TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Criteria to Assess the Information Security of Cloud Services (PiTuKri)

Traficom publications
PiTuKri - version 1.0 - April 2019

125/2019

Contents

Introduction 3
Use 4
- Use cases 4
- Assessment methods 4
- Risk assessment 5
- Structure 5
- Information types 6

Characteristics of cloud computing services 8
- Cloud computing service models 8
- Cloud computing deployment models 9
- Service provision 9
- Location of information and services 9

Subdivision 1: Framework conditions 11
Subdivision 2: Security management 14
Subdivision 3: Personnel security 22
Subdivision 4: Physical security 26
Subdivision 5: Communications security 32
Subdivision 6: Information system security 36
Subdivision 7: Data security 42
Subdivision 8: Operations security 44
Subdivision 9: Transferability and compatibility 48
Subdivision 10: Change management and system development 49

Annex 1: Examples of application of the criteria 52
- Example 1: Customer system implemented as IaaS service 52
  - Security of the cloud computing platform 52
  - Security of the customer system 52
  - Special cases 52
- Example 2: A customer system implemented as SaaS 53
  - Security of the service configuration 53
  - Security of the settings and secure use of the service configuration 53

Annex 2: Assessment and accreditation by the competent authority 54
- Background 54
- Assessment process 54
- Accreditation process 55
- Accreditation by a competent authority 56

Finnish Transport and Communications Agency
Traficom
National Cyber Security Centre Finland
ISBN 978-952-311-464-7
ISSN 2669-8757 (online publication)

Introduction

The objective of the Criteria to Assess the Information Security of Cloud Services (PiTuKri) is to improve the security of authorities' information to be kept secret in situations where the information is processed in cloud computing environments. The criteria are intended as a tool for security assessment of cloud computing services. The criteria were prepared from the perspective of Finland's national needs. The national legislation reform initiatives have been taken into account so that the criteria also support the reformed legislation[1]. The preparation process made use of the BSI Cloud Computing Compliance Controls Catalogue (C5)[2], the Cloud Controls Matrix (CCM) of the Cloud Security Alliance (CSA)[3], the ISO 27001[4] and ISO 27017[5] standards as well as the Katakri criteria[6]. A further objective of the criteria is to support and make the implementation of the Ministry of Finance's Guidelines for Public Sector on Data Communications Services[7] more concrete.

The criteria address authorities' protection level IV classified information as well as other information to be kept secret. The security requirements described in the criteria are designed to keep the most typical risks facing classified and other information to be kept secret at a tolerable level. Security arrangements for information of higher protection levels are addressed only in connection with the assessment of the general applicability of cloud computing services. The criteria may also be used to protect the authorities' public information and to respond to the needs of business and industrial life.

The National Cyber Security Centre Finland (NCSC-FI) continues to develop the criteria. The NCSC-FI gathers feedback and further development wishes related to the criteria. The feedback will be taken into account in the updated future versions of the criteria. Support tools and materials with additional information will be provided for the application of the criteria.

Use

Use cases

The criteria are intended for the assessment of information security of cloud services. They can also be used to support cloud service providers' independent information security work. The criteria have been designed to support different cloud computing services and different use cases. In order to use the criteria appropriately, their application should be use case specific. In some use cases, it may be advisable to apply the requirements described in the criteria only to the part that the cloud service provider is responsible for; in some cases, to the parts of the service provider and the cloud service customer alike; and in some cases, only to the part that the customer is responsible for. In order to use the criteria appropriately, the security assessor, cloud service provider and cloud service customer must possess adequate competences.

Assessment methods

Different methods may be used for the information security assessments of cloud services. When assessing the protection of some types of information, it may be adequate to rely on the cloud service provider's self-assessment, possible other certifications and contractual commitments. When evaluating the protection of other types of information, it is advisable to additionally require verification by an independent external party. The reliability of the verification results greatly depends on the reliability of the methods used. For instance, the degree of reliability achieved through documentation review differs from the level achieved by also using technical testing for the verification of cloud service security. It is often possible to apply, for example, continuous auditing as a source for additional evidence to improve the quality of verification. When evaluating the protection of certain types of information, it is advisable to use the assessment service of the National Communications Security Authority[8]. More information about challenges related to the assessment of cloud services as well as some proposed solutions can be found in the deliverables of the EU-SEC project[9], for example.

With certain limitations, other frameworks and valid certifications may be utilised to demonstrate the fulfilment of the requirements described in the PiTuKri. When evaluating the possibilities for such utilisation, it is particularly recommended to pay attention to the fact that the different frameworks and certifications measure different things. For instance, some frameworks enable the certification of the information security management system so that the assessment of the adequacy of technical controls relies on the risk management decisions of the target organisation of the certification. This approach is different from the model generally used for the protection of classified information, in which the originator of the information (the authority who owns the information) sets minimum requirements for the protection of information; these requirements accompany the information throughout its life cycle in all processing environments and situations. When evaluating the possibilities for utilisation, it should also be kept in mind that certifications may be limited to cover only part of the process or processing environment of the information to be kept secret, that the requirements of different frameworks aim for different assurance levels of protection, and that the reliability of verification of the fulfilment of the requirements also varies.

[1] The Administration Committee of the Parliament of Finland. 2019. URL: https://www.eduskunta.fi/FI/vaski/Mietinto/Documents/HaVM_38+2018.pdf.

[2] Bundesamt für Sicherheit in der Informationstechnik. 2017. Cloud Computing Compliance Controls Catalogue (C5) - Criteria to assess the information security of cloud services. URL: https://www.bsi.bund.de/EN/C5.

[3] Cloud Security Alliance. 2018. The Cloud Security Alliance Cloud Controls Matrix (CCM). URL: https://cloudsecurityalliance.org/working-groups/cloud-controls-matrix.

[4] ISO/IEC 27001:2013 — Information technology — Security techniques — Information security management systems — Requirements.

[5] ISO/IEC 27017:2015 — Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

Risk assessment

Each authority is responsible for ensuring the adequate security of its information processing. Each authority is ultimately responsible for arranging comprehensive and reliable assessment for the use case at hand and for risk-based handling of the assessment observations.

Appropriate use of PiTuKri requires interpreting the requirements specifically for the use case in question. Requirements may also be substituted with other controls of a similar level of effectiveness. The requirements or implementation examples do not describe sufficient protection measures for every environment or every special case.

It is possible to implement services on a cloud computing platform with the customer bearing the main responsibility for protection. On the other hand, particularly the availability of a service is affected by a number of factors, and a failure in any one of them may completely block access to the service. For instance, availability failures in the platform layer may prevent the application layer from providing the service for the customer. Similarly, even if the platform layer had been designed to support high availability, defects on the application layer may block access to the service. Access may also be prevented by a failure on the customer's device or in the connection between the device and the cloud service. On the other hand, all of the requirements described in the criteria are not as such suitable for all use cases and require case-specific assessment. It may be advisable to establish some of the protection measures on the cloud service platform and some only in the client system. Examples of application of the criteria are described in Annex 1.

In those use cases in which the goal is to achieve accreditation by the competent authority for a cloud service platform or a customer system placed on the platform, the protection measures must match the risk assessment findings of both the target organisation and the competent authority. Particularly in cases involving use of compensatory controls, the target organisation must be able to demonstrate that the sufficient level of protection is achieved. The assessment and accreditation process of the National Cyber Security Centre's NCSA function is described in more detail in Annex 2.

Structure

PiTuKri is divided into ten subdivisions. Subdivision 1, Framework conditions, has a special role with respect to the other subdivisions. The framework conditions define the possibilities for further assessment and support the risk management work of the authorities responsible for the protection of national information to be kept secret. For certain information to be kept secret, there are grounds for carrying out further assessment of a public, multinational cloud service, for instance. For some information, risk-based further assessment possibilities may be limited to nationally provided private cloud computing services.

The subdivisions consist of requirement cards. A requirement card includes a description of the theme of the requirement, the concrete requirement, the scope of application, the security objective and additional information to support implementation and interpretation of the requirement. The descriptions of the requirements are intended to support different ways of implementation. Some of the requirements address only the protection of classified information, while others also cover other information to be kept secret. The information types addressed by the requirements are described in detail for each requirement.

[6] Ministry of Defence of Finland. 2015. Katakri 2015 - Tietoturvallisuuden auditointityökalu viranomaisille. URL: https://www.defmin.fi/Katakri.

[7] Ministry of Finance of Finland. 2019. Julkisen hallinnon pilvipalvelulinjaukset. URL: http://urn.fi/URN:ISBN:978-952-251-982-5.

[8] National Cyber Security Centre. 2018. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-NCSA-toiminnon-suorittamat-tietoturvallisuustarkastukset.pdf.

[9] The European Security Certification Framework (EU-SEC). 2019. URL: https://www.sec-cert.eu/.

Information types

Different types of information are subjects to different risks. For instance, it is generally considered that classified information of the authorities should be protected from the perspective of the security of the State (the public interest). On the other hand, it is reasonable to assume that actors interested in classified information are often not the same as actors interested in non-classified personal data, for instance. Information types are divided into categories based on their protection requirements. The categories are presented in Table 1.

Table 1. Types of information.

Type of information	Description
Public	Public information. Needs for protection are typically related to integrity and availability.
Salassa pidettävä (Information to be kept secret)	Information of the authorities that is to be kept secret but has not been classified and does not contain personal data. This information type covers non-classified, protection level IV information governed under the effective legislation (at the time of publishing the criteria in April 2019) as well as non-classified information to be kept secret that does not contain personal data and is governed under the renewed legislation[10].
Personal data	Data pursuant to special legislation (such as the EU's General Data Protection Regulation[11]) related to the protection of personal data. Most information to be kept secret of the authorities contains personal data and is, therefore, also included within the scope of personal data -related specific legislation.
TL IV	Classified protection level IV ('KÄYTTÖ RAJOITETTU', national RESTRICTED) information of the authorities. The need for protection generally arises from the security of the State (the public interest). Protection must also take into account legislation-derived risks[12].
A large quantity of information to be kept secret (TL III aggregate)	The aggregate effect may sometimes be considered to constitute a level III ('LUOTTAMUKSELLINEN', national CONFIDENTIAL) classified information resource. For instance, comprehensive personal data of the government security authorities and/or other personal data that can compromise operational security.
A large quantity of TL IV information (TL III aggregate)	The aggregate effect may sometimes be considered to constitute a level III ('LUOTTAMUKSELLINEN', national CONFIDENTIAL) classified information resource.
Preparedness	Information needs to be accessible also in exceptional circumstances (preparedness). In this context, 'exceptional circumstances' refer to a situation in which network connections of the society are limited to the geographical boundaries of Finland.
TL III and TL II	Level III ('LUOTTAMUKSELLINEN', national CONFIDENTIAL) and/or II ('SALAINEN', national SECRET) classified information of the authorities. The need for protection generally arises from the security of the State (the public interest). Protection must also take into account legislation-derived risks.

The division shown in Table 1 does not cover all the use cases of the authorities. For instance, preparedness involves different needs with different authorities, and the division provided addresses these only partly. Appropriate use of PiTuKri requires identifying the information types being processed and assessment of the risks associated with each use case.

[10] The Administration Committee of the Parliament of Finland. 2019. URL: https://www.eduskunta.fi/FI/vaski/Mietinto/Documents/HaVM_38+2018.pdf. (In Finnish.)

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

[12] Legislation-derived risks refer to possibilities under legislation of different countries to obligate cloud service providers to cooperate with the authorities of the country in question and to provide, for instance, direct or indirect access to the cloud service customers' information to be kept secret. In addition to the physical location of information to be kept secret, legislation-derived risks may extend to disclosure of information administrated from another country through management connections. In many countries, legislation-derived disclosure and right to view data are limited to the police and the intelligence authorities.

Characteristics of cloud computing services

The descriptions provided in this chapter relating to cloud services are based on the concepts used in the definitions of NIST[13] and the concepts used in the Ministry of Finance's Guidelines for Public Sector on Data Communications Services. PiTuKri specifies the concepts in more detail from the security perspective, mapping them to a risk-based cloud security assessment. 'Cloud computing', or 'cloud service', refers to data processing capacity or service that is accessible over network, and which is provided applying a model of shared, scalable and flexible resources and automated to be partially provided on a self-service basis.

