing the measures listed below: 1) Backups are processed and stored throughout their lifecycle in systems of at least an equivalent level of security. 2) If backups are transferred outside the physically protected security area of the security class in question, the procedures in TEK-16 (electronic transmission) and/or FYY-08 (mail/courier) and TEK-18 (transport outside a physically protected area) must be carried out. 3) Backup media are disposed of reliably. 4) The restoration of the system and information is tested regularly, e.g., in an automated manner, so that the information can be restored to its correct state to ensure integrity.
Legislation	TihL 13(1), 15(1); TLA 2(2), 7, 11(1) item 4
References	Julkri: VAR-09; Katakri: I-20
Other additional information	ISO/IEC 27002:2022 8.13; Information Management Board: Collection of recommendations on the application of certain information security regulations (2020:21, chapter 5); PiTuKri KT-03
Identifier	**TEK-20.1, C:TL IV, I:, A:, DP:**
Title	Backup – TL IV
Requirement	The subcriterion specifies the requirement of the main criterion.
Overview	When processing the information of different owners using the same backup system, separation procedures enabling the right of audit must be implemented for the interfaces and storage media of the backup system (e.g., encrypted tapes specific to owner/project, with different encryption keys, stored in customer-specific safe/safe compartments).
Implementation example	When the information of different owners who reserve the right of audit is processed using the same backup system, the separation procedures enabling the right of audit must be implemented according to the security class in question with regard to the interfaces and storage media of the backup system.
Legislation	TihL 13(1), 16; TLA 7, 10(1), 11(1) item 3
References	Katakri: I-06, I-20
Other additional information	ISO/IEC 27002:2022 8.13; Information Management Board: Collection of recommendations on the application of certain information security regulations (2020:21, chapter 5); PiTuKri KT-03

Identifier	TEK-20.2, C:TL III, I:, A:, DP:
Title	Backup – backup registration and tracking of processing
Requirement	The subcriterion specifies the requirement of the main criterion.
Overview	
Implementation example	There are registers of the backup copies, and the processing of the backup copies is recorded in an electronic log, information system, case management system, manual record or in the information itself (for example, as part of a document).
Legislation	TLA 14
References	Katakri: F-08.3, I-20
Other additional information	

Identifier	TEK-21, C:Secret, I:, A:, DP:Special category of personal data
Title	Destruction of electronic information
Requirement	The destruction of electronic information is reliably organised. Methods of destruction of secret information are used to prevent any or all of the data from being reassembled.
Overview	Data protection must be ensured until the end of the data life cycle. This must be taken into account especially in situations where a third-party service is used to destroy data, such as for melting hard drives. As a practical implementation model, a procedure in which the organisation responsible for the data monitors the data destruction process until the end of the life cycle. The secure destruction of data must also be taken into account in the lifecycle management and disposal of devices, including peripheral devices and various memory devices. The role of personnel should also be taken into account in the destruction processes. The organisation must provide the personnel with an unambiguous method of destroying the data.
Implementation example	Destruction with the combination of different methods Other methods to reliably prevent the assembly of data (e.g., melting of shredded hard drive) may also be used to replace or support shredding. Encryption can also significantly reduce the risks to information at different stages of the information and hardware lifecycles. Considerations in destroying information in electronic format The procedures for the reliable destruction of electronic information must cover all hardware where classified information has been stored during its lifecycle. The reliable destruction of security classified information contained in hardware components (hard drives, memory, memory cards, etc.) must be ensured in particular in the event of decommissioning, dispatching to service or reuse. If reliable emptying (e.g. a sufficiently secure overwriting procedure) is not possible, the part containing classified information must not be handed over to third parties. In situations where it is not possible to reliably erase the device memory or equivalent prior to maintenance, third-party maintenance should be monitored to ensure that classified information is not taken during maintenance.
Legislation	TihL 21(2); TLA 15

References	Julkri: FYY-11, FYY-11.1, FYY-11.2, FYY-11.3; Katakri: T-12, F-08.3, F-08.4, I-21
Other additional information	Traficom: Lifecycle management of hard drives (26 October 2016); CPNI: Secure destruction of sensitive items (2017); ISO/IEC 27002:2022 7.10, 7.14; Information Management Board: Collection of recommendations on the application of certain information security regulations (2020:21, chapter 4); PiTuKri SI-02
Identifier	**TEK-21.1, C:Public, I:Minor, A:Minor, DP:Personal data**
Title	Destruction of electronic information – archiving
Requirement	The obligation to archive information has been taken into account in the management of the information lifecycle.
Overview	
Implementation example	
Legislation	TihL 21
References	
Other additional information	
Identifier	**TEK-21.2, C:Secret, I:, A:, DP:Personal data**
Title	Destruction of electronic information – destruction of information in cloud services
Requirement	The subcriterion specifies the requirement of the main criterion.
Overview	Considerations particularly in implementations that use cloud technology: - If unclassified secret information is stored in a cloud service only in an encrypted format that is considered sufficiently reliable, the residual risks may be acceptable if the keys used for encryption can be reliably destroyed. The procedure may also be suitable for the destruction of personal data after its statutory storage period.
Implementation example	
Legislation	TihL 21(2)
References	
Other additional information	ISO/IEC 27002:2022 5.23; PiTuKri SA-03

Identifier	TEK-21.3, C:TL IV, I:, A:, DP:
Title	Destruction of electronic information – TL IV
Requirement	The subcriterion specifies the requirement of the main criterion.
Overview	
Implementation example	Destruction by overwriting When destroying classified material by overwriting, it is recommended that the requirements of the National Cyber Security Centre's guide "Lifecycle management of hard drives" be complied with for overwriting and reusing storage devices. Destruction by shredding When destroying classified material by shredding, the requirements set out in the Ministry of Finance recommendation 2021:5 "Recommendation on the handling of classified documents" for the shred size of the classified material in question must be complied with.
Legislation	TihL 21(2); TLA 15
References	Julkri: FYY-11.1, FYY-11.2, FYY-11.3; Katakri: I-21
Other additional information	Traficom: Lifecycle management of hard drives (26 October 2016); Information Management Board: Recommendation on the handling of classified documents (2021:5)

Identifier	TEK-21.4, C:TL II, I:, A:, DP:
Title	Destruction of electronic information – information prepared by another authority
Requirement	If the information has been prepared by another authority, the destruction of the information that has become unnecessary must be reported to the authority that has prepared the information, unless it is returned to the authority that has prepared the information.
Overview	
Implementation example	
Legislation	TLA 15(2)
References	Katakri: I-21
Other additional information	

Identifier	TEK-21.5, C:TL II, I:, A:, DP:
Title	Destruction of electronic information – executor of destruction
Requirement	The data may only be destroyed by a person assigned to this task by an authority. Versions of the preparatory phase can be destroyed by the person who created them.
Overview	
Implementation example	
Legislation	TLA 15(2)
References	Katakri: I-21
Other additional information	

Identifier	TEK-21.6, C:TL I, I:, A:, DP:
Title	Destruction of electronic information – TL I
Requirement	The subcriterion specifies the requirement of the main criterion.
Overview	
Implementation example	In the destruction of information of security classification level I in electronic format, the shred sizes compiled for class II in the Ministry of Finance recommendation 2021:5 "Recommendation on the handling of classified documents" can be used, provided that the protection is supplemented with procedures approved by an authority. Such procedures typically include the further processing of the shreds by controlled incineration or melting.
Legislation	TLA 15
References	Katakri: I-21
Other additional information	

Identifier	TEK-22, C:, I:, A:Normal, DP:
Title	Availability of information systems
Requirement	Authorities must ensure the availability of information systems throughout their lifecycle.
Overview	The implementation of the availability requirements must take into account the load duration, fault tolerance and recovery time required of the information system.
Implementation example	Availability requirements have been identified. At least the longest time that a system can be out of use, the recovery time objective and the recovery point objective have been identified.
Legislation	TihL 13(1), 15(1) item 4
References	Julkri: VAR-02
Other additional information	ISO/IEC 27002:2022 8.6, 8.14

Identifier	TEK-22.1, C:, I:, A:Normal, DP:
Title	Availability of information systems – procedures safeguarding availability
Requirement	The implementation of procedures safeguarding availability is proportional to the recovery time objective.
Overview	
Implementation example	Procedures safeguarding availability have been implemented with system-specific protection. Protection may include, for example, duplication of essential network connections, hardware and application runtime environments.
Legislation	TihL 13(1), 15(1) item 4
References	Julkri: VAR-02, VAR-06, VAR-07, VAR-08
Other additional information	ISO/IEC 27002:2022 5.30
Identifier	**TEK-22.2, C:, I:, A:Normal, DP:**
Title	Availability of information systems – monitoring of services
Requirement	The availability of services and information systems is tracked and monitored at the level required by their criticality.
Overview	
Implementation example	1) If the service has availability requirements, its availability is monitored by a monitoring system. 2) The monitoring system must send an alarm about any observed availability deviations.
Legislation	TihL 13(1), 15(1) item 4
References	Julkri: HAL-07
Other additional information	ISO/IEC 27002:2022 8.16
Identifier	**TEK-23, C:, I:Important, A:Important, DP:**
Title	Operational usability of information systems
Requirement	The authority has ensured the fault tolerance and functional usability of information systems essential for the performance of its tasks.

Overview	To ensure operational usability, it is recommended to use both technical usability tests and user-run usability tests or heuristic expert assessments. In customised systems, usability should be specified and planned according to a method approved by the organisation. Usability should be tested continuously during development. The usability of standard software should be tested in connection with acceptance testing. Testing should be carried out from the perspective of different user groups. Usability testing can already be carried out at the procurement stage, in which case the suitability of the system to be procured can be better ensured. Compliance with the Information Management Act can also be supported by procedures related to the accessibility of services provided to the public in accordance with the Act on the Provision of Digital Services (306/2019).
Implementation example	1) Information systems relevant for the performance of official duties have been identified. There is a list of information systems identified as essential. 2) The fault tolerance and functional usability of information systems identified as essential are ensured through testing both during the procurement phase and in connection with major maintenance activities. In the assurance, particular attention is paid to the following: a) the information system is easy to learn, b) the operating logic of the information system is easy to remember, c) the operation of the information system supports the tasks for which the user uses the system, and d) the information system promotes its fault-free use.
Legislation	TihL 13(2)
References	Julkri: HAL-17, HAL-17.1
Other additional information	

5 Preparedness and continuity management

Criteria concerning the preparedness and continuity management of normal conditions have been compiled for the area. The criteria are based on the requirements of the Information Management Act (e.g., section 4, subsection 2, item 2, section 13, subsections 1, 2 and 4 and section 15) and on general requirements for guidelines to be drawn up and information security measures, as well as management methods describing the continuity of information security described in the standard ISO/IEC 27002. The measures covered by the Emergency Powers Act concerning the continuity of operations in emergency conditions are excluded from the criteria. However, the criteria also support the organisation in meeting the requirements for preparing for emergency conditions.

The criteria in this section mainly concern items classified as important or critical in terms of availability. The availability levels are described in section 4.2 Classification levels. The criteria can also be applied on a risk-based basis to lower availability categories. However, the examination of continuity requirements and the legislation behind them applies in principle to all organisations.

Key criteria in this sub-area include preparedness measures for various serious disruptions, operational continuity plans and recovery plans for information systems, and training for them. Continuity management is closely related to incident and deviation management processes, the criteria of which are described in the HAL and TEK sub-areas.

Identifier	VAR-01, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Legislation guiding preparedness
Requirement	The organisation has identified the national and EU legislation governing ICT preparedness, related to its operations and services, and other standards related to ICT preparedness.
Overview	Legislation and standards determine the minimum level for implementing ICT preparedness. In addition, the organisation must take into account any needs arising from the special features of its own operations. Understanding the internal and external dependencies of operations is a basic prerequisite for cost-effective management of preparedness.
Implementation example	The organisation examines legislation, regulations, instructions, standards and agreements related to ICT preparedness and continuity management as well as any international obligations. It is particularly important that both an organisation procuring a service and an organisation providing a service are familiar with the regulations affecting the service and keep each other aware of them. In most cases, the legislation and other documents guiding the organisation's operations have been identified and listed in the basics of information security and risk management policy. Government-level guidance documents governing ICT preparedness have been taken into account in the strategies, principles and planning of operations.
Legislation	TihL 4(2) item 2; 13(1)
References	Julkri: HAL-05
Other additional information	PiTuKri TJ-07, PiTuKri EE-02

Identifier	VAR-02, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Specification of continuity requirements
Requirement	The continuity requirements for operations and related essential services and information systems have been specified.
Overview	The recovery-time objectives of a service or system must be determined according to how long the system can be unavailable from the perspective of the organisation's operations. From the operational point of view, it is necessary to determine how much or how long data can be lost.
Implementation example	The organisation must specify continuity requirements in cooperation with risk management, information security, data protection, operations and architectures. The services and systems in core functions and processes to be protected have been identified, and availability targets have been set for them in accordance with the requirements for core functions or processes. The ability to initiate recovery procedures is specified by service.
Legislation	TihL 4(2) item 1, 13(1) and (2), 15(1)
References	Julkri: HAL-05
Other additional information	Collection of recommendations on the application of certain information security regulations 2021:65 chapters 6 and 11; ISO/IEC 27002:2022 5.30

Identifier	VAR-02.1, C:Public, I:Minor, A:Minor, DP:Personal data
Title	Specification of continuity requirements – service transfers
Requirement	The continuity requirements take into account service repatriations and transfers of services to other service providers.
Overview	When procuring the service, it should be noted that it may be difficult to repatriate the service or transfer a supplier-locked service to another service provider. In particular, this requirement must be taken into account when procuring cloud services.
Implementation example	
Legislation	TihL 4(2) item 1, 13(1), (2) and (4), 15(1)
References	Julkri: HAL-05
Other additional information	Guidelines on using cloud services 2020:73; ISO/IEC 27002:2022 5.23

Identifier	VAR-03, C:, I:, A:Important, DP:
Title	Continuity plans
Requirement	Continuity plans have been prepared and put into use.
Overview	The organisation's continuity plan contains principles on how the activities are organised systematically in different situations. The continuity planning of an organisation identifies the services on which the organisation's core functions depend and assesses the impacts of disruptions in ICT services of different lengths on the organisation's core functions. Continuity plans must also take into account the maintenance of the required level of information security during exceptional situations.
Implementation example	The continuity plan includes the personnel available, key persons and deputies and an assessment of their availability. The continuity plans describe how to proceed during disruptions and how to return to normal operation after them. If necessary, the organisation has a plan to transfer the production of ICT services to other premises if the current premises become unusable. Continuity plans are coordinated with stakeholders to a sufficient extent throughout the operating chain. Planning the communication during disruptions is part of the continuity plan.
Legislation	TihL 4(2) item 2, 15
References	
Other additional information	Collection of recommendations on the application of certain information security regulations 2021:65 chapter 11; ISO/IEC 27002:2022 5.23

Identifier	VAR-03.1, C:, I:, A:Important, DP:
Title	Testing and training of continuity plans
Requirement	Continuity plans are regularly tested and practised.
Overview	By practising, the functionality of the plans is tested in different situations. The observations are used to develop the plans.
Implementation example	Organisations are responsible for their own practice activities and specify the practices for testing continuity plans. The organisation practises internally in both national and regional and local exercises to the extent required by the activities.
Legislation	TihL 4(2), 13(2), 15
References	Katakri: I-13
Other additional information	ISO/IEC 27002:2022 5.23

Identifier	VAR-04, C:, I:, A:Important, DP:
Title	Resources and competence
Requirement	People are familiar with continuity and recovery plans related to their own activities and know how to act accordingly. Deputies have been designated, and their ability to perform tasks in normal situations has been ensured.
Overview	
Implementation example	Each trained person is familiar with the principles of the organisation's preparedness and knows the impact of different situation models on their own tasks. They are encouraged to participate in various cooperation groups that support preparedness.
Legislation	TihL 4(2)
References	Julkri: HAL-03; Katakri: T-04
Other additional information	

Identifier	VAR-05, C:, I:, A:Important, DP:
Title	Personnel availability and substitute arrangements
Requirement	In order to carry out critical tasks, special-situation alternative operating methods and personnel availability and substitute arrangements have been planned and prepared.
Overview	
Implementation example	Measures enabled by legislation have been identified and implemented to the extent necessary, for example with regard to the removal of right to strike, the use of emergency work and personal reservations (VAP).
Legislation	TihL 4(2) item 2, 13(1), 15(1) item 4
References	
Other additional information	Working Time Act (872/2019) 19; Act on Collective Agreements for Public Officials in Central Government (664/1970) 11; Conscription Act (1438/2007) 89

Identifier	VAR-06, C:, I:, A:Important, DP:
Title	Ensuring the availability of communications
Requirement	The availability during disruptions of services that are important for operations has been taken into account in communications services and agreements.
Overview	
Implementation example	The network environments and communications services for important services are backed up by, for example, duplicating them. Communications can be physically duplicated on two different routes with two different carriers. In important environments, it is ensured that the failure of an individual communication component does not interrupt the operation of the service. For example, a separate data connection can be installed on selected workstations to allow access to a public data network. The fault tolerance of connections outside Finland should also be taken into account in the contract phase.
Legislation	TihL 13(1), (2) and (4), 15
References	Julkri: HAL-16.1
Other additional information	Collection of recommendations on the application of certain information security regulations (2021:65, chapter 11)

Identifier	VAR-07, C:, I:, A:Important, DP:
Title	Redundancy of IT environments
Requirement	The availability during disruptions of services that are important for operations has been taken into account in IT environments and related agreements.
Overview	
Implementation example	The IT environments of important services are backed up, for example, by duplicating them, so that failure of individual components does not cause downtime beyond the service level required by the operations. IT environments can be backed up by back-up power or back-up power connections so that electricity supply can be started quickly enough and maintained for a sufficient time in relation to the operational requirements.
Legislation	TihL 13(1), (2) and (4), 15
References	Julkri: HAL-16.1
Other additional information	Collection of recommendations on the application of certain information security regulations (2021:65, chapter 11)

Identifier	VAR-08, C:, I:, A:Critical, DP:
Title	Fault tolerance
Requirement	Based on the risk assessment, the ICT infrastructure and essential information systems have been implemented with sufficient fault tolerance and reliability.
Overview	Preparations have been made for disruptions in information systems to ensure rapid recovery. Recovery leverages mechanisms that aim at real-time or near real-time fault tolerance to maintain the availability of critical systems.
Implementation example	The network, server and device environments of critical services are backed up, for example, by duplication. In addition to backups, the organisation also takes protective copies of the systems, which are stored at least in a different combustion space than where the actual data is located. Based on a risk assessment, the information material is distributed geographically to at least two different locations and sufficiently far from each other within Finland's borders. As far as possible, the most critical public administration services and their telecommunication will be implemented in accordance with the requirements of the security network.
Legislation	TihL 13(1) and (2), 15
References	
Other additional information	Collection of recommendations on the application of certain information security regulations (2021:65, chapter 6)

Identifier	VAR-08.1, C:, I:, A:Critical, DP:
Title	Fault tolerance – dependencies
Requirement	The dependence of services on other services and other actors has been taken into account in the design of the entire information processing environment and its fault tolerance.
Overview	
Implementation example	The organisation has identified critical services and their entire supply chain. The entire service chain has been implemented using sufficiently fault-tolerant services. The implementation of fault tolerance makes use of fault-tolerant platform solutions, such as the security network.
Legislation	TihL 13(1) and (2), 15
References	
Other additional information	Security Strategy for Society 2017

Identifier	VAR-09, C:, I:, A:Important, DP:
Title	Recovery plans for information systems
Requirement	Recovery plans for information systems must be prepared, implemented and mutually adapted.
Overview	Recovery plans have been specified for recovering from disruptions in information systems that are important for the organisation's operations.
Implementation example	The minimum levels required by ICT services can be specified in the SLA agreement prepared for the service and in the recovery plan. Minimum levels can be set as time requirements, hardware platform or at least the required communication capacity. The customer of the service is always responsible for the existence of recovery plans. In an outsourced service, the service provider is responsible for preparing system-specific recovery plans. The orderer ensures that the service provider is regularly testing the recovery plans.
Legislation	TihL 4(2) item 2, 13(1) and (2), 15(1)
References	Julkri: VAR-02
Other additional information	

Appendix 1B: Privacy criteria

Personal data include data that can be used to identify a person directly or indirectly, for example by combining individual data with other data that enable identification. A person can be identified, for example, on the basis of a name, a personal identity code, or technical information that identifies the person or the devices used by the person.