Cloud computing service models

The most common cloud computing service models include Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). In the IaaS model, the entire infrastructure related to providing services is acquired from the service provider. In the PaaS model, services are provided using a provided software platform. In the SaaS model, the service provider provides the services as a whole.

In each one of these models, security-related responsibilities are divided between the service provider and customer. The division of responsibilities depends on the service model and the details of the service implementation in question. A typical division of responsibilities is illustrated in Figure 1.

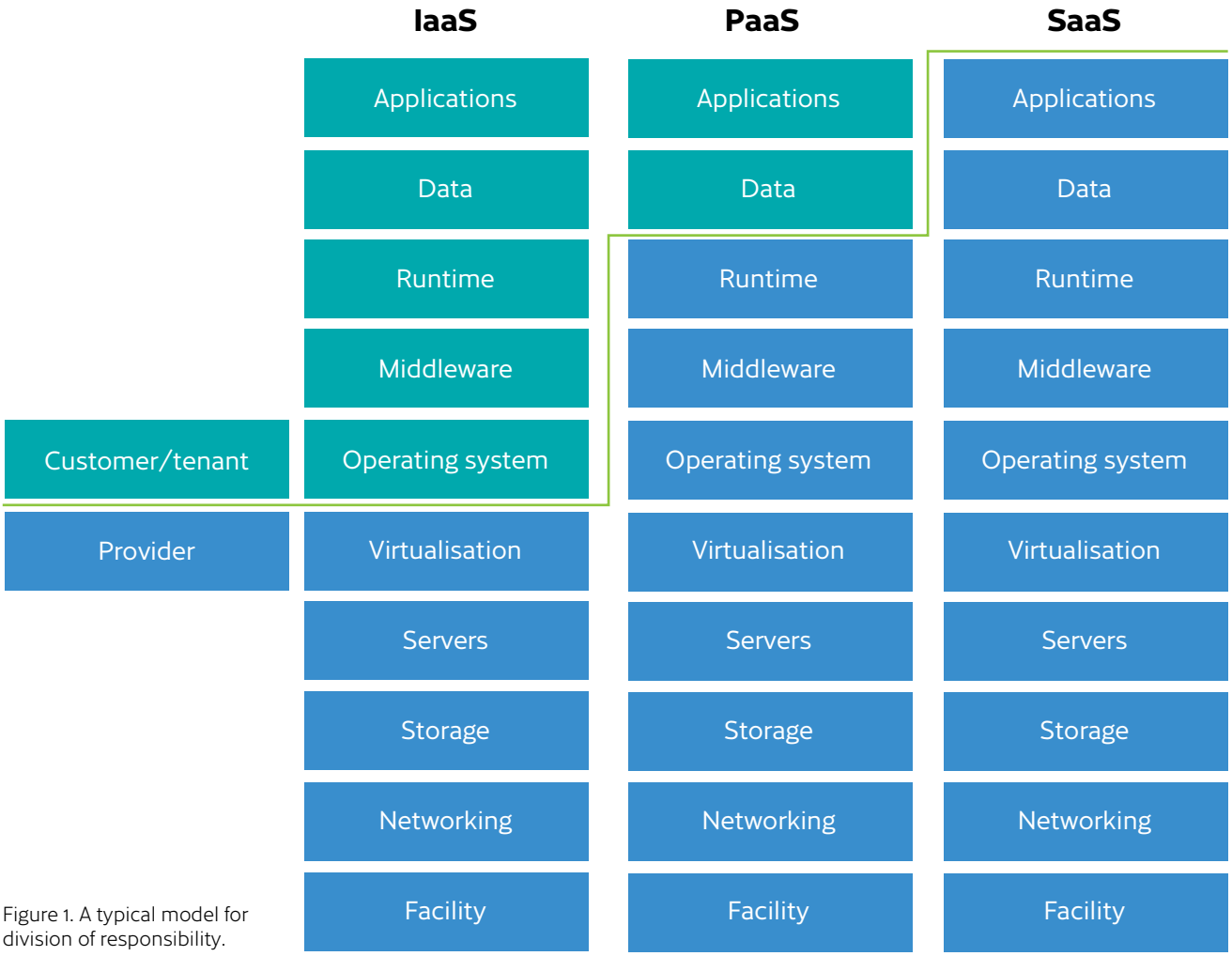


Figure 1. A typical model for division of responsibility.

[13] National Institute of Standards and Technology (NIST). 2011. Special Publication 800-145: The NIST Definition of Cloud Computing. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

Cloud computing deployment models

The most common cloud computing deployment models are private cloud, hybrid cloud and public cloud. Other deployment models, such as community/government clouds, can usually be assessed on the basis of the most common deployment models.

Private cloud refers to service provided for exclusive use by a single organisation. The service may be operated from the service provider's and/or the user organisation's data center. A typical strength of a private cloud is reliable isolation of the information from other data processing environments, user organisations and external parties. Typically, a private cloud can provide services of a higher security level compared with the other deployment models.

A public cloud is a service publicly available for open use by anyone. The service is practically always provided from the service provider's data centers. Compared with a private cloud, a public cloud involves a larger attack surface for other users or external parties.

A hybrid cloud combines a private and public cloud into a single service configuration. For instance, a private cloud on the organisation's own data center may be supplemented with services from a public cloud. The security level achieved typically depends on the type of information that may travel from the private cloud into the public cloud and on the implementation of security measures at the interface of the two clouds.

Service provision

The cloud service provider typically has access to any unencrypted information processed through the service. Different service providers involve different risks. Service providers can be divided into the following categories:

- The organisation itself
- A national authority/public operator
- A national private operator
- A multinational authority/public operator (e.g., a community of authorities of the EU countries)
- A non-national private operator (the EU or the EEA)
- A non-national private operator (other countries).

What is essential from the security perspective is the level of assurance at which the service provider's ability and trustworthiness can be established. For instance, the trustworthiness of Finnish service providers can be assured as part of the national Facility Security Clearance process. In situations that involve more than one service provider organisation[14], risks must be assessed and taken into account for each organisation participating in the provision of service.

Location of information and services

Processing or storage of data processed by cloud computing, as well as maintenance and other administrative measures related to the provision of the cloud computing service, may reside at different geographical locations. Different locations may involve different risks, associated for instance with applicable law. From the security perspective, different locations can be categorised as follows:

- Finland
- Areas enabled by data protection regulations, often the EU area/the EEAA
- Other countries.

Various agreements between countries or organisations may affect location-related risks. From the security perspective, also other requirements concerning the service, such as requirements related to data protection or preparedness, may set geographical limitations to the choice of cloud computing service.

[14] An example of this is a setting in which a cloud service provider A provides a cloud computing platform on which customer B's service is implemented, with company C in charge of the maintenance and implementation of its application functionality.

Subdivision 1: Framework conditions

EE 01	System description
Requirement	A system description is required of the cloud computing service. The description must enable the assessment of the general applicability of the service for the use case in question. At least the following must be described: a) The service and deployment models and related Service Level Agreements (SLAs). b) The principles, procedures and security measures, including monitoring measures, of the cloud computing service life cycle (development, use, disposal). c) Description of the infrastructure, network and system components used for the development, maintenance/management and use of the cloud computing service. d) Change management policies and practices, particularly the processes of changes affecting security. e) Processes for significant abnormal events, such as procedures in major system failures. f) The roles and division of responsibilities between the customer and service provider relating to the provision and use of the cloud computing service. This also includes cooperation obligations and the cloud service customer's corresponding monitoring measures. g) Operations transferred or outsourced to subcontractors.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV
Security objective	The purpose of the description is to enable the assessment of the general applicability of the service and the assessment of risks in relation to the customer's use case.
Additional information	The description of infrastructure, network and system components must be sufficiently detailed so that it can be used to assess the general applicability of the service and its risks in relation to the customer's use case. Cf. KT 01 (System description to promote continuity and operations security). The description of infrastructure may, to a certain extent, utilise the source code from which the infrastructure is being built. Service models include, for instance, Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Deployment models include, for instance, private cloud, hybrid cloud and public cloud. Some cloud computing service providers offer their customer the possibility to use new functionalities that are still in the preview or testing phase. If such functionalities are considered for processing of information to be kept secret, it is recommended to consider questions such as deployment-related responsibilities in risk assessment. New functionalities may still contain security flaws, and liability for possible damage resulting from them is often assigned to the customer in agreements.

EE 02	Legislation-derived risks
Requirement	1) Any legislation-derived risks and obligations associated with the cloud computing service must be described. The descriptions prepared by the service provider must enable the assessment of the general applicability of the service for the use case in question. The descriptions must cover the entire life cycle of the use of the service and of the information processed through the service. The descriptions must include at least: a) The physical location of the information processed in the service for the entire life cycle of the information. b) The physical location of the different functions (such as maintenance/management solutions, back-ups) and components of the service for the entire life cycle of the information. c) Any other parties participating in the provision of the service (outsourcing). d) The law applied to the use of the service and the information processed through the service as well as the place of jurisdiction. e) Parties that may, pursuant to applicable law, have access to the information processed through the service. 2) Legislation-derived risks do not limit the applicability of the cloud computing service for the use case in question. 3) The information of a cloud computing customer may be kept only in the physical locations described in the agreement throughout the life cycle. An exception is a situation in which a cloud computing service customer has in advance approved in writing the transfer and processing of information in other physical locations.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV
Security objective	The purpose of the description is to enable the assessment of the general applicability of the service and the assessment of risks in relation to the customer's use case.
Additional information	Legislation-derived risks refer to possibilities provided by law in different countries to obligate cloud computing service providers to cooperate with the authorities of the country in question and provide, for instance, direct or indirect access to cloud service customers' information to be kept secret. In addition to the physical location of information to be kept secret, legislation-derived risks may extend to disclosure of information administrated from another country through management connections. In many countries, legislation-derived disclosure and right to view data are limited to the police and the intelligence authorities. 1a) and 3) In case the physical location of the information may vary, the description must include all the possible locations in which information may end up during its life cycle. It is recommended to apply the general principles of further assessment described in Table 2.

Table 2. Possibilities for further assessment.

Information type	Type of cloud computing service	Physical location	Cloud service provider	Additional information
Public	No limitations	No limitations	No limitations	In the assessment of suitable protection measures, the focus is on ensuring adequate integrity and availability.
Information to be kept secret	No limitations	No limitations	No limitations	If no personal data are included. If includes personal data, see next row.
Personal data	No limitations	Areas enabled by data protection regulations, often the EU/EEA	No limitations	The service configuration must comply with the special legislation related to the protection of personal data (including the EU's General Data Protection Regulation). Location and management of data in an area enabled by national and/or the EU's data protection regulations.
TL IV (national RESTRICTED)	No limitations	Finland	National	Authorities of other countries must not have direct or indirect access to the information. The limitation to physical location also covers administration, back-up and other maintenance solutions. The security of a service provider can be assessed (e.g., as part of the national Facility Security Clearance process).
A large quantity of information to be kept secret (TL III, national CONFIDENTIAL, aggregate)[15]	Private/community[16]	Finland	National	Authorities of other countries must not have direct or indirect access to the information. The limitation to physical location also covers administration, back-up and other maintenance solutions. The security of a service provider can be assessed (e.g., as part of the national Facility Security Clearance process). With regard to the aggregate effect, such methods must be taken into account that limit access to only a single or limited part of the information content that is necessary for the task at hand and detect attempts of more extensive unauthorised access to the data content. Cf. Katakri (2015/01/Additional information/ Aggregate effect).
A large quantity of TL IV information (TL III, national CONFIDENTIAL, aggregate)	Private/community	Finland	National	Authorities of other countries must not have direct or indirect access to the information. The limitation to physical location also covers administration, back-up and other maintenance solutions. The security of a service provider can be assessed (e.g., as part of the national Facility Security Clearance process). With regard to the aggregate effect, such methods must be taken into account that limit access to only a single or limited part of the information content that is necessary for the task at hand and detect attempts of more extensive unauthorised access to the data content. Cf. Katakri 2015 (I 01/Additional information/ Aggregate effect).
Preparedness	No limitations	Finland	National	Information must be accessible also in exceptional circumstances (preparedness). Information management must be possible in a situation in which network connections of society are limited within the geographical boundaries of Finland. The security of a service provider can be surveyed (e.g., as part of the national Facility Security Clearance process).
TL III (national CONFIDENTIAL) and TL II (national SECRET)	Private/community	Finland	National	Authorities of other countries must not have direct or indirect access to the information. The limitation to physical location also covers administration, back-up and other maintenance solutions. The security of a service provider can be assessed (e.g., as part of the national Facility Security Clearance process). Requirements for additional protection at protection level III and/or II must be taken into account, Cf. Katakri 2015.

[15] The aggregate effect is considered to constitute a level III classified information resource. For instance, comprehensive personal data of the government security authorities and/or other personal data that can compromise operational security.

[16] A community/government cloud with certain limitations, such as a service limited to the use of government or other community of authorities.

Subdivision 2: Security management

TJ 01	Security principles
Requirement	1) The organisation has a security principles approved by the senior management, describing how the organisation's security measures are linked to the organisation's activities. 2) The security principles are comprehensive and appropriate with regard to the cloud computing service provider and the information being protected. 3) The security principles govern the security activities. Implementation of the security principles is reported and regularly monitored.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV
Security objective	The organisation's security principles aim to ensure that the management is committed to security work in the organisation and that the security work supports the organisation's activities.
Additional information	The security principles are communicated to the personnel and, where necessary, stakeholders. The principles can be presented in many ways, such as a single document or as a part of the organisation's policy documentation. Valid ISO 27001 certification can support demonstrating fulfilment of the requirement, provided that the certification (including application plan) covers the processes used for the development and provision of the cloud computing service.

TJ 02	Security responsibilities
Requirement	1) The duties and responsibilities related to the management of cloud service security are specified and documented. 2) The division of responsibilities between the customer and service provider relating to the provision and use of the cloud computing service are described. Cf. EE 01. 3) A designated person is in charge of cloud service security.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV
Security objective	The purpose of specifying the duties and responsibilities of security work is to ensure that persons in charge are designated to the most important domains of security and they know their responsibilities and authority.
Additional information	It is essential to specify the security responsibilities to enable the persons in charge to perform the security duties they are responsible for. If not otherwise described, all security responsibilities lie with the management of the organisation. The purpose of specifying a cloud computing policy (or a similar description) is to make clear which security duties are the responsibility of the customer and which are the responsibility of the service provider.

TJ 03	Security risk management
Requirement	1) The service provider has a risk management process in place. Risk management must be a regular, continuous and documented process. Risk management decisions and respective persons in charge are documented. 2) A systematic and comprehensible method must be used for the risk analysis. 3) Risk management must cover at least the subdivisions of security management, physical security and information security. 4) Identified risks related to relevant stakeholders must be taken into account. The cloud service provider must ensure compliance with customer data-related obligations also in situations in which data are processed by assignment of the cloud service provider. Cf. TJ 08 (Security of service providers and suppliers). 5) The risk management process and its results are utilised when setting security goals for the cloud service provider, assessing the impact of security events, planning security measures, in change management and, where applicable, in procurement. 6) Security measures are scaled taking into account the protection level, quantity, format and classification basis of the information as well as the designated information processing environment in relation to an estimated risk of hostile or criminal activity. 7) The cloud service provider documents the essential content of the monitoring and security measures to be applied.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV
Security objective	The objective of risk management is to identify and manage factors that could potentially compromise the operation and keep any risks at a level that does not put operations and goals at risk.
Additional information	**Taking account of the legislation and regulatory requirements in security level planning** The cloud service provider must be aware of the legislative or regulatory requirements that govern their operations. Meeting these requirements to obtain an accreditation from the authorities, for instance, may require implementing protection measures that are stricter than the cloud service provider's internal security standards. Cf. TJ 07 (Compliance and data protection). **Allocation of risk management measures from the perspective of information to be kept secret** Risk management measures must be allocated to the environment in which the information to be kept secret is to be processed. Risk management measures may be administrative (e.g., training and instructions for the personnel) or technical (e.g., technical security measures of the environment). **The principle of defence in-depth in risk management** The planning of risk management measures aims at reducing risks aimed at the operations. Defence-in-depth is a good principle to apply to the planning of these measures. This means that should an individual security arrangement fail, there are still other protection measures left. Sufficient protection against individual risks may be achieved by single reliable security measures or by combining several measures. **Risk management and analysis methods** There are many different methods available for risk management and analysis. Each one of them has its strengths and weaknesses. Many systematic methods are based on the identification of threats and vulnerabilities, assessment of probabilities and impacts, specification of risk mitigation measures, assessment of residual risk and follow-up of corrective measures.

TJ 04	Management of security incidents
Requirement	1) The cloud service provider must have procedures in place to appropriately address security incidents. 2) The cloud service provider must have clearly defined processes for the reporting of security incidents. The organisation must have designated persons/parties to who security incidents or suspected incidents are reported. 3) The number and types of security incidents must be monitored. Recurrence of incidents must be prevented as efficiently as possible in correction plans. 4) Security incidents and suspected security incidents relating to the processing of customer data must be reported to the customer in question.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV
Security objective	Security incident management aims to ensure that the organisation can function efficiently in unwanted situations, minimising damage and restoring the situation to normal. The obligation to report to the customer supports the customer's risk assessment activities and, among others, minimisation of damage.
Additional information	The following model, for instance, may be used to meet the requirement: The management of security incidents is 1) planned, 2) instructed and trained, 3) documented at an adequate level for the operational environment, 4) practiced and, in particular, 5) communication routines and responsibilities are specified. It is recommended that, in particular, anomalies, security breaches and attempts thereof are reported to the National Cyber Security Centre. It is recommended to also report any detected criminal activity to the police.

TJ 05	Continuity management
Requirement	Continuity management processes and procedures are planned, implemented, tested and described in a manner that enables fulfilment of the requirements of service level agreements and law as well as other business-related requirements of the cloud computing service. The arrangements must particularly take into account that a) adequately quick recovery and assurance of continuity with regard to the operating requirements is taken into account in the planning, b) preventive and recovery measures must be incorporated into contingency plans to minimise the effects of major failures or exceptional events on data processing and storage, c) observations of anomalies are included as part of risk assessment, and recovery and contingency plans are updated according to the observations and results, and d) plans related to ensuring continuity take into account the need to protect information in emergencies to prevent unauthorised access to information, disclosure of information or loss of integrity and availability.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV
Security objective	The objective of continuity management is to ensure the continuity of service so that it is possible to meet the availability, integrity and confidentiality requirements associated with the service.
Additional information	The following model, for instance, may be used to meet the requirement: The effects on business are analysed and plans concerning business continuity and preparedness are verified, updated and tested at regular intervals (at least once a year) or always after substantial changes concerning the organisation or environment. The testing also concerns customers and major third parties (such as important suppliers) that are affected by these matters. The tests are documented and the results are taken into account in future security measures concerning the continuity of business. Data center services (such as water supply, electricity, adjustment of temperature and humidity, communications and Internet connections) are ensured, monitored and maintained as well as tested at regular intervals to ensure their continuous efficiency. The services are designed to include automatic fault-resilient mechanisms and measures such as mirroring. Maintenance work is carried out in accordance with the maintenance intervals and objectives recommended by the supplier, and only authorised personnel may perform the work. Maintenance logs and any entries in them on suspected or detected defects protocols are retained for a predefined period of time. Cf. FT 05 (Preparedness and continuity management) and KT 03 (Backup copies).

TJ 06	Classification and labelling of information and other assets
Requirement	1) A consistent method is in place for the classification and labelling of assets (information, equipment, software, premises) that are essential with respect to providing the cloud computing service and processing customer data. 2) Assets with information content that must be kept secret and protected (information materials, equipment and systems) are classified pursuant to legal requirements. 3) The equipment and software related to providing the cloud computing service and processing customer data are identified. 4) The equipment and software are classified according to their degree of criticality. 5) An owner/person in charge is designated for each set of equipment and software. 6) Up-to-date records are kept of equipment and software, so that any changes to the approved configuration can be detected by comparing the configuration with the records. (Cf. MH 01: Change management.)
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV
Security objective	The purpose of classification is the identification and correct scaling of security measures according to the need for protection. The purpose of labelling is to enable the practical implementation of the security measures according to the classification.
Additional information	Depending on the information, processing environment and users, classification may be indicated in various ways. By classifying information processing environments in accordance with the information material, it is possible to clearly indicate the security measures related to each information processing environment. To fulfil item 2 of the requirement, it is also possible to use a procedure in which the cloud service provider classifies all material produced by the customer for the service in accordance with the service provider's internal classification, so that the protection of assets (information materials, equipment and systems) with such classification meets the protection requirements for information to be kept secret across the entire life cycle of the information. Automated procedures are recommended for the maintenance of equipment and software records. Alternatively, the records being up-to-date can be ensured by, for example, monthly manual checks. The change history of the records (the changes made) must be traceable.

TJ 07	Compliance and data protection
Requirement	1) The cloud service provider must identify, document and regularly update the provisions of laws and regulations applicable to the cloud computing service, as well as the procedures to ensure compliance. 2) At least once a year, independent third parties carry out an audit of the operations, processes and IT systems related to the cloud computing service as applicable, in accordance with the description included in a specific audit plan. The purpose of the audit is to identify any cases that are not in compliance with the law or regulations. The audit plan must cover the security of the service in such a manner that all the most important areas affecting security are audited at least every three years. Any detected deviations are documented, prioritised and rectified according to their degree of criticality. 3) An internal audit of the cloud computing service is performed at least once a year. The purpose of the audit is to survey how the service as a whole complies with its security practices and fulfils its contractual and legal responsibilities. 4) The senior management is responsible for ensuring that any deviations detected are prioritised and protection measures are replaced or rectifications made in due course.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV
Security objective	Fulfilment of legal and contractual obligations.
Additional information	The cloud computing service provider must ensure the security of functions such as personal data processing in accordance with article 32 of the General Data Protection Regulation (GDPR) (EU) 2016/679. Classification of personal data and processing according to the classification may be necessary if there are different protection needs associated with different personal data (legal requirements, value, inclusion of special categories of personal data) or/and data are processed in a different way in the cloud service provider's different functions or systems. The Office of the Data Protection Ombudsman (Tietosuojavaltuutetun toimisto, TSV) is the authority supervising the protection of personal data in Finland. Substantial personal data breaches must be reported to the TSV and the users in accordance with articles 33 and 34 of the GDPR. Other legislation must also be taken into account when reporting personal data breaches. For instance, Regulation (EU) No. 611/2013 regulates on telecommunications companies' obligation to report personal data breaches to the Finnish Transport and Communications Agency Traficom and the users. Cf. TJ 04 (Management of security events).

TJ 08	Security of service providers and suppliers
Requirement	The cloud service provider must ensure compliance with customer data-related obligations also in situations in which the cloud service provider assigns data processing tasks to others. In particular, the service provider must ensure that a) before employees of the service provider/supplier are provided with access to assets, they must be subjected to the same protection measures (agreements, non-disclosure obligations, security clearance, training) as the cloud service provider, b) the service providers/suppliers have received written instructions and signed agreements under which they undertake to implement protection of at least the same level as the cloud service provider, c) reliable procedures are in place for ensuring and controlling compliance with contractual obligations, d) service providers and suppliers who directly or indirectly participate in the processing of classified information have valid official accreditation or are included within the scope of a similar procedure. The procedure must cover, as applicable, the areas of administrative (security management), physical and technical security.
Applicability	Security of the service provided as a whole, insofar as external service providers or/and suppliers are involved.
Information types	1a–1c: Information to be kept secret, personal data 1d: TL IV
Security objective	The security of the assets is also ensured in circumstances in which the cloud service provider's own service providers or/and suppliers have direct or indirect access to them. Cf. MH 02 (System development).
Additional information	The security of the outsourcing and supply chains often has a direct effect on the protection of information processed through the cloud computing service. If the security of the cloud service provider's service to any extent relies on outsourcing or supply chains, their security must also be taken into account in the planning and maintenance of the overall security of the cloud computing service.