The processing of personal data must comply with the requirements of the GDPR when the processing is entirely or partly automatic or the data form part of the register. The GDPR protects personal data regardless of the technology used in data processing. The storage method of the data is also irrelevant. Data can be stored, for example, in an information system, a video surveillance system, or a paper archive.

The information security criteria for the areas described above can be used to protect personal data. Each criterion in the sub-areas is classified according to whether it also applies to the processing of personal data and, if applicable, whether it concerns all personal data or only special categories of personal data.

Identifier	TSU-01, C:, I:, A:, DP:Personal data
Title	Identification of the personal data to be processed
Requirement	The organisation identifies all the personal data it processes.
Overview	The identification of the personal data to be processed is a necessary prerequisite for the protection of personal data and is closely linked to the preparation of the organisation's information management model and the identification of the organisation's information resources in connection with it.
Implementation example	The identification and documentation of the personal data to be processed can be carried out as part of the organisation's identification of the assets to be protected, when an account of processing operations is prepared, or when a data management model is established.
Legislation	TihL 5; GDPR art 5(1)(c)
References	Julkri: HAL-04
Other additional information	

Identifier	TSU-01.1, C:, I:, A:, DP:Special category of personal data
Title	Identification of personal data to be processed – special categories of personal data or data relating to criminal convictions and offences
Requirement	The organisation identifies information belonging to special categories of personal data it processes or related to criminal convictions and offences.
Overview	Special categories of personal data include information on a person's race or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as genetic or biometric information (for the purpose of unambiguous identification of the person), health information or information on the person's sexual behaviour and orientation. The above-mentioned special categories of personal data are, to a large extent, secret information under the Act on the Openness of Government Activities and are subject to higher security requirements than ordinary personal data. For this reason, the organisation must identify if the processing concerns special categories of personal data and classify the data as belonging to special categories of personal data. Personal data related to criminal convictions and offences are also secret and subject to higher security requirements than ordinary personal data and to separate requirements related to the lawfulness of the processing, which is why they must be identified and classified separately.
Implementation example	The identification and documentation of personal data to be processed, in these categories of personal data, can be carried out as part of the organisation's identification of the assets to be protected, when an account of processing operations is prepared, or when a data management model is established.
Legislation	GDPR art 9, 10
References	Julkri: HAL-04.2
Other additional information	

Identifier	TSU-02, C:, I:, A:, DP:Personal data
Title	Roles of the organisation
Requirement	For the personal data they process, the organisation determines whether the organisation acts as a controller, joint controller or processor.
Overview	A controller is a natural or legal person, company, authority or entity that determines the purposes and means of the processing of personal data. The controller is usually the organisation itself, not a person belonging to the organisation Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. The processor of personal data is a third party, other than the controller, that processes personal data on behalf of the controller in accordance with the controller's instructions. Note! The organisation can have a different role in each case of personal data processing, as it depends on who determines the purposes and means of the processing. The organisation may process personal data on behalf of another party as a processor. However, it is the controller of the processing of personal data which it processes on its own behalf and not on behalf of the controllers who are customers. An organisation is the controller, for example, when it processes the personal data of the organisation's own personnel. A processor may process personal data only for purposes specified by the controller. A processor cannot start processing the data processed on behalf of the controller for its own purposes by determining the purposes and means of processing the personal data.
Implementation example	The organisation's role can be documented as one input in the documentation describing the processing of personal data, for example in the reports on processing operations and the information management model.
Legislation	GDPR art 4(7–8), 26, 28
References	
Other additional information	

Identifier	TSU-03, C:, I:, A:, DP:Personal data
Title	Joint controllers
Requirement	When acting as joint controller, an organisation determines, by means of a transparent arrangement with other joint controllers, compliance the obligations of the controllers and informing the data subjects.
Overview	Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They determine, by mutual arrangement and in a transparent manner, each party's area of responsibility in order to comply with the obligations laid down in the GDPR, in particular as regards the exercise of data subjects' rights and informing data subjects. In connection with the arrangement, a contact point may be designated for data subjects. The arrangement must duly reflect the actual roles and relations of the joint controllers with the data subjects. The essential elements of the arrangement must be available to the data subject. Regardless of the terms of the arrangement, the data subject may exercise their rights under the GDPR in relation to each controller and against each controller.

Implementation example	For example, an organisation may conclude an agreement with different joint controllers or document in writing the procedures related to joint controllership, publish them online and make them available at sites.
Legislation	GDPR art 26
References	
Other additional information	
Identifier	**TSU-04, C:, I:, A:, DP:Personal data**
Title	Processor of personal data
Requirement	The organisation uses only processors that implement adequate safeguards.
Overview	A controller may only use processors that have adequate safeguards to implement appropriate technical and organisational measures so that the processing complies with the requirements of the GDPR and ensures the protection of the data subject's rights. The activities of processors may be very limited, such as outsourcing of mail delivery. The tasks can also be extensive and common and may involve managing a particular service on behalf of another organisation, such as tasks related to the payment of salaries of a company's employees. Regulation on the processor applies to, for example, the following service providers: - IT service providers, software integrators, cybersecurity companies and IT consulting companies with access to the controller's personal data. - A health laboratory that handles samples on behalf of the controller. - Marketing and communications agencies that process personal data on behalf of their customers. - More generally, all organisations whose services include the processing of personal data on behalf of another organisation. - A public authority or organisation can also be considered a processor of personal data. Software vendors and hardware manufacturers, such as manufacturers of working-time tracking devices, biometric devices or medical devices, are not considered processors of personal data if they do not have access to personal data and do not process personal data.
Implementation example	The organisation can assess the processor's capability, for example through documentation provided by the processor, approved codes of conduct or certification.
Legislation	GDPR art 28
References	Julkri: HAL-16
Other additional information	

Identifier	TSU-04.1, C:, I:, A:, DP:Personal data
Title	Personal data processor – agreements
Requirement	The organisation prepares agreements with personal data processors that meet the requirements of the GDPR.
Overview	The processing carried out by a processor must be determined by an agreement or other legal instrument in accordance with union or member state law binding on the processor in relation to the controller, setting out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects, the obligations and rights of the controller. More detailed content requirements of the agreement are specified in article 28 of the GDPR.
Implementation example	The organisation may draw up an agreement on the processing of personal data, for example by using the document Tietosuoja-asetuksen huomioiminen kilpailutettaessa julkisia hankintoja (authors: Hansel, Association of Finnish Local and Regional Authorities, KL-Kuntahankinnat, hankinnat.fi) as part of the agreement. In addition to the contractual terms, the controller must provide the processor with or otherwise agree with the processor on the instructions to be followed in the processing of personal data. The processor may only use the services of another processor (sub-processor) with the written consent of the controller. Consent may be granted for a particular processor or may be general, in which case the controller must be informed of the changes in the sub-processors and be given the opportunity to object.
Legislation	GDPR art 28
References	Julkri: HAL-16.1
Other additional information	

Identifier	TSU-05, C:, I:, A:, DP:Personal data
Title	Tasks and responsibilities
Requirement	The organisation determines the tasks and responsibilities related to the processing of personal data.
Overview	The task of the organisation's management is to determine the responsibilities related to personal data processing. Data protection responsibilities are related to the specification of information security responsibilities, for example with regard to measures related to processing security, which in many situations are common to personal data and other data processed by the organisation.

Implementation example	Tasks and responsibilities are recorded in workflows, job descriptions, operating instructions or responsibility matrices. Tasks can also be recorded on a role basis, but in this case it must be ensured that the persons associated with the roles can be easily found based on the documentation. The scope of data protection tasks varies by organisation. Personal-data-intensive organisations may, for example, act by assigning one or more persons to be responsible for the development, implementation, maintenance and monitoring of an organisation-wide management and data protection programme, in order to ensure compliance with all applicable personal data processing laws and regulatory requirements. Some organisations may also need to separately designate individuals to carry out requests for data subject rights. Even if a specific natural person is designated to ensure compliance with data protection rules, that person is not a controller but acts on behalf of the legal person ultimately responsible for the breach as a controller. Similarly, even if a particular department or unit has operational responsibility for ensuring compliance with certain processing operations, this does not mean that that department or entity becomes a controller (rather than the entire organisation).
Legislation	GDPR art 12, 24
References	Julkri: HAL-02
Other additional information	
Identifier	**TSU-05.1, C:, I:, A:, DP:Personal data**
Title	Tasks and responsibilities – data protection officer
Requirement	The organisation appoints a data protection officer suitable for the task and publishes their contact details.
Overview	An authority must designate a data protection officer (DPO), except in the case of a court entrusted with its judicial functions. Several authorities may have a joint data protection officer. The person appointed as the data protection officer must have expertise in data protection legislation and the ability to perform the tasks specified for the data protection officer in the decree. The data protection officer may be a member of personnel or perform tasks on the basis of a service contract. The organisation must publish the contact details of the data protection officer and notify them to the supervisory authority.
Implementation example	
Legislation	GDPR art 37–39
References	
Other additional information	

Identifier	TSU-05.2, C:, I:, A:, DP:Personal data
Title	Tasks and responsibilities – status and tasks of the data protection officer
Requirement	The organisation determines the position, resources and powers of the DPO in such a way as to enable them to carry out the duties of the DPO.
Overview	The data protection officer has the following tasks: - monitors compliance with data protection rules throughout the organisation and take up any shortcomings identified - provides information and advice on obligations under data protection rules to management and employees processing personal data - advises upon request on how to conduct a data protection impact assessment and oversees the implementation of the impact assessment - is the contact person for data subjects in matters related to the processing of personal data - is the contact person for the Office of the Data Protection Ombudsman and cooperates with the Office of the Data Protection Ombudsman In order to ensure the position and operating conditions of the data protection officer, the organisation must: - ensure that the data protection officer is involved in the processing of data protection matters - secure the resources of the data protection officer and access to the necessary information - ensure the independence of the data protection officer in the performance of their duties The data protection officer is subject to the obligation of professional secrecy in connection with their duties (sections 22–23 of the Act on the Openness of Government Activities 621/1999)
Implementation example	The performance of the tasks of the data protection officer may vary widely depending on the scope and nature of the processing of personal data within the organisation. The data protection officer may perform other tasks, provided that they do not create conflicts of interest with the tasks of the data protection officer. In large organisations, the tasks of the data protection officer can be decentralised to several persons.
Legislation	GDPR art 37–39; JulkL 22–23
References	
Other additional information	

Identifier	TSU-06, C:, I:, A:, DP:Personal data
Title	Instructions for the processing of personal data
Requirement	The organisation draws up instructions for the processing of personal data and ensures that personal data are processed in accordance with these instructions.
Overview	The processor or any person acting under the control of the controller or processor who has access to the personal data must not process them except in accordance with the controller's instructions. The controller and the processor must take measures to ensure that any natural person acting under the controller or the processor who has access to personal data processes them only in accordance with the controller's instructions.

Implementation example	The organisation may form general instructions on the processing of personal data and supplement them as necessary with process-specific additional instructions. The organisation must also ensure, through the distribution of instructions, orientation, training and communication, that up-to-date instructions on the processing of personal data are available and known to everyone who needs them.
Legislation	GDPR art 29, 32(4)
References	Julkri: HAL-12
Other additional information	
Identifier	**TSU-07, C:, I:, A:, DP:Personal data**
Title	Lawfulness of processing
Requirement	The organisation identifies the legal grounds for the processing of personal data that it processes, and documents them.
Overview	The processing of personal data always requires legal grounds for processing. Processing is lawful only if and only to the extent that at least one of the following applies: a) the data subject has given consent to the processing of their personal data for one or several specific purposes; b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; c) processing is necessary for compliance with a legal obligation to which the controller is subject; d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. (Item f is not applied to data processing carried out by public authorities in connection with their duties.) If the processing concerns a personal identity code, special categories of personal data, criminal convictions and offences and the related security measures, or is based on consent, the organisation must take into account the additional requirements associated with them.
Implementation example	The organisation determines all the grounds for the processing of personal data before the processing begins. When the processing of personal data is bound to one of the grounds for processing, the grounds can no longer be changed. The organisation documents the processing criteria.
Legislation	GDPR art 5(1)(a), 6, 7, 8, 10; Data Protection Act 4, 5, 7, 29
References	
Other additional information	

Identifier	TSU-07.1, C:, I:, A:, DP:Personal data
Title	Lawfulness of processing – consent
Requirement	If the processing of personal data is exceptionally based on consent, the organisation ensures that the conditions laid down in the GDPR for consent are met.
Overview	In order for consent to be valid, it must be a voluntary, specific, informed and unambiguous expression of will. Particular attention must be paid to the assessment of the voluntary nature of consent. An authority can only use consent for data processing as an exceptional basis for processing, as there is often a clear imbalance of power between the data subject and the controller. In most cases, it is also clear that the data subject has no realistic options other than accepting the data processing by the authority. The GDPR lays down the following conditions for requesting consent: 1. Where the processing is based on consent, the controller must be able to demonstrate that the data subject has given consent to the processing of their personal data. 2. If the data subject gives their consent in a written declaration that also concerns other matters, the request for consent must be clearly separated from other matters in an easily understandable and accessible form in clear and simple language. No part of such a notification that violates the GDPR is binding. 3. The data subject has the right to withdraw their consent at any time. Withdrawal of consent does not affect the legality of the processing carried out on the basis of consent prior to its withdrawal. Prior to giving consent, the data subject must be informed accordingly. Withdrawing consent must be as easy as giving consent. 4. When assessing the voluntary nature of consent, account must be taken as fully as possible of, for example, whether consent to the processing of personal data not necessary for the performance of the contract is conditional on the provision of the service or on the performance of another contract.
Implementation example	The organisation determines the processes for both requesting and withdrawing consent to ensure that all conditions for requesting are met. Documentation must be taken into account in the processes so that the fulfilment of the preconditions for consent can be demonstrated afterwards. In order to ensure that the requirements for consent are met, the organisation can use the instructions on the website of the Data Protection Ombudsman.
Legislation	GDPR art 4(1)(11), 7
References	
Other additional information	

Identifier	TSU-07.2, C:, I:, A:, DP:Personal data
Title	Lawfulness of processing – personal identity code
Requirement	The organisation identifies the grounds for the processing of the personal identity code, and documents them.

Overview	The personal identity code may be processed with the consent of the data subject or if the processing is provided for by law. In addition, the personal identity code may be processed if it is important to identify the data subject unambiguously for: 1) carrying out a statutory task; 2) the exercise of the rights and obligations of the data subject or the controller; or 3) historical, scientific or statistical research. The personal identity code may be processed in the provision of credit or recovery of a claim, in insurance, credit institutions, payment services, rental and lending operations, in credit reporting activities, in health care, social welfare and the provision of other social security services, or in matters concerning government or private employment and other service relationships and related interests. In addition, if the personal identity code is already available to the recipient, the personal identity code may be disclosed in order to update address information or to avoid multiple postal items.
Implementation example	For example, an organisation may separately specify all processing operations in which the personal identity code is used and, in the case of each operation, ensure that there is a legal basis for the use of the personal identity code.
Legislation	Data Protection Act 29
References	
Other additional information	
Identifier	**TSU-07.3, C:, I:, A:, DP:Special category of personal data**
Title	Lawfulness of processing – special categories of personal data
Requirement	The organisation identifies the grounds for the processing of special categories of personal data that it processes, and documents them.
Overview	As a rule, processing of special categories of personal data, such as data on ethnic origin or health, is prohibited. However, processing is possible when an exception to the prohibition is provided for in the GDPR or national legislation.
Implementation example	Before commencing the processing of special categories of personal data, the organisation may, for example: - examine and document the grounds for processing and ensure that they are based on an exception specified in the GDPR or national legislation.
Legislation	GDPR art 9; Data Protection Act 6(1)
References	
Other additional information	

Identifier	TSU-07.4, C:, I:, A:, DP:Personal data
Title	Lawfulness of processing – personal data relating to criminal convictions and offences
Requirement	The organisation identifies the grounds for the processing of personal data related to criminal convictions and offences and related preventive measures that it processes, and documents them.
Overview	Processing of personal data relating to criminal convictions and offences or related preventive measures on a lawful basis is only possible under the supervision of an authority or if: a. the processing is necessary to investigate, establish, present, defend or resolve a legal claim; b. the processing of data is regulated by law or directly due to the controller's statutory task; or c. the data are processed for scientific, historical or statistical purposes. A comprehensive criminal record is maintained only under the supervision of a public authority.
Implementation example	Before commencing the processing of personal data related to criminal convictions and violations, the organisation may, for example: - examine and document the grounds for processing and verify their appropriateness.
Legislation	GDPR art 10; Data Protection Act 7
References	
Other additional information	

Identifier	TSU-08, C:, I:, A:, DP:Personal data
Title	Necessity and proportionality
Requirement	The organisation ensures that the processing of personal data is necessary and proportionate to achieve the legitimate purposes of the processing.
Overview	Personal data should be processed only if the purpose of the processing cannot be reasonably achieved by other means.
Implementation example	Before starting the processing of personal data, the organisation investigates and documents whether the purpose of the processing can reasonably be carried out without the processing of personal data. If the purpose of the processing, such as the implementation of the service, can be done in such a way that certain data are not processed, the processing of personal data in such cases is not necessary and the personal data must not be processed.
Legislation	GDPR art 5
References	
Other additional information	

Identifier	TSU-09, C:, I:, A:, DP:Personal data
Title	Purpose limitation
Requirement	The organisation collects personal data only for specific, explicit and legitimate purposes and does not process personal data in a manner incompatible with the original purposes at a later date.
Overview	The purpose(s) of the processing of personal data must be clearly planned and specified before the processing commences. Personal data may only be collected for specific, explicit and legitimate purposes. Data may not be processed at a later time in a manner incompatible with the original purposes. The processing of personal data may be possible not only for the specified purpose but also for a purpose that is considered compatible with the original purpose. The processing must also be lawful from the perspective of other data protection provisions; a compatible purpose does not entitle the controller to deviate from other data protection provisions. The processing of personal data for the following purposes is compatible if the GDPR safeguards are properly observed. - archiving in the public interest - scientific or historical research - statistical purposes
Implementation example	The organisation can ensure compliance with the purpose limitation, for example, by the following means: - carefully documenting all personal data uses and processing processes - regularly checking that personal data are not used for other purposes, and - informing about the principle of purpose limitation in instructions and training.
Legislation	GDPR art 5(1)(b), 6(4)
References	
Other additional information	

Identifier	TSU-10, C:, I:, A:, DP:Personal data
Title	Data minimisation
Requirement	The organisation processes personal data only to the extent necessary for the purpose of the processing.
Overview	Data minimisation means minimising the amount of data collected and processed regarding data subjects. The personal data to be processed must be: - appropriate, i.e., the collected data must be data capable of fulfilling the intended use - essential, i.e., the collected personal data must have a clear link to the specified purpose, and - limited, i.e., necessary for a specified use of personal data. In order to assess the correct amount of personal data, it is necessary to clearly identify why the personal data are needed. The purpose of the processing makes it possible to determine which personal data are necessary for the purpose of the processing The organisation ensures that a personal identity code is not entered unnecessarily in documents printed or prepared on the basis of the personal data file.