Subdivision 3: Personnel security

HT 01	Taking into account the different phases of employment
Requirement	The cloud service provider has a procedure in place to ensure security in the different phases of employment. Particular attention must be paid to measures in connection with recruitment, changes in duties, and termination of employment.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV
Security objective	Mitigation of personnel-related risks during the different phases of employment.
Additional information	Security awareness typically requires instructions, which must be made available to the relevant personnel and the personnel must be trained in their application. The instructions may be divided into categories according to the phase of employment, for instance. The categories may include recruitment instructions, induction training, instructions for changes during employment, instructions for the termination of employment and instructions for more detailed measures, such as changes in access rights.

HT 02	Assessment of personnel's trustworthiness and reliability
Requirement	1) The backgrounds of internal and external employees with access to cloud service customers' information or shared IT infrastructure are checked before the beginning of employment, using procedures enabled by local law. Within the limits allowed by law, the background check must include at least the following: a) Verification of identity. b) Verification of job history. c) Verification of educational background. 2) The trustworthiness of individuals associated with the handling of classified information is checked and monitored by clearance procedures of a relevant level.
Applicability	The overall security of the service provided.
Information types	1: Information to be kept secret, personal data, TL IV 2: TL IV (employees with main responsibility for security, technical administrators or similar employees with an access to a large quantity of TL IV information or opportunity to influence the protection of this information).
Security objective	Reduction of risks associated with personnels' trustworthiness.
Additional information	2: If there is direct or indirect access to customers' protected information. For instance, virtualisation platform (hypervisor) administrators often in practice also have access to customer information processed in virtual machines.

HT 03	Non-disclosure agreements and secrecy commitments
Requirement	A non-disclosure or secrecy commitment procedure is in place. Non-disclosure agreements must be signed before the beginning of a contractual relationship or before granting access to cloud service customers' information.
Applicability	Internal employees of the cloud service provider; employees of external service providers and suppliers.
Information types	Information to be kept secret, personal data, TL IV
Security objective	Reduction of risks associated with personnel's' trustworthiness, particularly through increased awareness.
Additional information	At least the following must be described in a non-disclosure agreement (or similar document): • Which information is subject to non-disclosure • Terms and conditions of the non-disclosure agreement • What measures should be taken at the expiry of the agreement (e.g., destroy or return the data storage media) • Who owns the information • What rules and regulations apply to the use of information to be kept secret and its disclosure to other parties, if applicable • Consequences of breaching the non-disclosure agreement.

HT 04	Security awareness
Requirement	1) The essential principles and procedures associated with security must be described. 2) The personnel must be instructed in secure procedures so that an adequate level of security awareness can be ensured. 3) The up-to-datedness and practical implementation of security-related descriptions/instructions must be checked regularly and at least once a year. 4) The security-related instructions cover the processes and processing environments of information to be kept secret for the entire life cycle of the information. 5) Compliance with the security instructions is monitored and the need for changes is regularly assessed.
Applicability	Internal employees of the cloud service provider; employees of external service providers and suppliers.
Information types	Information to be kept secret, personal data, TL IV
Security objective	The principles (cf. TJ 01) and descriptions/guidelines as well as their practical implementation aim to ensure that secure procedures have been planned and the personnel can also in practice act in a secure manner, including taking into account special circumstances. Cf. KT 01 (System description to promote continuity and operations security).
Additional information	It is essential to specify the security responsibilities to enable the persons in charge to perform the security duties they are responsible for. If not otherwise described, all of the security responsibilities lie with the management of the organisation. Cf. TJ 02 (Security responsibilities). The following procedure may be used to fulfil the requirement: 1) Instructions and training are provided for the personnel on appropriate handling of information to be kept secret. 2) Training on the handling of information to be kept secret is provided on a regular basis and the persons participating in the training are documented. 3) Compliance with the security instructions is monitored and the need for changes is regularly assessed. 4) Information security-related security trainings and security awareness development programmes tailored for the target groups are available and mandatory for all internal and external employees of the cloud service provider.

HT 05	Need-to-know and separation of duties
Requirement	1) The service provider keeps a list of duties that require handling of information to be kept secret. These duties also include such development and maintenance duties that enable direct or indirect access to information to be kept secret or otherwise have substantial influence on the protection of information to be kept secret. 2) Access to information to be kept secret cannot be granted, until the need-to-know related to the person's duties has been determined. 3) The service provider keeps a protection level-specific list of access rights to classified information. 4) Where possible, duties and areas of responsibility are separated to reduce the risk of unauthorised or unintentional alteration or misuse of assets. If high-risk duty combinations may develop, there must be a monitoring mechanism in place to control them.
Applicability	The overall security of the service provided.
Information types	1–2: Information to be kept secret, personal data, TL IV 3-4: TL IV
Security objective	The security objective is to ensure that information to be kept secret can only end up with authorised persons on the need-to-know basis, in order to reduce exposure of information to be kept secret to risks.
Additional information	Determination of the need-to-know is easier when the organisation has described the principles of access to information to be kept secret by the organisation's people and a process or instructions for granting and managing task-based access in situations of change. Avoidance of high-risk job or role combinations should be taken into account in access right specifications as well as job and role specifications. The assessment of the requirement must also consider the division of responsibilities between the cloud service provider and the customer. Typically, for instance, the cloud service provider cannot usually influence the determination of need-to-know for developers or administrators of the system section that the customer is responsible for.


TECHNOLOGY

Subdivision 4: Physical security

FT 01	Defence-in-depth and risk management
Requirement	1) Physical security measures are implemented according to the principle of defence-in-depth. 2) The premises in a building are classified as an administrative area, security area or technical security area, with clearly defined and visible boundaries. 3) Security measures are scaled to an adequate level, so that they match the risks identified by the cloud service provider's risk assessment.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV
Security objective	The security objective is prevention of unauthorised access to the cloud service provider's data center and information to be kept secret, as well as prevention of theft, damage, loss, financial loss and interruptions, and minimisation of their effects.
Additional information	Defence-in-depth principle means implementing a number of security measures that complement each other. If possible, areas form zones inside each other so that the innermost areas have the highest need for protection. Security measures are designed as an entity, which takes into account the protection level and quantity of information to be kept secret and the environment and structure of buildings. The cloud service provider must have a risk management process in place (cf. TJ 03). The risks of premises or buildings containing sensitive or critical information, information systems or other network infrastructure are regularly assessed (at least once a year) by the cloud service provider. The risks have designated owners, persons in charge of the assessment and persons in charge of specified management measures. The risk assessment is documented. The following procedure may be used to fulfil the requirements: A building is designed so that the walls, ceiling and floor form the first protection layer. Access to the building is controlled and managed by means such as access control systems and locks. Information with a higher protection level is processed in the inner parts of the building so that intrusion into the premises would be a difficult and slow task. Technical security solutions complement the structural solutions. The design takes into account windows, doors and other openings.

FT 02	Structures and security systems
Requirement	The outer limits of premises or buildings containing sensitive or critical information, information systems or other network infrastructure are protected in a physically resistant manner and with modern and appropriate security measures.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV
Security objective	The security objective is prevention of unauthorised access to the cloud service provider's data center and information to be kept secret, as well as prevention of theft, damage, loss, financial loss and interruptions, and minimisation of their effects.
Additional information	There are no special structural requirements for the fence surrounding the area or the outer walls, ceiling, floor, windows, doors and other openings of the buildings. Structures that suit the use of the buildings are adequate. The security technology must support the overall security of the area and building. Possible security measures could include a location at a sufficient distance from external parties, fences, security guards or technical surveillance systems (e.g., access control, alarm device and video surveillance systems). The systems must be regularly serviced in accordance with the manufacturer's recommendations and their working order must be ensured. Security systems and equipment must be tested (at least once a month) and kept in working order. All testing must be documented. The following or similar procedure may be used to fulfil the requirements: • The structure of the walls of the building: reinforced concrete (50 mm), mineral wool for heat insulation (80 mm), reinforced concrete (60 mm). The wall structure of a data center in which information is stored: fire board (12 mm), gypsum board + wool + gypsum board (70mm). • The entire building is protected by an access control and alarm device system. The routes leading into the data center are covered by camera surveillance. The systems are managed and monitored by an external private security company with which the organisation has signed a security contract. Responsibility for the servicing, maintenance, testing and documentation of the systems is assigned to the person in charge of security in the organisation. The functioning of the systems is tested once a month.

FT 03	Prevention of unauthorised access
Requirement	1) Access to spaces or buildings that include sensitive or critical information, information systems or other network infrastructure is protected and surveilled by an electronic access control system and/or mechanical/electromechanical keys to prevent unauthorised access. 2) Access management is arranged so that unauthorised access to information to be kept secret is prevented. Access to areas that include information to be kept secret is allowed only on the need-to-know basis related to work duties.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV
Security objective	Only authorised persons have access to information to be kept secret processed through the cloud computing service, the equipment processing the information or the systems overseeing their security.
Additional information	The following procedure may be used to fulfil the requirements: a) The organisation uses ID cards with photographs or other similar visible identifiers that are kept visible when on premises. b) A document or log exists of the access rights granted and mechanical keys used, maintained by a designated person in charge in the organisation. The process for the granting and cancellation of access rights and mechanical keys as well as the process for lost keys is described in writing. Access rights and keys are checked regularly and according to need (at least every six months, or at the beginning and end of employment, or when a person changes job within the organisation). c) The designated person in charge of key management has a chart of the locking system and a key card. d) The access control system uses an identification system that is based on two factors (e.g., identifier + PIN code). Access rights and mechanical keys are individualised for each user. If shared identifiers are used, an alternative method is in place for the reliable identification of each person. e) The mechanical keys are of a model whose copying is restricted. The mechanical keys to the data center are of a different series than the other keys to the building. Spare keys or an access identifier (for emergencies, etc.) are kept sealed in a locked space. The receipt of a check-out of a key or access identifier can be verified afterwards.

FT 04	Service providers and visitors
Requirement	1) Visitors are identified, provided with a visitor badge and recorded. The cloud service provider has a documented visitor policy. The host principle is always applied to visitors. 2) The cleaning, maintenance and other personnel of service providers are identified, provided with a visitor badge and recorded. Regular service providers are provided with an ID card with a photograph. 3) A security clearance has been run on service providers who may independently move on premises or access protected information. Persons without security clearance always have an escort on premises. Cf. HT 02. 4) Practices related to servicing, updates and maintenance are described and documented in writing.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV
Security objective	Only authorised persons assessed to be reliable have access to information to be kept secret stored the cloud computing service, the equipment processing the information or the systems overseeing their security.
Additional information	The practices and guidelines should take into account at least the following: a) ensuring the integrity of information throughout the life cycle, b) secure removal of information to be kept secret before repair or maintenance performed by an external party, c) on premises where information to be kept secret is stored and in the area outlining the premises, any maintenance work, installation and cleaning of the technical spaces and their equipment may only be carried out by security-cleared individuals who have been granted special permission to enter the secured area and who are under the supervision of the personnel of the organisation, d) agreements have been signed with the relevant service providers (e.g., fuel for spare power machines), e) the organisation has valid security agreements in place with a private security company (security services) and the company providing property maintenance services (ventilation, water, electricity, fuel, cleaning), f) response time to an alarm is such that the risk of being caught is high, g) the organisation has precautionary measures in place for maintenance and other breaks and a written description of the measures has been given to the personnel, h) any installation and maintenance work on security systems is performed by a designated company with security-cleared personnel, i) cleaning takes place once a month or as needed. The cleaners are security-cleared. The cleaners have ID cards with a photograph.