Implementation example	The assessment of the necessity of personal data can be specified as part of the processes related to initiating the processing of personal data and changing situations. The assessment must review all individual personal data groups and assess their necessity in relation to the purposes of the processing. Before starting the processing of personal data, the organisation may, for example: - pseudonymise or anonymise data where possible - ensure that the views of the systems and the documents to be printed or prepared do not show unnecessary personal data (in particular the personal identity code and special categories of personal data), for example by planning the views of the systems, providing instructions on the matter, raising the issue in orientation and training sessions or by carrying out inspections of documents containing personal data - ensure that personal data are not, by default, made available to an unlimited number of individuals without the involvement of a natural person.
Legislation	GDPR art 51(c), 25(2); Data Protection Act 29(4)
References	
Other additional information	
Identifier	**TSU-11, C:, I:, A:, DP:Personal data**
Title	Storage restriction
Requirement	The organisation stores personal data in a format where the data subject is identifiable only for as long as is necessary for the purposes of the processing.
Overview	The controller must plan and be able to justify the storage period of the personal data. The retention periods of personal data must also be documented. The controller must assess the storage period and necessity of the personal data against the intended use. Personal data may only be stored for as long as necessary for the purpose of the use of the personal data. The retention period of personal data may also be affected by national legislation that provides for retention periods, such as the Accounting Act. The controller must take into account the storage periods derived from legislation. When personal data are no longer needed, they must be anonymised or deleted. The controller must ensure that the information system (including cloud services) and other processing processes in its use support compliance with and regular assessment of retention periods. A data subject may also request the controller to erase personal data when they are no longer needed for the purposes for which they were collected or processed. Personal data may be retained for longer than the original purpose only if the personal data are processed only for archiving, scientific or historical research or statistical purposes in the public interest, provided that the safeguards of the GDPR are properly observed. The safeguards must cover both technical and organisational measures guaranteeing, in particular, compliance with the principle of data minimisation. The principle of minimisation also requires as short a storage period as possible. Personal data may not be processed if it is possible to implement the purposes with anonymous data.

Implementation example	The organisation may specify, as part of the process of initiating the processing of personal data, the grounds of determination of the retention period of personal data or the basis for determining it, as well as the process of erasing personal data at the end of the retention period. The organisation ensures that backups are also deleted when personal data are deleted.
Legislation	GDPR 5(1)(e), 25(2)
References	
Other additional information	
Identifier	**TSU-12, C:, I:, A:, DP:Personal data**
Title	Accuracy
Requirement	The organisation ensures that the personal data are accurate and, if necessary, updated, and takes all reasonable steps to erase or rectify without delay any personal data that are inaccurate or incorrect with regard to the purposes of the processing.
Overview	The organisation must ensure that the information in its possession is accurate and up to date. Ensuring the accuracy of the data is particularly important when decisions that are essential for an individual are made on the basis of personal data. Inaccurate and incorrect information may seriously jeopardise the rights of the data subject. For example, incorrect health information in a patient register may lead to incorrect treatment procedures. The organisation must take reasonable measures to ensure that personal data that are inaccurate and incorrect with regard to the purposes for which they are processed are erased or rectified without delay. The more important the accuracy of the data is, the more measures the controller needs to take to ensure the accuracy of the data. The controller must have methods in place for regular assessment of the accuracy and correctness of the information and for making the necessary updates. In general, a data subject also has the right to assess the personal data used by the controller and, if necessary, to request rectification of inaccurate or incorrect data and deletion of unnecessary data. If the controller discloses the personal data in its possession, records of the recipients should be kept. The controller is obliged to notify any rectification of personal data to each recipient to whom the personal data affected have been disclosed. It is only possible to deviate from the notification obligation when notification proves impossible or requires unreasonable effort. The data subject also has the right to request information on the recipients of personal data. If necessary, it must also be possible to transmit information on the incorrect nature of personal data to the original data source, which is why personal data must be accompanied by a data source when data are obtained from another controller.
Implementation example	For example, the controller may specify processes for regularly assessing the accuracy and correctness of the data, for making necessary updates and for informing each recipient to whom personal data have been disclosed and the source from which the original corrected data have been obtained.
Legislation	GDPR art 5(1)(d)
References	
Other additional information	

Identifier	TSU-13, C:, I:, A:, DP:Personal data
Title	Security of processing
Requirement	The organisation ensures the security of personal data by using appropriate technical or organisational measures.
Overview	Taking into account the costs of implementation, the nature and scope of processing, and the risks of varying likelihood and severity, the controller and the processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate: a) the pseudonymisation and encryption of personal data; b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In assessing the appropriate level of security, account must be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. Compliance with an adopted code of conduct or an approved certification mechanism may be used as one of the elements to demonstrate compliance with the requirements set.
Implementation example	The security of the processing of personal data can be ensured as part of the specification and implementation of the organisation's other information security controls by making the risks for personal data a part of the risk assessment when deciding on the level of technical and organisational safeguards to be applied to the information that the organisation is responsible for. The organisation can ensure the safety of processing, for example by implementing criteria in accordance with this set of criteria and paying particular attention to the selection of criteria that complement the minimum criteria on a risk basis.
Legislation	GDPR art 5, 32
References	
Other additional information	

Identifier	TSU-13.1, C:, I:, A:, DP:Special category of personal data
Title	Security of processing – special categories of personal data or data relating to criminal convictions and offences
Requirement	When processing personal data belonging to special categories of personal data or relating to criminal convictions and offences, the organisation must take appropriate and specific measures to protect the rights of the data subject.

Overview	These specific measures include: 1) measures that enable subsequent checking and verification of the identity of the person who has recorded, altered or transferred personal data; 2) measures to improve the competence of the personnel processing personal data; 3) designation of a data protection officer; 4) internal measures by the controller and the processor for preventing access to personal data; 5) pseudonymisation of personal data; 6) encryption of personal data; 7) measures that ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services related to the processing of personal data, including the ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident; 8) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing; 9) specific rules of procedure for ensuring compliance with the Data Protection Regulation and this act when personal data are transferred or processed for another purpose; 10) a data protection impact assessment in accordance with article 35 of the Data Protection Regulation; 11) other technical, procedural and organisational measures.
Implementation example	When processing personal data belonging to special categories of personal data or relating to criminal convictions and violations, the organisation: - ensures the security of the processing of personal data, taking into account that it may involve secret personal data whose confidentiality and integrity are subject to higher requirements and risks - assesses the need for special measures to protect the data subject's rights and, based on the risk assessment, implements the necessary measures.
Legislation	GDPR art 5, 32; Data Protection Act 6(2), 7(2)
References	
Other additional information	
Identifier	**TSU-14, C:, I:, A:, DP:Personal data**
Title	Data breaches
Requirement	The organisation documents all personal data breaches and specifies procedures for reporting them to the supervisory authority and data subjects.
Overview	A personal data breach refers to an event that results in the destruction, loss, alteration, unauthorised disclosure of personal data or access to them by a party without the right to process them. In the event of a personal data breach, the related elements, its effects and the corrective actions taken must be documented. A breach must be reported to the Office of the Data Protection Ombudsman without undue delay and, as far as possible, within 72 hours of the detection of the breach if the breach is likely to pose a risk to the rights and freedoms of persons. Where a breach may pose a high risk to individuals, they must be notified of the breach in person without undue delay. If an organisation acts as the processor of personal data, it must notify the controller without undue delay after becoming aware of a personal data breach.

Implementation example	For example, an organisation may specify the assessment and processing of personal data breaches as part of the overall incident management process, including instructions and responsibilities for the assessment, processing, and collection of data related to data breaches, and the reporting of data breaches to the Data Protection Ombudsman and data subjects. The organisation collects and records, among other things, the description of the personal data breach (such as the nature of the breach and the data subject), the logs of the incident time, the information needed to fulfil the reporting obligations, information on the impacts and consequences of the breach, the risk assessment and the measures taken and the decisions related to the breach.
Legislation	GDPR art 33
References	Julkri: HAL-08, HAL-09
Other additional information	
Identifier	**TSU-15, C:, I:, A:, DP:Personal data**
Title	Accountability
Requirement	The organisation can demonstrate compliance with the requirements of the GDPR.
Overview	The processing of personal data must comply with the provisions of the General Data Protection Regulation. Accountability means that the controller must also be able to demonstrate compliance with data protection legislation. The controller must take the necessary technical and organisational measures to meet the accountability requirement. Accountability also means the obligation to document, in practice taking and recording certain measures. Those measures must be reviewed and updated where necessary. The GDPR contains requirements on accountability, compliance with which must be assessed on a case-by-case basis. The extent of accountability depends, among other things, on the size of the organisation, the amount of personal data and the type of personal data that the controller processes. The controller must take accountability into account already at the planning stage of the processing of personal data.
Implementation example	In order to achieve accountability, the organisation may, for example, specify and document in writing all processes related to the implementation of data protection and ensure that the end result of these processes is documentation that can be used to demonstrate compliance with the processes.
Legislation	GDPR art 5(2), 24
References	Julkri: HAL-09
Other additional information	