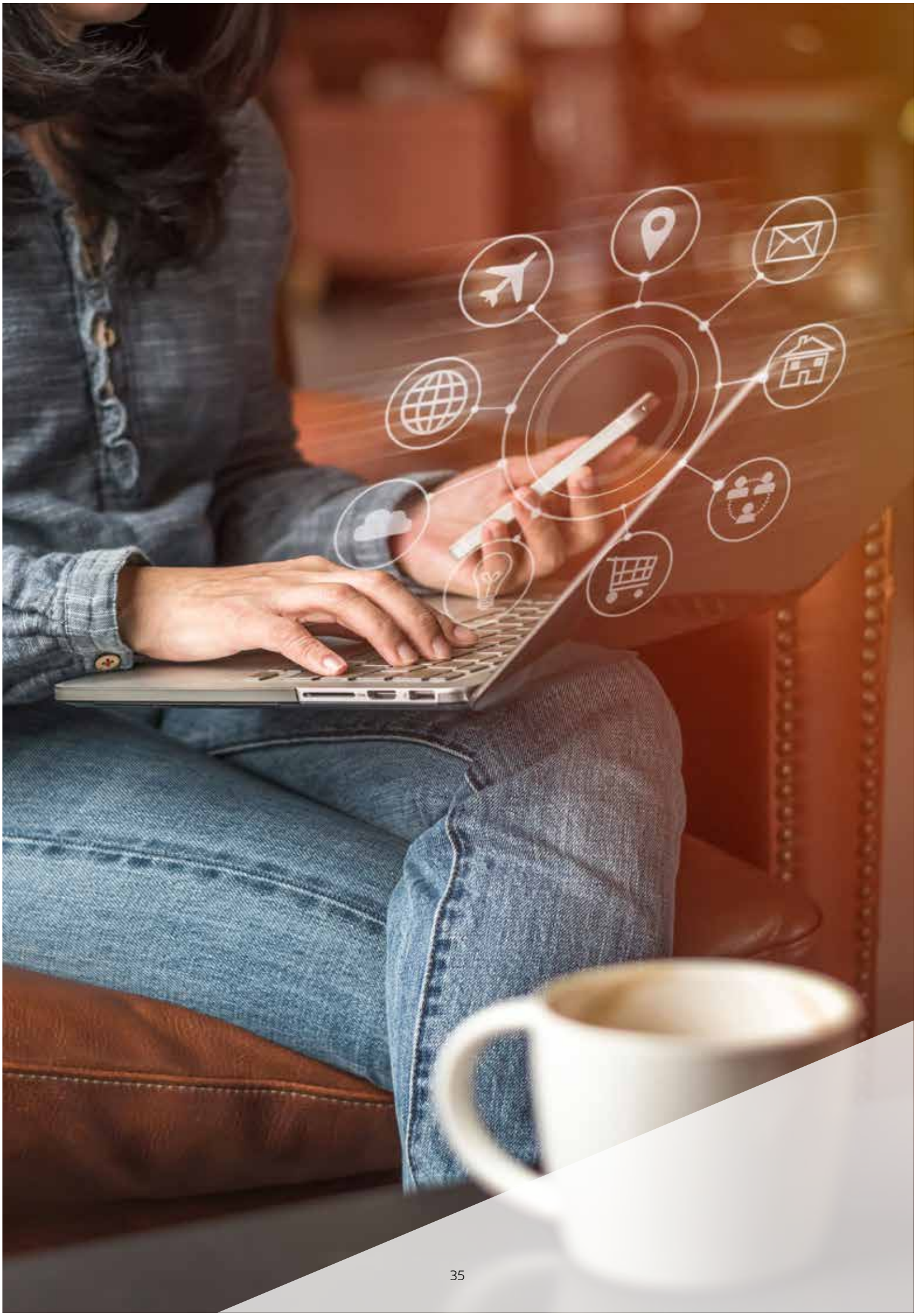
FT 05	Preparedness and continuity management
Requirement	1) Premises or buildings that contain information to be kept secret or critical information, information systems or other network infrastructure are protected from fire, water damage, explosion, unrest and other threats caused by the nature or people with structural, technical and organisational security measures. 2) At least the following security measures are implemented to protect the essential infrastructure: a) Structural security measures: Structural fire protection (fire resistance of wall, floor, ceiling and door/window structures and sealing of lead-throughs with products matching the fire resistance class). b) Technical security measures: i. Connection of the premises or building to a fire alarm system that alerts the emergency response centre. ii. The protected area is equipped with a ventilation system separate from the rest of the building and with automatic fire dampers (e.g., automatic smoke dampers). iii. The area is equipped with environmental condition, temperature and humidity detectors (mains current or pressure fluctuations, heat/coldness, water leaks) adequate with respect to the protected information. iv. Automatic extinguishing systems that detect a fire at an early stage and initiate first-aid extinguishing. v. Undisturbed electricity supply must be ensured with suitable equipment (UPS, reserve power). vi. Telecommunications backups, mirroring of information systems, backup copies and redundancy of the cooling system. c) Organisational security measures: i. Preparation of an emergency response plan. ii. A designated person in charge or party who receives information about alarms. iii. Regular emergency safety drills and fire safety inspections to verify compliance with fire safety regulations. iv. Continuity planning.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV
Security objective	The continuity of cloud service data centers (and similar spaces) is protected against common risks.
Additional information	Applicable security measures to promote continuity typically include the following: Structural protection: - Compartmentation to confine a fire or leak. - Use of fire-resistant materials (60 or 90 minutes, for example). - Fire seal products to prevent smoke and fire gases from entering other areas. Technical protection: - Regular testing and documentation of equipment. - Efficient functioning of processes and delivery of information to the right parties or individuals. - Emergency cablings and connections, doubling of systems, backup copy cycle and extent of backup copying. - Failures included in contingency planning concerning full availability of a) premises b) systems c) personnel. Organisational protection: - The purpose of the emergency response plan and continuity management is to describe the measures used to prevent, minimise, limit and recover from failures, accidents, damage and exceptional occurrences. - These plans should be updated at least annually. Critical servers and equipment must be identified and authenticated in accordance with the functional requirements. Cf. TJ 05 (Continuation management) and KT 03 (Backup copies). If the functional requirements on the system are high, the availability of systems must be secured against theft, vandalism, fire, heat, gases, dust, vibration, water and failures in electricity supply. Remote access is denied to HVAC automation management monitoring critical server and equipment spaces. Environmental sensors of critical server and equipment spaces are protected and controlled. The main infrastructure of the cloud service implementation should be placed in at least two separate locations.

Subdivision 5: Communications security

TT 01	Structure of the communications network
Requirement	1) The cloud computing environment is isolated from other environments. 2) Within the perimeter, the cloud computing environment is divided into separate areas (zones, segments, microsegments or similar). 3) Traffic is monitored and controlled so that only pre-authorised traffic essential for the operation is allowed (default-deny) at the perimeter of the cloud computing environment and between the internal areas.
Applicability	Network firewalls (or similar network devices, such as routers), software firewalls on workstations and servers, other systems in the cloud computing environment (including management).
Information types	Information to be kept secret, personal data, TL IV
Security objective	The purpose of limiting traffic in the service provision environment to necessary connections is to reduce the risk of attacks from unsecure networks and to limit the protected environment to a manageable size. The purpose of filtering between internal areas is to limit damage caused by possible security incidents (incl. security breaches) or attempts thereof and to improve detection of anomalies.
Additional information	The information processing environment processing protected information must be isolated from other environments. A correctly configured firewall or similar network device must be used for separation at the perimeter. The firewall (or similar network device) used for the separation must also be protected against unauthorised access. With regard to ensuring availability and adequate documentation, often the appropriate solution is backup copying of firewall settings and firewall configurations and adequate protection of the stored backup copies. The division of responsibilities between the service provider and customer should be considered in the interpretation of the requirement. If the purpose of assessment is to acquire a comprehensive picture of the adequacy of the protections concerning information to be kept secret, the assessment should, as a rule, cover the parts that are the cloud service provider's responsibility as well the parts that the customer is responsible for, throughout the life cycle of the information. The assessment should consider, for example, that in the IaaS model, the cloud service provider typically cannot take a stand on the security of the configuration of software firewalls that are the customer's responsibility. On the other hand, a customer typically cannot influence the protection measures for the IaaS infrastructure platform provided by the cloud service provider. If the customer has implemented software firewalls using a software component provided by the cloud service provider, the customer typically can influence only the security of the configuration implemented by the customer on the firewalls. Therefore, in this use case, it is recommended to ensure that the cloud service provider is responsible for the software components it provides also in case of security-related deficiencies in these software components that affect the protection of the customer's information to be kept secret. In these cases, it is recommended to also consider liabilities with respect to rectification of security defects and payment of damages. In situations in which the security of the infrastructure or, for example, traffic filtering relies on software code, particular attention must be paid to software code access and version control. Cf. MH 01 (Change management), MH 02 (System development) and KT 05 (Remote use and management). On the other hand, an implementation relying of software code may, with certain limitations, enable describing the environment and assessment of its security, supported by version management.

TT 02	Protection against common network attacks
Requirement	1) The cloud service provider must maintain a risk assessment procedure that takes into account protection against common network attacks. 2) The protection measures must be scaled so that common network attacks do not compromise the confidentiality, integrity or availability of the service or the information processed through the service.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV
Security objective	Access to the information processed by the cloud computing service is not prevented, or their confidentiality or integrity is not compromised as a result of common network attacks.
Additional information	All connected IT systems should basically be treated as untrusted and preparations should be done for common network attacks. Preparing for common network attacks also includes measures such as keeping only the necessary functionalities running. In other words, there should be a well-founded functional need for each functionality that is running. A functionality should be limited to the narrowest subset which fulfils the operational requirements (e.g., limitation of the visibility of functionalities). In addition, measures such as prevention of spoofing and limitation of the visibility of networks should be considered. Particularly at Internet interfaces, protection against (distributed) denial-of-service attacks must also be ensured. On the other hand, at some internal interfaces, the risk of denial-of-service attacks may be acceptable without specific protection measures. The division of responsibilities between the service provider and customer should be considered in the interpretation of the requirement. For instance, in the IaaS model, the cloud service provider typically cannot take a stand on questions such as the fault resiliency of the customer system's software layer or the security of the configuration of software firewalls that are at the customer's responsibility. On the other hand, in the SaaS model, the cloud service provider often has considerable responsibility for the management of the denial-of-service risk, for example.

TT 03	Management connections
Requirement	1) In the cloud computing environment, management access must take place through limited, managed and controlled points. 2) Management access must require strong user identification that is based on several authentication factors. 3) In remote use, management traffic must be encrypted with a approriate method, preferring validated and standardised encryption solutions/protocols. Cf. JT 08 (Encryption procedures and key management). 4) The management of classified information of the authorities may be possible only from terminal devices that match the protection level in question. 5) Remote access to management of classified information of the authorities may only be allowed through a management connection that is encrypted with a solution approved by the authorities. KT 05 (Remote use and remote management).
Applicability	Network devices and servers as well as workstations and other terminal devices. Covers the cloud computing platform and the customer system implemented on the platform.
Information types	1–3: Information to be kept secret, personal datapersonal data, TL IV 4–5: TL IV
Security objective	Management connections are protected at an adequate level, so that unauthorised access to customer data or the cloud service through the connections is prevented.
Additional information	The assessment of the protection of management connections should particularly consider the risk of disclosure of information processed by the cloud computing service through the management connection in question. Most management connection procedures enable access to information either directly (e.g., database maintenance usually can access the content of the database when necessary) or indirectly (e.g., network device maintenance usually can change the firewall settings that protect the information system). As a rule, any means of connection that can be used to alter the protection of information to be kept secret are considered to be management connections. Typically, management connections also include web consoles and other similar remote management connections provided for the cloud service customer. Cf. KT 05 (Remote use and remote management). Especially in situations in which the management connection provides a direct or indirect access to information to be kept secret, the management connection and the terminals connected to it should be kept at the same protection level as the information processing environment. Because of the security-critical nature of management traffic, the management of an environment used for the processing of classified data is not basically possible from environments or terminals with a lower level of protection. The so-called jump host procedure can be used to support adequate traceability; all management actions are executed and logged through the jump host. Remote management is described in more detail in requirement card KT 05 (Remote use and remote management).



Subdivision 6: Information system security

JT 01	Access rights management
Requirement	Access rights management must be based on the least privilege principle: a) A predefined process must exist for the creation, approval and maintenance of user accounts. b) Users of the information processing environment are only provided with the information, rights or authorizations that are necessary for them to perform their duties. c) A list must be kept of the users of the system. An entry (printed or electronic) must be made of all access rights granted. d) When granting access rights, it must be checked that the person receiving the rights is an employee or otherwise entitled. e) Instructions must be provided for the processing and granting of access rights. f) When user accounts and rights are no longer needed (e.g., a user leaves the organisation or a user account has not been accessed for a specified period of time), they must be deleted. g) A clear and efficient procedure must be in place for the immediate reporting of any changes in personnel to the relevant parties as well as an efficient procedure for making the required changes. h) Access rights must be regularly audited, at least every six months.
Applicability	Network devices and servers as well as workstations and other terminal devices.
Information types	Information to be kept secret, personal data, TL IV
Security objective	Access rights management is based on the least privilege principle: User credentials are granted and given only to those who have a right to receive them and need them in their job/role. Access rights are limited to the necessary functionalities, applications, equipment and networks.
Additional information	The division of responsibilities between the cloud service provider and the customer must be considered when applying this requirement. Typically, the cloud service provider is responsible for the access rights management of the system configuration related to the provision of the cloud computing service, while the customer is responsible for the access rights management of the part that is built on the service provider's service configuration (IaaS, PaaS or SaaS).

JT 02	User identification
Requirement	1) Users from the service provider's organisation involved in providing the cloud service as well as the customer's maintenance users must be identified and reliably authenticated before they can access protected information: a) They must use individual personal user identifiers. b) All users must be identified and authenticated. c) A well-known technique that is considered secure must be used for the identification and authentication, or the requirement must be covered in some other reliable way. d) User identifiers must be locked if authentication fails too many times in a row. e) The maintenance identifiers for systems and applications must always be personal. If this is not technically possible in all systems or applications, agreed and documented password management procedures enabling the identification of a user are required for identifiers in use by multiple persons. f) The authentication is performed within a physically protected area using at least the password. If password authentication is used, i. users have been instructed on good practices in the choice and use of a password, ii. the application that monitors access sets up certain minimum security requirements for the password and requires changing the password at appropriate intervals. g) Authentication of management connections in remote use must be strong, relying on at least two factors (e.g., password + token). The management connection must be encrypted with a appropriate method, preferring validated and standardised ncryption standards/protocols. Cf. JT 08 (Encryption procedures and key management). 2) In addition, the following applies to services processing classified information of the authorities: In situations in which the management connection passes outside the physically protect-ed area (e.g., between the cloud service provider's data center and the terminal of maintenance/the customer), the communication must be protected with an encryption solution approved by the authorities.
Applicability	Network devices and servers as well as workstations and other terminal devices.
Information types	1: Information to be kept secret, personal data, TL IV 2: TL IV
Security objective	Limiting access to information and services only to authorised users.
Additional information	Setting up a reliable identification and authentication procedure includes at least the following: 1) the authentication method is protected against man-in-the-middle attacks, 2) no additional information is disclosed in the login phase, before the actual authentication of the user, 3) the authentication credentials are always in an encrypted format if they are sent across the network, 4) the authentication method is protected against replay attacks, 5) the authentication method is protected against brute force attacks.

JT 03	Traceability and detection capability
Requirement	1) Reliable methods are in place for tracing security events. In particular: a) Records must be comprehensive enough to detect occurred or attempted security breaches afterwards. b) Essential records must be kept for at least six months, unless legislation or contracts specify a longer retention period. c) Log files and respective register services must be protected against unauthorised access (access rights management, logical access control) in accordance with the least privilege principle. d) Essential log files are sent from log sources to a separate log collector (or to separate log collectors). e) The transmission of log files between the log sources and log collector must be protected. The parties to the transmission must be identified. Log files being transferred must be encrypted with a appropriate method, preferring validated and standardised encryption solutions/protocols. Cf. JT 08 (Encryption procedures and key management). Alternatively, log files can be transmitted through a specific management network. f) Clocks are synchronised to the agreed reference time source. 2) At the customer's request and concerning the system components included within the cloud service provider's area of responsibility, the service provider provides the log files in such a format that the customer may study the cases affecting the customer. 3) The cloud service provider offers the possibility (technical interface) for real-time information exchange with the customer (log files, event data, security findings). 4) Reliable methods are in place for the detection of security incidents. In particular: a) A procedure is in place to detect anomalies on logs (see KT 04) (in particular, an unauthorised attempt to use the information system must be detected). b) The baseline of the network traffic (volume of traffic, protocols and connections) is known. c) A procedure exists to detect abnormal events in the network traffic (e.g., abnormal connections or attempts for such). d) A procedure is in place to recover from detected incidents.
Applicability	The overall security of the service provided.
Information types	Information to be kept secret, personal data, TL IV
Security objective	Detection of any unauthorised alteration to information or other unauthorised or inappropriate information processing, including detection of security breaches and support for the planning of corrective measures.
Additional information	Traceability refers to recording the events of the system environment so that, in an incident, it is possible to find out what measures had been taken in the environment and by whom, and what effects such measures have had. Essential records typically include the log data of central network devices and servers. In addition, log data of workstations, etc. are also very often covered by this. The coverage requirement can in most cases be met by checking that logging is on at least for workstations, servers, network devices (especially firewalls, but also for software firewalls on workstations). It should be possible to afterwards check from the network device logs as to what management functions were performed on the network devices, when and by who. Event logs should be compiled of the use of the system, user activities as well as security-related functions and exceptions. A recommended method to protect the logs is to forward all essential logging information to a strongly safeguarded logging server (or servers), the information content of which is regularly backed up. To support the legal protection of administrators and promote investigation of suspected security breaches, it is recommended to separate tasks so that the logging data maintenance duty is separated from other maintenance duties. The functioning of logging data storage and surveillance software must also be monitored. In practice, in most environments, automatic observation and alarm tools are required to be able to detect misuse attempts. Manual viewing of logging data is usually sufficient only in environments in which the logging data mass is very small and there are enough human resources to be allocated to checking of logs. The restoration of an information processing environment to a protected state within reasonable time usually requires planned, described, trained and rehearsed processes and technical methods. There are many solutions available for monitoring network traffic and limiting the effects of a detected attack, ranging from monitoring at the network node level to workstation/server sensors and combinations of these. Regardless of the network devices or operators, the actual capability to detect changes at the network level typically requires understanding the baseline of the network traffic.

JT 04	Systems hardening
Requirement	1) A procedure is used through which systems are installed systematically, resulting in a hardened configuration. 2) A hardened configuration contains only such components, services, user and process rights which are mandatory in order to fulfil the operational requirements and ensure security.
Applicability	Equipment and software related to the provision of cloud computing service. When processing classified information of the authorities, this also covers the terminal devices used for management, including their background systems (e.g., directory services).
Information types	Information to be kept secret, personal data, TL IV
Security objective	Reduces the risk of software flaws and faulty configurations by removing from use functionalities that are not needed.
Additional information	Writing secure software code has turned out to be challenging. The more software code an environment includes, the higher the risk of software flaws, that is, vulnerabilities. The higher the number of services relying on the security of software code, the more probable it is that the services also include vulnerabilities. Risks can be reduced by reducing the attack surface, that is, by exposing only the necessary services to attacks. Systems are usually full of features. These features are usually on by default and easy to take into use. On the other hand, these features are also often run with too vulnerable settings. If unnecessary features are not removed from use, a malicious party can also access them. If the too vulnerable settings of unnecessary services are not changed, they are also accessible to malicious parties. By default, systems often include e.g. predefined administrator passwords, preinstalled unnecessary software and unnecessary user accounts. Security hardening of the system means, in general terms, making changes to the settings to reduce the system's attack surface. In general, only functions, equipment and services that are essential to meet the service requirements should be taken into use in systems. Similarly, for instance, automated processes should be only provided with data, rights or authorisations that are necessary to perform their tasks in order to limit damage caused by accidents, errors or unauthorised use of system resources. Configuration management tools can often also be used for security hardening and its maintenance.

JT 05	Separation of data
Requirement	Customers' information to be kept secret are kept reliably apart in shared virtual or physical systems.
Applicability	Network devices, storage systems, memory, transmission media, etc. related to the processing of customer information to be kept secret.
Information types	Information to be kept secret, personal data, TL IV
Security objective	Customers' information to be kept secret can only be accessed by the customer in question.
Additional information	If the same equipment is used for simultaneous processing of several customers' data, adequately secure physical and logical isolation of the data must be ensured. If adequate assurance of this cannot be obtained, separate physical devices must be used for the processing of data. For instance, classified information can be kept on a physically separate virtualisation platform, where potentially vulnerable processor interfaces can only be accessed by the authorised users of classified information. If the same equipment is used for the processing of several customers' data, but not simultaneously, adequately secure removal of the previous customers' data from the equipment must be ensured (e.g., all parts, BIOS, cache memories of various other devices). If adequate assurance of this cannot be obtained, separate physical devices must be used for the processing of data. Cf. TA 03 (Data destruction). The separation must be adequately reliable, using either logical and/or physical separation methods. Encryption is a common separation method for shared network devices and storage systems, for instance. The customer-specific keys used for the encryption of communications (data-in-transit) and storage (data-at-rest) can also be used to support other security objectives, such as the secure disposal of equipment. Cf. TA 02 (Encryption within a physically protected area) and KT 03 (Backup copies). The owners of classified information to be kept secret may reserve themselves the right to audit all networks/systems in which their information is kept. The audit often requires physical or logical access to the environment to be audited. Therefore, it is often technically possible for the auditors to also access data processed at that environment. Especially in environments with a need to process information of multiple owners, it should be ensured that the design of the network/system enables audits without enabling owners of information to access each other's information during the audits. Particularly with the IaaS and PaaS service models, secure separation must be ensured physically with separate networks or encrypted virtual or software-based local networks. Cf. TA 02 (Encryption within a physically protected area).

JT 06	Protection against malware
Requirement	Reliable methods for the prevention and detection of, resilience against and recovery from malware threats are established for the cloud computing service, including the system environments used for the management of the cloud service.
Applicability	Systems used for the provision of the cloud computing service, including the system environments used for its management.
Information types	Information to be kept secret, personal data, TL IV
Security objective	The integrity, confidentiality or availability of customer data are protected at an adequate level against common malware risks.
Additional information	The methods for protection against malware risks include security hardening of systems (cf. JT 04), limitation of access rights (cf. JT 01), keeping systems up-to-date with security updates (cf. KT 04), incident detection (cf. JT 03), ensuring the personnel's security awareness (cf. HT 04) and also use of anti-malware software. Risks can also be mitigated by separating high-risk environments from other production environments and, for instance, restricting the use of portable media devices, such as USB memories.

JT 07	Transfer and removal of protected information
Requirement	1) Equipment, software, transmission media, etc. may be transferred outside physically protected premises only with specific authorisation. 2) Transfer and processing of information outside physically protected premises must be carried out according to the classification of the information being transferred. 3) The principles of secure remote use must be applied when transferring a customer's information to be kept secret. KT 05: Remote use and remote management).
Applicability	Equipment that contains customer data.
Information types	1–2: Information to be kept secret, personal data, TL IV 3: TL IV
Security objective	Protected customer data are not compromised when transferred outside of physically protected areas (e.g., data centers).
Additional information	In particular: • Secure deletion of data and destruction of the data storage medium. • Encryption of removable storage media. • Transfer of data to a new data storage medium when the data storage medium is replaced.