Identifier	TSU-16, C:, I:, A:, DP:Personal data
Title	Management of data protection risks
Requirement	The organisation assesses the essential risks related to the processing of personal data and implements the necessary technical and organisational measures in accordance with the risk assessment.
Overview	Management of data protection risks refers to systematic, coordinated and continuous activities that identify, analyse, assess, process and monitor risks to the rights and freedoms of the data subject. The assessment of data protection risks must be made from the perspective of the data subject, i.e., the organisation must assess - which freedoms and rights of the data subject may be compromised by the processing, and - what damage (physical, material or intangible) may be caused to the data subject by the intended processing of personal data. The assessment of data protection risks must take into account the following factors: a) the nature of the processing (e.g., special categories of personal data, the difficulty for the data subject to exercise their rights, due for example to the unpredictability or opaque nature of the processing, new technologies and innovations, the poor status of the data subject), b) the scope of processing (number of data subjects, amount of data, retention period, geographical coverage), c) the context of the processing (e.g., confidentiality, sanctity of the home, combining personal data collected in different contexts), d) the purposes of the processing (e.g., monitoring, tracking and supervision of data subjects, assessment or scoring of persons, automated decision-making with implications for the data subject), and e) risks to the rights and freedoms of natural persons, of varying likelihood and severity. The importance of risk identification is particularly emphasised when the controller determines technical and organisational measures to ensure data protection in the processing of personal data. Technical and organisational measures refer, for example, to instructions given to personnel for the implementation of data protection, access control through self-monitoring, information system data security, notification of a personal data breach, encryption of personal data, pseudonymisation of personal data and other safeguards. Risk management is a continuous activity: the adequacy of the measures in relation to the risk associated with the processing must be assessed continuously and updated as necessary. The controller is also accountable for compliance with the risk-based approach.
Implementation example	Data protection risk management is part of the organisation's operations and other risk management. The organisation implements management methods in accordance with these criteria and pays particular attention to the selection of criteria that complement the minimum criteria on a risk basis. Risks arising from stakeholders and supply chains have been taken into account in the management of data protection risks. Data protection impact assessment (TSU-17) and the specific data protection risk assessment included therein are mandatory when the intended processing may pose a high risk to individuals' rights and freedoms.
Legislation	GDPR art 24, 25, 32–34, 35
References	Julkri: HAL-06
Other additional information	

Identifier	TSU-17, C:, I:, A:, DP:Personal data
Title	Data protection impact assessment
Requirement	Before processing personal data, the organisation carries out an assessment of the impact of the planned processing operations on the protection of personal data, if the processing of personal data involves high risks for the data subject.
Overview	The purpose of the impact assessment is to help identify, assess and manage the risks inherent in the processing of personal data. The impact assessment describes the processing of personal data and assesses the necessity, proportionality and risks arising from the processing of personal data, as well as the measures necessary to address the risks. The objective is to assess whether the residual risk is justified and acceptable in the circumstances at hand. The impact assessment helps the controller comply with, document and demonstrate the requirements of data protection legislation. The organisation must carry out an impact assessment when planning the processing of personal data that is likely to pose a high risk to the rights and freedoms of the data subject. The impact assessment must be carried out before the processing commences and updated if necessary. The impact assessment must be carried out in particular when: - new technology is used in the processing of personal data - there is large-scale processing of personal data related to criminal convictions and offences or special categories of personal data, such as data on health, ethnic origin, political opinions, religious conviction or sexual orientation; - an individual's personal characteristics are assessed through automated processing, systematically and comprehensively, and the assessment leads to decisions that have legal or otherwise significant effects on the person; - an area open to the public is monitored systematically and on a large scale. On its website, the Office of the Data Protection Ombudsman has published a list of the types of processing operations for which the controller must carry out a data protection impact assessment. In addition, national special legislation may require an assessment of the impact of data protection. The requirements for carrying out an impact assessment also apply to processing operations that started before 25 May 2018 and are already ongoing.

Implementation example	The organisation may specify a process for assessing the necessity of an impact assessment for various personal data processing activities carried out by the organisation. For the purpose of carrying out impact assessments, the organisation may establish guidelines and documentation procedures to ensure the correct and consistent implementation of impact assessments. The organisation must seek the advice of the data protection officer in carrying out the impact assessment if the controller has designated a data protection officer. Where personal data are processed in part or in full by a processor, they must help carry out the impact assessment. When drawing up guidelines and templates for impact assessments, the organisation can use the instructions on the website of the Data Protection Ombudsman. Please note The majority of the information collected in the impact assessment and the measures to be taken are those that must be carried out for all personal data processing activities, regardless of whether an impact assessment is required or not. The organisation should ensure that such input data are available and used in the impact assessment.
Legislation	GDPR art 35
References	
Other additional information	
Identifier	**TSU-17.1, C:, I:, A:, DP:Personal data**
Title	Data protection impact assessment – prior consultation
Requirement	If necessary, the organisation consults the Office of the Data Protection Ombudsman before starting the processing of personal data.
Overview	The organisation must consult the Data Protection Ombudsman before commencing the processing of personal data where an impact assessment shows that the processing would pose a high risk to the data subject and the controller has not mitigated the risk by its own actions. The data protection authority shall be consulted, for example, where data subjects could suffer significant or irreversible consequences that they may not be able to counter. Following prior consultation, the Data Protection Ombudsman will issue written instructions to the controller or processor on the measures to be taken to mitigate the risk. If necessary, the Data Protection Ombudsman may also use the powers conferred on it by the GDPR in connection with the prior consultation, such as a warning. The controller and processor must carry out additional procedures in accordance with the instructions before starting the processing of personal data in order for the processing to be considered lawful.
Implementation example	The organisation may specify the determination of the need for prior consultation as one of the processes, such as impact assessment and initiation of the processing of personal data.
Legislation	GDPR art 36
References	
Other additional information	

Identifier	TSU-18, C:, I:, A:, DP:Personal data
Title	Transfer of personal data outside the EEA
Requirement	The organisation has identified the international transfers of personal data outside the EEA related to its activities and the transfer criteria used for them, and has ensured on a case-by-case basis that the personal data transferred are, in the legislation and practices of the third country, guaranteed a level of protection of personal data that essentially corresponds to the EEA level.
Overview	The organisation may transfer personal data to public bodies or international organisations in third countries on the basis of an adequacy decision adopted by the European Commission (art. 45). In the absence of an adequacy decision suitable for the transfer, the data may be transferred based on: - international agreements between public bodies (Art. 46 (2)(a), - administrative arrangements between public bodies (Art. 46 (3)(b), - the application of other appropriate protective measures (Art. 46), or - as a last resort, applying and narrowly interpreting exceptions to specific situations if appropriate safeguards are not possible (Art. 49); the use of exceptions must relate mainly to occasional, non-recurring processing operations. The organisation has assessed on a case-by-case basis whether the transfer mechanism used is sufficient to ensure essentially the same level of data protection as in the EEA and, where appropriate, has introduced additional safeguards. Please note With respect to processors of personal data (e.g. cloud service providers), the organisation has also taken into account where personal data are physically located. For example, remote access to personal data by a processor acting as a service provider from outside the EEA is considered to be a transfer of personal data outside the EEA. Please note As a rule, a cloud service provider always has access to the information processed in its service, if the information is in plain-text format in the service during its lifecycle (for example, displayed as an image to the customer) or the service provider has access to the encryption keys used to encrypt the information. Please note If the conditions for any of the transfer criteria are not met, personal data cannot be transferred outside the EEA.

Implementation example	The identification and documentation of personal data to be transferred to third countries, the transfer criteria used, the recipients of the transfer and the operators of the transfer may be carried out as part of the identification of the assets to be protected by the organisation, the reporting of processing operations or the establishment of a data management model. The organisation may ensure that the personal data transferred are appropriate, relevant and limited to what is necessary in relation to the purposes for which they are processed, for example in accordance with the processes and practices specified for assessing the accuracy of the data (TSU-13). At an early stage, the organisation may make use of the guidelines available on the website of the EDPS and the EDPB (in particular EDPB guideline 2/2020 transfers of personal data between EEA and non-EEA public authorities and bodies) to ensure compliance with the GDPR in legally binding instruments or administrative arrangements between public bodies (international agreements). When assessing on a case-by-case basis whether a level of protection of personal data that is essentially equivalent to the level of the EEA is provided for the personal data to be transferred in the law and/or practice of a third country, and when selecting any additional safeguards that may be necessary, the organisation may make use of the EDPB recommendations 1/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, as well as the European recommendations 2/2020 on the European Essential Guarantees for surveillance measures. The organisation determines the appropriate procedural requirements if it transfers personal data to a third country or international organisation by applying one of the following safeguards: standard contractual clauses (art. 46(2)(c) and (d) GDPR), administrative arrangements between public bodies (art. 46(3)(b) GDPR), approved code of conduct (art. 46(2)(e), approved certification mechanism (art. 46(2)(f) GDPR) or ad hoc contractual clauses (art. 46.3(a) GDPR). In the assessment of applicable procedural requirements, you can use the EDPB recommendations 1/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. The organisation assesses regularly, together with the recipients of the transfer, whether changes occur in the level of protection of personal data in a third country or in the guidelines of the European data protection authorities, and updates the practices if necessary.
Legislation	GDPR chapter V
References	
Other additional information	

Identifier	TSU-19, C:, I:, A:, DP:Personal data
Title	Rights of data subjects
Requirement	The organisation implements the rights of the data subject.
Overview	When processing personal data, the controller must take appropriate measures to enforce the rights of data subjects and facilitate the exercise of those rights. The organisation must verify the identity of the data subject making the requests and comply with the deadlines for responding to the request set out in the GDPR. Under the GDPR, the data subject has the right to: - receive information about the processing of their personal data - access information - rectify information - delete information and be forgotten - limit the processing of information - transfer information from one system to another - object to the processing of information - not be the subject of automated decision-making.
Implementation example	For the purpose of implementing the rights of data subjects, the organisation may implement and document processes to ensure and demonstrate the realisation of the rights of data subjects. The design of processes related to data subjects' rights is particularly important in cases where data subjects are known to exercise a high level of rights.
Legislation	GDPR art 12–21
References	
Other additional information	

Identifier	TSU-19.1, C:, I:, A:, DP:Personal data
Title	Data subject rights – identification of the data subject's available rights
Requirement	In accordance with the identified legal basis for processing the personal data, the organisation has specified what data subject's rights are related to the processing in question.
Overview	The data subject cannot exercise all their rights in all situations. The rights that the data subject can exercise at any given time depend on the basis on which the personal data in question are processed. The organisation may use the material available on the website of the Office of the Data Protection Ombudsman to determine how the grounds for processing affect the rights available. The exercise of each right may be denied in individual cases. Denial is possible if there is a relevant reason for denying the right, or if the prerequisites for exercising the right are otherwise not met. Exceptions to the rights may also be provided for in specific legislation concerning the organisation in question.