JT 08	Encryption procedures and key management
Requirement	1) The processes of encryption procedures and encryption key management are designed, implemented and documented. 2) Secret keys can be used by authorised users and processes only. The processes require at least a) cryptographically strong keys, b) secure key delivery, c) secure key storage, d) regular key changes, e) changing of outdated or compromised keys and f) prevention of unauthorised key changes. 3) In the protection of classified information of the authorities, the encryption procedures, algorithms and cryptographic products must be approved by the authorities.
Applicability	Direct or indirect protection of customer data when the protection is carried out by encryption.
Information types	1–2: Information to be kept secret, personal data, TL IV 3: TL IV
Security objective	The use of encryption methods provides an adequately reliable level of protection.
Additional information	Several aspects must be taken into account in the assessment of encryption solutions. In addition to verifying the strength of the algorithm and the correct functioning of the encryption solution, also the threat level of the user environment must be taken into account. For instance, in traffic across the Internet, the threat level is considerably higher compared with transferring encrypted information within a managed and protected physical area. Other aspects to be taken into account when evaluating the encryption solution include requirements of the use case on the secrecy period and integrity of the information. The protection effect of encryption may be fully or partially lost in situations in which the weaknesses of key management can be exploited by unauthorised parties. Cf. TA 01 (Encryption outside a physically protected area) and TA 02 (Encryption within a physically protected area). More information is available from the National Cyber Security Centre.

Subdivision 7: Data security

TA 01	Encryption outside a physically protected area
Requirement	1) When transferring a customer's information to be kept secret outside approved physically protected areas (e.g., the service provider's data center) or through a network with a lower security level, the information to be kept secret is encrypted with a appropriate method, preferring validated and standardised encryption solutions/protocols. Cf. JT 08 (Encryption procedures and key management). 2) Classified material of the authorities is encrypted using a method approved by the authorities (cf. JT 08).
Applicability	Encryption solutions between data centers, encryption solutions for traffic through other networks with a lower protection level.
Information types	1: Information to be kept secret, personal data, TL IV 2: TL IV
Security objective	The confidentiality or integrity of customer data is not compromised in transfer through unreliable networks.
Additional information	The Internet as well MPLS networks provided by operators and so-called dark fibres are considered public networks. Use of a radio interface on wireless network connections (e.g., WLAN, 3G) is interpreted as exiting a physically protected area. In other words, use of the radio interface is considered equal to traffic through public networks, which should be taken into account particularly in the encryption of traffic.

TA 02	Encryption within a physically protected area
Requirement	1) When a customer's information to be kept secret is transferred within approved physically protected areas and within a network of the same security level, lower-level encryption or unencrypted transfer may be used, provided that adequate protection of the information can be achieved by means of physical protection. Cf. JT 05 (Separation of data). 2) Customers' information to be kept secret must be saved in the cloud computing service in an encrypted format if shared equipment is used. Cf. JT 05 (Separation of data). 3) Encryption keys must be separated on a customer-specific basis. 4) Classified material of the authorities is encrypted using a method approved by the authorities (cf. JT 08).
Applicability	Customer data processing environments in a cloud computing configuration, including disk system and backup solutions.
Information types	1–3: Information to be kept secret, personal data, TL IV 4: TL IV
Security objective	Supporting the separation protection of different customers' information with technical encryption methods when information of different customers is processed on shared equipment. Implementation of multilevel protection, supporting protection throughout the life cycle.
Additional information	2: Does not apply to metadata related to invoicing or other management of customer relationships. Generally, it should be kept in mind that, as a rule, the cloud service provider always has access to the information processed in the service if the information during its life cycle exists in its decrypted format (e.g., an image shown to customers). For instance, common solution models that are based on the use of own keys (BYOK, Bring Your Own Keys) or equipment-based security modules placed in the service provider's physical data center (HSM, Hardware Security Model) limit but do not typically prevent the cloud service provider's access to the information processed by the service. However, encryption can be used for supplementary protection to support, for instance, the separation of the data of different customers, the destruction process of assets or separation of duties. Cf. JT 05 (Separation of data). Encryption is often particularly advisable for the combination of the scalability of cloud computing services and customer-specific separation.

TA 03	Data destruction/disposal
Requirement	1) The destruction of data materials is reliably arranged. The destruction methods used prevent full and partial recovery of the data. The destruction must cover the entire life cycle of the information to be kept secret insofar as the information has resided in cloud computing service. 2) A customer's information to be kept secret must be reliably destroyed particularly in the following cases: a) The customer requests destruction of their data. b) The customer's agreement expires. c) Equipment servicing, maintenance and replacement (e.g., replacement of a broken disk that contains information to be kept secret of the customer).
Applicability	Storage media and similar systems that have contained protected information of a customer.
Information types	Information to be kept secret, personal data, TL IV
Security objective	The confidentiality of a customer's information to be kept secret is not compromised when storage media or similar systems used for the processing of the information are taken out of use or access of the cloud service to the customer data must be prevented for other reasons.
Additional information	<u>Shredding</u> Shredding of materials can be performed as follows, for instance: – maximum particle size of shredded paper is 30 mm2 (DIN 66399/P5 or DIN 32757/DIN 4), – maximum particle size of shredded magnetic hard disks is 320 mm2 (DIN 66399/H-5), – maximum particle size of shredded SSD disks and USB memories is 10 mm2 (DIN 66399/E-5), and – maximum particle size of shredded optical media is 10 mm2 (DIN 66399/O-5). With the above particle sizes, shredding waste can be disposed of as normal office waste. <u>Overwriting</u> Information may be destroyed also by overwriting the storage areas that contained a customer's information to be kept secret. Particular attention must paid to the applicability of the overwriting method used for the storage medium in question, as well as the process and the parties responsible for the process. More information on destroying electronic materials is available in the guideline by the National Communications Security Authority (available in Finnish: www.ncsa.fi > Ohjeita > "Kiintolevyjen elinkaaren hallinta - Ylikirjoitus ja uusiokäyttö"). <u>Combined methods</u> Other methods in addition to shredding may also be used for enhanced protection to ensure that the destroyed information cannot be recovered (e.g., burning shredded material or melting hard disks). The possibility to recover documents depends also on the amount of shredded material handed over to external parties. Encryption can also considerably reduce the risks associated with information to be kept secret in the different life cycle phases of information and equipment. If information to be kept secret is stored in the cloud only in an encrypted format that has been assessed to be adequately reliable (cf. TA 02: Encryption within a physically protected area), residual risks may be acceptable for some data types if the set of keys used for the encryption can be reliably destroyed. <u>Details to be taken into account when destroying electronic materials</u> Procedures for the reliable destruction of electronic materials in particular should cover any equipment on which information to be kept secret has been stored during its service life. Reliable destruction of information to be kept secret contained by equipment components (hard disks, memories, memory cards, etc.) must be ensured particularly when a device becomes obsolete, is sent to be serviced or is included in a recycling process. If reliable deletion (such as an overwriting procedure approved by the authorities) is not possible, a component containing information to be kept secret cannot be delivered to a third party. If reliable erasure of the memory content of a device is not possible before servicing, servicing by a third party should be carried out under supervision to ensure that information to be kept secret is not disclosed during the work. Cf. Reduction of residual risks by encryption (TA 02: Encryption within a physically protected area).

Subdivision 8: Operations security

KT 01	System description to promote continuity and operations security
Requirement	1) Comprehensive system descriptions must exist of the cloud computing service as well as instructions for secure maintenance and management of the service. The descriptions and instructions must be at such a level that it is possible to credibly avoid errors during use and ensure recovery from disruptions pursuant to contractual obligations. 2) The system descriptions and instructions must be kept up-to-date. 3) The system descriptions and instructions must be implemented in practice for the personnel and made available according to role.
Applicability	The cloud computing service as a whole.
Information types	Information to be kept secret, personal data, TL IV
Security objective	The objective is to avoid failures during use and ensure recovery from disruptions pursuant to contractual obligations.
Additional information	In particular, if an important system component of the cloud computing service fails, adequate documentation of the system must exist to support the restoration of service. The documentation must be accessible to those individuals who need them for recovery measures. The documentation also provides support when key persons are unavailable to rectify an abnormal situation. Adequate documentation and instructions must also exist for situations in which the customer or a third party authorised by the customer maintains or develops a customer system on the cloud service platform. Continuity can also be supported by means such as automated correction of failures (e.g., restart of containers).

KT 02	Capacity management
Requirement	1) The capacity of the cloud computing service is designed so that the service level pursuant to the service level agreements can be reliably provided. The design must include monitoring of the actual capacity need as well as forecast for future capacity needs. 2) A cloud computing customer is able to supervise and monitor the distribution of the system resources provided (e.g., data processing or storage capacity) to prevent congestion of resources.
Applicability	The cloud computing service as a whole.
Information types	Information to be kept secret, personal data, TL IV
Security objective	The objective is to be able to reliably provide the service level specified in service level agreements.
Additional information	Monitoring of capacity demands helps the assessment of future needs and optimisation of utilisation rate as well as fulfilment of obligations pursuant to service level agreements.

KT 03	Backup copies
Requirement	1) Backup and recovery processes are designed, implemented, tested and documented as part of the contingency plan, so that the obligations pursuant to service level agreements and law as well as other business requirements of the cloud service can be fulfilled. In particular: a) Backup frequency is adequate considering the criticality of the data being backed up. Requires determining how large data loss is tolerated (recovery point objective, RPO). b) The speed of the recovery process is adequate for the operational requirements. Requires determining how quickly recovery is required to be executed (recovery time objective, RTO). c) The correct functioning of backup copying and the recovery process is regularly assessed through testing. d) The physical location of backup copies is adequately isolated from the actual system (separate sag/fire space, sufficient distance between backups and the system space.). 2) Backup copies are protected throughout their life cycle with methods of at least the same level as the original data. A large quantity of data may require stricter protection (aggregate effect). In particular: a) Access to backup copies is limited in accordance with the least privilege principle to approved individuals or roles. b) The backup and recovery processes are traceable (logging) and controlled so that it is possible to detect unauthorised activity (e.g., unauthorised recovery runs). c) When backup copies are kept in a different physical location, the management of physical and logical access to this location must be at least at the same level. d) When backup copies are transferred outside the physically protected area (e.g., to another data center of the cloud service provider) through a network, the information/communication must be encrypted with a appropriate method, preferring validated and standardised encryption solutions/protocols. Cf. JT 08 (Encryption procedures and key management). e) When backup copies are transferred outside the physically protected area on a transmission media (e.g., backup tapes or disks), the transmission media is transferred under continuous supervision. It is recommended to encrypt the transmission media or the data it contains. f) Backup media must be reliably destroyed (cf. TA 03: Data destruction). 3) For backup copies containing classified information of the authorities, the following must also be taken into account: a) When backup copies are transferred outside the physically protected area (e.g., to another data center of the cloud service provider) through a network, the information/communication must be encrypted with an encryption solution approved by the authorities. b) When processing data of different owners in the same backup system, separation procedures (e.g., encryption and/or physically separate storage systems and media) must be implemented for backup system interfaces and storage media. Cf. JT 05 (Separation of data) and TA 02 (Encryption within a physically protected area).
Applicability	Cloud service backup and recovery processes. Situations in which some processes depend on the implementation of the customer system must also be taken into account.
Information types	1–2: Information to be kept secret, personal data, TL IV 3: TL IV
Security objective	Protection of the availability, integrity and confidentiality of customer data in the backup and recovery processes.
Additional information	Recovery testing may also be automated to be run once a week, for example. Recovery of data must also be protected at least at the same level as the original data.