Implementation example	In accordance with the processing criterion, the organisation determines which data protection rights are related to the processing in question. The organisation describes how rights are taken into account in the processing of personal data and how requests concerning the rights are processed and implemented.
Legislation	GDPR art 14(5)(b–d), 17(3), 20(1) and (3), 21(1) and (6), 22(2), 23, 85, 89; Data Protection Act 31–34
References	
Other additional information	

Identifier	**TSU-19.2, C:, I:, A:, DP:Personal data**
Title	Data subject rights – transparent information
Requirement	The organisation informs the data subjects of the processing of personal data in the prescribed manner.
Overview	Personal data must be processed in a transparent manner in relation to the data subject. There are some exceptions to this general informing. The purpose of the informing is to provide the data subject with a comprehensive and clear understanding of the processing of personal data as a whole. The controller must assess whether the information provided is understandable from the perspective of the target group in terms of language and consistency. More detailed information requirements partly depend on whether the data are collected from the person or from elsewhere. More detailed information requirements are: - information content - presentation requirements - distribution and delivery method requirements - time requirements The information must be provided in connection with the collection of the data or within a reasonable time (at the latest one month) of receipt of the personal data if the data have not been received from the data subject. The information must be provided at the latest when the data subject is first contacted, or when the data are first disclosed in situations where the data are obtained from a person other than the data subject and are used to communicate with the data subject or are to be disclosed to another recipient.
Implementation example	In connection with electronic data collection, the information can be provided by means of a privacy statement, for example, to which there is a direct link from a form used to collect data. The privacy notice is communicated about with visible notices. If the data collection takes place while the data subject is physically present, the information may be provided in writing or, on request, orally. It is essential that the data subject easily obtains information on the processing of personal data in a concise, transparent, easily understandable and clear format.
Legislation	GDPR art 5, 13–14
References	
Other additional information	

Identifier	TSU-19.3, C:, I:, A:, DP:Personal data
Title	Rights of the data subject – access to data
Requirement	Upon request, the organisation must provide the data subject with a copy of the personal data processed and information on the processing of personal data.
Overview	The data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning them are being processed, and, where that is the case, access to the personal data and information such as purposes of processing, categories of personal data, recipients and retention periods. Where personal data are transferred to a third country or to an international organisation, the data subject has the right to be informed of the appropriate safeguards relating to the transfer. The controller must provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information must be provided in a commonly used electronic form.
Implementation example	The organisation may specify the process for fulfilling the data subjects' requests and include information on how the requests are to be submitted to the controller. If there are many requests, it is also advisable for the organisation to plan and provide instructions on procedures that can be used to fulfil the requests efficiently.
Legislation	GDPR art 15
References	
Other additional information	

Identifier	TSU-19.4, C:, I:, A:, DP:Personal data
Title	Data subject rights – correction, erasure and transfer of data, restriction of and objection to processing
Requirement	Requests for rectification, erasure, transfer, restriction and objection are executed by the organisation.
Overview	The data subject has a set of rights related to personal data that the organisation must implement on request, such as: The data subject has the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning them. Taking into account the purposes of the processing, the data subject has the right to have incomplete personal data completed, including by means of providing a supplementary statement. The data subject has the right to obtain from the controller the erasure of personal data concerning them without undue delay, and the controller has the obligation to erase personal data without undue delay, where one of the following grounds of the regulation applies: These criteria include, for example, the end of the need to use the data or the withdrawal of consent. The data subject has the right to restrict the processing by the controller in certain situations, such as if the data subject disputes the accuracy of the personal data. The controller is also obliged to notify each recipient of personal data of the above measures. The data subject has the right to receive the personal data concerning them, which they have provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller, if the processing is based on consent or agreement. The data subject has the right, on grounds relating to their particular personal situation, to object at any time to the processing of personal data relating to them based on public interest, the exercise of public authority or a legitimate interest. Where personal data are processed for direct marketing purposes, the data subject has the right to object at any time to processing of personal data concerning them for such marketing, which includes profiling to the extent that it is related to such direct marketing.
Implementation example	Detailed processes for exercising rights can be designed taking into account the number of requests and the details of the different rights specified in the GDPR. If there are many requests, it is advisable to design and instruct the processes carefully. Otherwise, it is sufficient for the organisation to ensure the ability to execute data subjects' requests where necessary and to have sufficient knowledge of the detailed requirements set out in the GDPR.
Legislation	GDPR art 16–21
References	
Other additional information	

Identifier	TSU-20, C:, I:, A:, DP:Personal data
Title	Automated individual decisions
Requirement	The organisation identifies situations where the processing of personal data involves automated decision-making and ensures that automatic decision-making is not carried out except in cases specifically permitted by the GDPR.
Overview	The organisation must not make decisions concerning data subjects based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects them. Automatic decision-making (including profiling) is permitted, if the decision: - is necessary for entering into, or performing, a contract between the data subject and a data controller; - is approved by union or member state law applicable to the controller; - is based on the data subject's explicit consent. Profiling refers to the automatic processing of personal data in which the personal characteristics of a person are assessed. Profiling refers in particular to the analysis or anticipation of features related to work performance, financial situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling - is automatic or partly automatic - targets personal data and - assesses personal characteristics. Decision-making is automatic when - it is a decision based solely on automated processing of personal data; and - the decisions to be made have legal or otherwise significant effects on the data subject.
Implementation example	If the organisation does automated decision-making or profiling, the organisation may, at the start of processing and periodically, verify in relation to the detailed requirements set out in the GDPR that the requirements related to automatic decision-making and profiling are met. The organisation must secure at least the following safeguards in connection with automated decision-making (including profiling): - the data subjects are informed about the processing of data - the data subjects are offered simple ways to require human participation in the processing of data, present their own position and challenge the decision - the data and algorithms processed are regularly reviewed to ensure that the decision-making process works as intended and does not lead to, for example, discriminatory data processing for individuals - an impact assessment has been carried out on the processing of personal data
Legislation	GDPR art 22
References	
Other additional information	

Identifier	TSU-21, C:, I:, A:, DP:Personal data
Title	Records of processing activities
Requirement	The organisation prepares a written description of the personal data processing activities carried out by the organisation.
Overview	A description on processing operations must be prepared if the organisation has more than 250 employees, and it must cover all processing operations. A description of the processing operations must be made irrespective of the number of employees when: - the processing of personal data is likely to pose a risk to the rights and freedoms of the data subject, or - the processing of personal data is not random, or - the personal data processed contain special categories of data or personal data related to criminal convictions and offences. In this case, only the related processing operations must be included in the report.
Implementation example	The controller and the processor may prepare reports on processing operations, for example by using the instructions and templates available on the Data Protection Ombudsman's website.
Legislation	GDPR art 30
References	
Other additional information	

Appendix 2: Julkri tool

The appendix is available as a separate file at https://urn.fi/URN:ISBN:978-952-367-193-5

Liite on tallennettu omana tiedostonaan osoitteeseen https://urn.fi/URN:ISBN:978-952-367-193-5

Bilagan finns som en separat fil på adressen https://urn.fi/URN:ISBN:978-952-367-193-5

Appendix 3: Julkri tool user manual

1 Using the tool

This manual describes how to use the Julkri criteria using the Excel tool developed for it (appendix 2). The idea of the tool is that the user first provides the prerequisites describing the assessment situation, on the basis of which the tool selects the relevant, optional and excluded criteria.

1.1 Specification of preconditions

The tool starts with specifying the input data for the assessment using the drop-down menus on the Preconditions sheet. The following information must be entered as preconditions:

- confidentiality, integrity, and availability of the object to be assessed (the classification levels used are specified in chapter 4.2 of the Julkri recommendation),
- whether the object to be assessed includes personal data and whether such data belong to special categories of personal data,
- sub-areas to be included in and excluded from the assessment,
- use case, if a use case suitable for the assessment exists.

1.2 Essential criteria and supplementing them

Based on the given preconditions, the tool displays on the Selected criteria sheet for each criterion whether it is relevant, optional, or excluded from the assessment (Not included in the assessment). The organisation makes an individual decision on the application of each criterion. Decisions are recorded on a criterion-by-criterion basis in the Decision on application column.

The Decision on application column must include, in particular, the justification for the optional criteria that the organisation decides not to implement on the basis of a risk assessment. The justifications must be recorded so that they clearly indicate on what basis, despite the non-application of the criterion, the risk has been assessed to

be at an acceptable level. The justification can be recorded, for example, by describing compensatory controls or by referring to a separate risk assessment.

In principle, the essential criteria must be applied. The organisation makes a decision on the application of the optional criteria on the basis of a risk assessment and a case-by-case assessment. As a rule, criteria not included in the assessment do not need to be applied. The organisation may, for justified reasons, derogate from this principle.

1.3 Using the criteria in assessment

The criteria formed on the basis of the phases described above are used in the object of the assessment either for the assessment of information security or for the planning of information security measures preceding the assessment.

The list of applicable criteria on the tool's spreadsheet Selected criteria serves as a basis for documenting the results of the assessments and the measures, schedules and responsibilities for correcting the deficiencies.

1.4 Operating principles of the tool

The selection of the criteria is based on the combined effect of the selection criteria provided by the preconditions. When selecting criteria, the tool follows the following selection logic:

- Security levels
  - The criterion is essential if the security level specified for the criterion is equal to or lower than the security level of the object under review specified by the user in the preconditions. In other words, if the user has specified that the subject of the assessment contains secret information, all criteria classified as secret or public information are essential.
  - When processing personal data, essential criteria are those that have been classified as personal data in terms of data protection.
  - When processing data belonging to special categories of personal data, all criteria classified as data protection are relevant.
  - The criterion is essential on the basis of security levels if it is essential on the basis of a single security aspect (confidentiality, integrity, availability or data protection).

  - The criterion is optional if the criterion is not relevant and its security level is as high as the security level provided by the user in the preconditions. For example, if the object of the assessment contains secret information, the criteria classified at the TL IV level are optional and the user decides whether or not to apply them based on a risk assessment. In addition, when processing data belonging to the category personal data, the optional criteria are those classified at the level special category of personal data.

- Sub-areas
  - Each sub-area can be selected for assessment (Yes) or excluded (No).
  - If a sub-area has been omitted, no criteria for the sub-area are included in the assessment. For example, if the processing does not include personal data, the data protection sub-area may be omitted, or if the assessment of the administrative sub-area has already been carried out, it may be omitted.

- Use cases
  - The criterion is essential if it is specified as essential on the basis of the use case.
  - The criterion may be specified as optional in the case of use, in which case the organisation makes a decision on the application of the criterion based on whether the criterion is necessary in the assessment situation in question.

- Cumulative effect
  - The criterion is not included in the assessment if it is not included in the assessment based on security level, sub-area or use case.
  - The criterion is optional if it is optional on the basis of security level or use case and is not excluded from the assessment on the basis of security level, sub-area or use case.
  - In other cases, the criterion is essential.

1.5 Vertical view and filtering criteria

The Vertical view sheet displays the criteria in an easy-to-read format. The information displayed in the vertical view can be filtered based on the relevance of the criteria and the application decisions. The materiality of the criteria is determined by the selections made on the Preconditions sheet. Application decisions are made on the Selected criteria sheet.

Filters can be made using the drop-down menus in cells D1 and E1 on the Vertical view sheet. Standard Excel filtering features are used for filtering.

Vertical view cannot retrieve data based on the content of the criteria because the view only displays data from other sheets. You can search for information on the Criteria sheet.

2 Use cases

Use cases have been preconfigured in the criteria, containing criteria suitable for the situation in question. Organisations can also specify use cases themselves for frequent assessment situations. The specification of organisation-specific use cases can be used to make the use of criteria more efficient in different situations, when a suitable level can be selected for the use case based on pre-identified risks, and in addition, criteria that are not suitable for the situation can be dropped from the criteria.

2.1 Predetermined use cases

2.1.1 Administrative security assessment of the information management unit

The use case is intended for assessing the information management unit's minimum level of information security and data protection in accordance with the Information Management Act. It includes an assessment of the aspects of administrative security, data protection, and preparedness and continuity management. The use case can be supplemented with physical security and information system assessments.

2.1.2 Assessment of a SaaS cloud service

The use case is intended for the security assessment of SaaS cloud services. It can be used to assess whether the service to be assessed meets the requirements of the Information Management Act to ensure information security. The assessment can use the certificates, documentation and other possible evidence of compliance with the security requirements of the cloud service provider. If personal data are to be processed in the service used, the data protection criteria must also be taken into account in the assessment. With respect to confidentiality, the use case is limited to the processing of secret information in cloud services.

2.1.3 Procurement of expert work

The use case is intended for assessing the implementation of the security requirements of expert work and the procurement of consultancy services, in order to ensure the information security of the organisation providing expert services. The scope of the assessment depends on how the assignment is carried out. For example, if work is carried out on the equipment of the ordering organisation, the technical section may be omitted if the corresponding assessment has been carried out on the equipment and systems used. If the work is carried out at the supplier's premises, the requirements of physical security or remote work are applied to it.

2.1.4 Assessment of information system service production

The use case specifies the criteria for assessing the service production environment of an information system or the service provider. The use case can be used, for example, for the development of information systems or for the assessment of information processing environments used in service production or for the assessment of information security of suppliers offering similar services. In particular, the use case takes into account the criteria related to continuity management and physical security in service production.

2.2 Use cases by organisation

The use cases greatly facilitate the selection of criteria in frequently recurring situations. In addition to pre-specified use cases, the organisation can specify new use cases or edit existing ones. Special care should be taken in the specification and use of use cases so that essential criteria are not excluded and such flexibility is not lost that can be achieved with other criteria selection features.

When specifying use cases, the following procedures are recommended:

Scope: The organisation must specify the limitations of the use case, on the basis of which it can be decided whether a criterion is necessary in this particular use case or whether the matter is handled by a party outside the scope of the assessment. For example, if an organisation adds a new service to the organisation's common infrastructure, the criteria for the common infrastructure can be assessed once and excluded from the service-specific assessments.

Optional criteria: If it is possible that the criterion is applied in some cases and not in others, it should be specified as optional. Full exclusion of the criteria from a use case

should not be done if it is possible that it is necessary in some assessment situations included in the use case.

Risk assessments: The same risk assessment may be used in similar use cases of the same security level, in which case the same risk-based assessment of the criteria need not be unnecessarily repeated.

- This can be done by completely excluding from the use case criteria that are not applied on the basis of the risk assessment.
- Similarly, on the basis of a risk assessment carried out in advance, criteria that are classified as optional on the basis of the security level may be included in the use case. In this case, all optional criteria can be marked as applicable in the assessment situation without a new risk assessment.

Documentation: Use cases must be documented in sufficient detail. In particular, the limitations and risk criteria on which the inclusion or exclusion of criteria from the use case is based should be described. These criteria must be described in such detail that an independent party can also assess, if necessary, whether the exclusion of the criterion has been justified

2.3 Description of a use case in the tool

The name of the use case and a brief overview of the content of the use case are recorded on the Use case descriptions sheet. The general description of the use case describes the assessment situations that the use case is suitable for.

As there are several aspects to the application of a use case, it is also advisable to provide a separate detailed description of the use case to allow the user of the use case to assess whether the use case is suitable for the assessment situation.

The criteria to be applied in the use case are specified on the Use case criteria sheet. The top row of the sheet contains the names of the use cases specified on the Use case descriptions sheet. The criteria for the use case are specified in the column for each use case as follows:

- Essential criteria included in the use case: 1
- Optional criteria included in the use case: 2
- Criteria excluded from the use case: 0

Appendix 4: Terminology

Term	Definition	Source
Assessment	Analysing and interpreting information on the object of review and evaluating the object based on them. Cf. auditing. Self-assessment and external assessment.	TEPA Term Bank
Document	A document is defined as a written or visual presentation, and also as a message relating to a given topic or subject-matter and consisting of signs which, by virtue of the use to which they are put, are meant to be taken as a whole, but are decipherable only by means of a computer, an audio or video recorder or some other technical device.	Act on the Openness of Government Activities 5(1)
Authenticity/ Authentic	Genuine, non-counterfeit, reliable	Kielitoimiston sanakirja
Integrity	A feature of information that represents that the information has not been altered without authorisation or that it has not been altered accidentally and that any changes can be verified. The integrity of information or an information system may also mean that the information is internally consistent.	TEPA Term Bank
Special categories of personal data	Personal data belonging to special categories of personal data include data indicating a person's racial or ethnic origin, political opinions, religious or philosophical conviction, trade union membership, health data, sexual orientation or behaviour, and genetic and biometric data for identifying a person. As a rule, the processing of data belonging to special categories of personal data is prohibited. Particular care must be taken to protect the data, as their processing may pose significant risks to a person's fundamental rights and freedoms.	Tietosuoja.fi
Personal data	Personal data include all information related to an identified or identifiable person. A person can be identified, for example, by name, personal identity code or some factor that characterises the person.	Tietosuoja.fi
Public	An official document that has not been decreed or ordered to be kept secret. So-called discretionary documents are an exception to this, i.e., documents from the preparatory phase that have not yet become public.	Act on the Openness of Government Activities 1, 16 a, 22

Term	Definition	Source
Non-repudiation, irrefutability	Undeniable, irrefutable, irrevocable, self-evident, certain, unconditional. Non-repudiation is a property that indicates that the sender or recipient of information or an event related to information can also be reliably verified afterwards.	Kielitoimiston sanakirja
Use case	In Julkri, use case refers to a repeated assessment situation in which the same selected set of criteria can be applied. An example of a use case may be an assessment of the information security of a service provider, in which only criteria concerning authorities have been omitted.	
Confidentiality	A feature of information that reflects the fact that the information is available only to those entitled to use it and is not disclosed to third parties.	TEPA Term Bank
Availability	A feature of information that reflects how information, an information system or a service can be used at the desired time and in the required manner.	TEPA Term Bank
Secret (cf. security classification TL II, secret)	An official document that is subject to secrecy laid down in the Act on the Openness of Government Activities or other acts or which an authority has decreed as secret on the basis of law, or a document that contains information on which secrecy is required by law.	Act on the Openness of Government Activities 22, 24
Information	For the purposes of this recommendation, information means the same as document.	
Information material	A data set consisting of documents and other similar information related to a specific task or service of an authority.	Information Management Act section 2
Information management unit	An authority whose task is to organise information management in accordance with the requirements of the Information Management Act.	Information Management Act 2 and 4(1)
Information system	An overall arrangement consisting of information processing equipment, software and other information processing. Information systems include various cloud services and terminal devices used for software processing.	Information Management Act section 2

Term	Definition	Source
Classified document	An entry concerning a security class must be made if a document or the information contained in it must be kept secret on the basis of section 24, subsection 1, paragraphs 2, 5 or 7–11 of the Act on the Openness of Government Activities, and the unauthorised disclosure or unauthorised use of the information contained in the document may cause damage to national defence, preparedness for emergency conditions, international relations, crime prevention, public security or the functioning of the state and national economy or in a similar manner to the security of Finland.	Information Management Act section 18 Act on the Openness of Government Activities 24
Requirement	A requirement is an individual objective set for the object, which the object must be able to achieve. A requirement is part of a criterion. A requirement can be implemented in several ways. A requirement is as specific as possible, i.e., one requirement does not include several different requirements.	
Conformity	Fulfilment of the requirements recommended in Julkri in the subject of the assessment.	

MINISTRY
OF FINANCE

MINISTRY OF FINANCE
Snellmaninkatu 1 A
PO BOX 28, 00023 GOVERNMENT
Tel. +358 295 160 01
financeministry.fi

ISSN 1797-9714 (pdf)
ISBN 978-952-367-193-5 (pdf)

November 2022