KT 04	Vulnerability management
Requirement	Reliable methods are implemented for the entire life cycle of the cloud computing service to manage software vulnerabilities. In particular: a) Security bulletins of the authorities, equipment manufacturers, software suppliers and other similar parties are followed and security updates deemed necessary based on a risk assessment are installed in a controlled manner (cf. MH 01: Change management). b) The systems are automatically checked for known vulnerabilities at least once a month. If the planned settings or the security update level are departed from, the reasons are analysed and any deviations are corrected or documented in accordance with the security incident management process (see TJ 04: Management of security incidents). c) Components essential for the secure operation of the cloud computing service are regularly (at least once a year) tested using penetration tests of an independent party. Any significant deviations from normal are immediately corrected. d) The cloud service customers are informed about any significant vulnerabilities and their effects on the protection of customer data. Communication is particularly important in situations in which vulnerability management requires measures of the cloud service provider and the customer alike.
Applicability	The software and equipment included in the cloud computing service configuration.
Information types	Information to be kept secret, personal data, TL IV
Security objective	Keeping software vulnerability-related risks at a tolerable level.
Additional information	Writing secure software code has turned out to be challenging. Many types of attacks exploit software failures, or vulnerabilities, to some extent. Responsible suppliers fix vulnerabilities found in their software products. Risks can be reduced by installing patches. Vulnerability management involves continuous monitoring and development of the system environment, so that software suppliers' vulnerability patches can be installed as quickly as possible. In addition, software supplier's support for used software versions should be followed. No active updates are published for outdated software versions, which means that it may be impossible to patch security vulnerabilities. The effects of vulnerability patching on the service must be taken into account. If patching causes an interruption to the customer's service, it is recommended to schedule it so that inconvenience to the customer is minimised or to perform patching during a previously agreed service break. It may be advisable to test the patches first in a test environment to ensure that the patches do not cause unexpected changes in the service. Active vulnerability management can be carried out by • clearly establishing responsibilities and division of duties for patching vulnerabilities, • monitoring system development and the security status of any software used for the provision of service, and • agreeing on continuous monitoring procedures, e.g., by scanning one's own environment to detect known vulnerabilities. b: The check covers all systems which the system as a whole interfaces with. Programmed vulnerability scans or configuration management databases (CMDB) or similar can be utilised in the check. The installation of security updates may also use a method in which a reliable 'golden image' that is up-to-date with the security updates is maintained for the virtual machines, and the virtual machines in use are regularly replaced with this up-to-date 'golden image'. In this solution, particular caution must be exercised with methods aiming to ensure the integrity of the golden image.

KT 05	Remote use and remote management
Requirement	1) The remote use and remote management solution for a system requires strong user authentication that is based on at least two factors. 2) The remote use and remote management traffic is protected with a appropriate method, preferring validated and standardised encryption solutions/protocols. Cf. JT 08 (Encryption procedures and key management). 3) Remote management is possible only through a centrally managed and controlled point, a so-called jump host. 4) If data storage media (hard drives, USB memories, etc.) containing customer data are taken outside of the approved physically protected areas and they are not encrypted with a appropriate method, preferring validated and standardised encryption solutions/protocols, the data storage media are kept under a similar level or protection, such as locked office furniture of an administrative security area, or the data storage media are not left unattended. Cf. JT 08 (Encryption procedures and key management) and FT 01 (Defence-in-depth and risk management). In addition, when handling classified information of the authorities: 5) Equipment and remote connections used must be approved for the environment and match the protection level. 6) Remote use and a remote management solution require encryption of traffic with a method approved by the authorities for the protection level in question. 7) The encryption of data storage media must be approved by the authorities.
Applicability	Systems used for the remote use and remote management of cloud computing service systems, including terminal devices.
Information types	1-4: Information to be kept secret, personal data, TL IV 5–7: TL IV
Security objective	Remote use and remote management connections are protected at an adequate level, so that the connections do not enable unauthorised access to customer data or the cloud computing service.
Additional information	Remote use/management refers to the use/management of information systems outside physically protected areas or through an untrusted network. Normally, the terminal device is a portable computer of an employee provided by the organisation. In a cloud computing environment, remote management is usually the most typical management method for the actual cloud computing platform and the customer's systems alike. For instance, the cloud service provider's maintenance measures carried out from outside the physically protected data center are considered as remote management. In addition, the cloud service customer's maintenance measures performed on a part of the system that the customer is responsible for are also considered as remote management. Another example of remote use is the customer using a terminal device to use a system located in the cloud service. The so-called jump host procedure can be used to support adequate traceability; all management actions are executed and logged through the jump host. The management of a cloud computing platform that contains classified information must be limited to terminal devices that meet the security requirements for the protection level in question. It should also be noted that the terminal management solutions must also meet the security requirements of the protection level in question.

Subdivision 9: Transferability and compatibility

SI 01	Transferability and compatibility
Requirement	1) The application programming interfaces (API) of the cloud computing service must be published so that they enable interoperability with different software components and software products. 2) The cloud computing service must support commonly used formats for software transfer (such as Open Virtualization Format, Docker, Kubernetes or similar). 3) Upon the customer's request, the service provider must deliver the customer's data in an applicable, accessible and generally compatible format. The formats must be documented at an adequate level in agreements signed with the customer. 4) Secure, well-established network protocols must be used for the import and export of data as well as the administration of the service, so that the confidentiality, integrity and availability of the transferred data can be ensured. 5) Encryption solutions approved by the authorities must be used for transfers of the classified information of the authorities.
Applicability	The cloud computing service as a whole.
Information types	1-4: Information to be kept secret, personal data, TL IV 5: TL IV
Security objective	It is possible for the customer to change the cloud service provider and use a number of cloud service providers for the implementation of the customer's service. The transfer of customer data does not compromise the confidentiality, integrity or availability of the data.
Additional information	Case-specific assessment is required on how reasonable it is to require transferability in situations in which a service implemented in the cloud computing service uses the characteristics of the cloud computing platform in question for the implementation of the service. As a rule, however, it is always reasonable to require transferability of customer data (such as the content of a customer register stored in a database) in some easily machine-processable format.

Subdivision 10: Change management and system development

MH 01:	Change management
Requirement	1) A change management procedure that takes security into account is in place for changes made to the cloud computing service. The change management procedure also takes compliance (cf. TJ 07) and contractual obligations into account. 2) Risks associated with changes are assessed and submitted for approval to the applicable parties. 3) All changes are tested before their introduction into the production environment. 4) Testing environments are isolated from production environments. 5) Testing is designed and implemented so that it provides a reliable picture of the effects of the change before it is installed in the production environment.
Applicability	The cloud computing service as a whole.
Information types	Information to be kept secret, personal data, TL IV
Security objective	The confidentiality, integrity or availability of information processed through the cloud computing service are not compromised as a result of changes made to the service.
Additional information	The following procedure may support the fulfilment of the requirements: 1) Processes are specified for rolling back of changes in case of failures or security problems and the restoration of the affected systems or services to the state preceding the changes. 2) Before introducing a change into the production environment, the success of the planned tests is evaluated and the granting of required approvals is checked. 3) In emergencies (such as a major equipment failure or security breach), a lighter change management process can be used, provided that the security effects of the changes are analysed afterwards to the same extent as in the normal process (typically, within a week of the changes at the latest). 4) The isolation of the testing environment from the production environment is reliably implemented with either physical or logical isolation methods to avoid unauthorised access and changes to the production environment and data. To protect the confidentiality of data, production data are not transferred into development or testing environments. 5) Change management procedures involve role-based rights to ensure appropriate separation of duties in the development and deployment of changes as well as the transfer of changes between environments.

MH 02:	Systems development
Requirement	1) Applications and application programming interfaces (APIs) are designed, developed, tested and deployed in accordance with good security practices of the industry. 2) The production environment is isolated from the other environments (e.g., development, testing and quality assurance environments). 3) The security of version management is taken into account at least so that the procedures reliably prevent the transfer of unauthorised versions into the production environment. 4) The practices of secure software development process are implemented in each part of the organisation that has anything to do with the software in question. 5) In situations in which the design, development, testing or provisioning of the source code of the cloud computing service (or part thereof) is outsourced, agreements must particularly take into account the following: a) The requirements of a secure software development process (particularly with respect to design, development and testing), b) evidence of adequate testing, c) acceptance testing according to the agreed operational and non-operational requirements, and d) the right to test the development process and monitoring measures, also as spot checks.
Applicability	System development related to the cloud computing service configuration.
Information types	Information to be kept secret, personal data, TL IV
Security objective	The confidentiality, integrity or availability of information processed through the cloud computing service are not compromised as a result of system development performed on the service.
Additional information	1: Security procedures are provided by, for example, OWASP for web applications and system development life cycle models (SDLC, Systems Development Life Cycle). 5: Cf. TJ 08 (Security of service providers and suppliers).

Annex 1: Examples of application of the criteria

Example 1:
Customer system implemented as IaaS service

This is a compact example of how the criteria can be applied in a situation in which a customer system has been implemented applying the IaaS service model on the provided cloud computing service platform. In this example, the customer is Official V, who wants to assess the capacity of their recently completed customer system for the protection of class IV classified information. The planned users of the customer systems are V's employees. Other parties present in this example are cloud service provider P and company Y, which engages in the development and maintenance of the system by assignment of V.

In this case, use of the criteria can be divided into two use cases. The first use case concerns the cloud computing platform applying IaaS model. The second use case concerns the customer system implemented on the platform.

Security of the cloud computing platform

The security of the cloud computing platform can be divided into the administrative and personnel security domains and the physical and technical security domains of service provider P. If the stack model of Figure 1 (page 8) is used as reference architecture, technical security responsibilities typically reach up to the virtualisation platform and provisioning service interfaces. Security responsibilities for the upper layers lie with the cloud computing customer. In this example, the responsibilities of customer V also include company Y, which develops and maintains the customer system for V.

This means that security maintenance of the network devices as well as the storage and backup systems included in the cloud computing platform constitute part of the assessment of the cloud computing platform. In addition, encryption of communication between data centers and access rights management of cloud computing platform maintenance are typically part of the assessment of the cloud computing platform. Assessment of the cloud computing platform typically also includes arranging secure remote management connections for maintenance measures carried out by the cloud service provider P and for the provisioning needs of the customer's representatives (V and Y).

In this example, the National Communications Security Authority (NCSA) has recently assessed the security of the IaaS platform provided by P. The official V discusses the observations made during the assessment with the NCSA and cloud service provider P. V decides to use the observations of the recent assessment directly in its own risk assessment and does not have a specific assessment performed on the IaaS platform.

Security of the customer system

In the stack model described above, layers from the virtual machine on are the responsibility of the official V acting as the customer. Measures such as installing the virtual machine operating system from a reliable source, security hardening of the operating system and its updating procedures, are typically the responsibility of the cloud service customer. In addition, the customer is also responsible for the security of the software running on the operating system as well as the management connections for its maintenance.

In this example, the official V is responsible for the protection of its own data processing system and also responsible for protection on behalf of Y, who is working for V. The responsibilities cover the administrative security of the processing of classified information, personnel security as well as physical and technical security. Responsibilities related to technical security include, for instance, terminal devices used for the development and maintenance of the customer system as well as their management solutions. In this example, the official V has recently assessed its own security and the security of Y against the Katakri 2015 framework and focuses its assessment only on technical protection of the customer system, including maintenance procedures.

Special cases

Some cloud service providers offer software developed by the cloud service provider for the protec-

tion of the customer system. For instance, it may be possible to implement firewalling, backup or logging arrangements of the customer system using the cloud service provider's software components. In such cases, case-specific definition of responsibilities is required. For instance, if a software component of the cloud service provider could not provide adequate protection for a reason such as a software failure, there should be a specification in place indicating whether this is the responsibility of the cloud service provider or the customer.

The functionality, availability and security of customer systems may consist of a number of components. Interdependencies between different components may have great significance, particularly for the use of cloud computing services. For example, availability of the service may be affected by the internal functionality of software components that are the customer's responsibility, the internal functionality of software components of the cloud service provider's service platform, or combinations of their functionalities.

Example 2: A customer system implemented as SaaS

This is a compact example of how the criteria can be applied in a situation in which a customer uses the cloud service provider's software provided as SaaS. In this case, use of the criteria can be divided into two use cases. The first use case concerns the SaaS service configuration. The second use case concerns the security of the service settings and secure use of the service configuration.

Security of the service configuration

The security of cloud service configuration provided as SaaS can be divided into the cloud service provider's administrative and personnel security as well as physical and technical security. If the stack model of Figure 1 in chapter 'Cloud computing service models' is used as reference architecture, technical security responsibilities typically reach up to the level of the application layer programming interfaces and the operating system. The customer's security responsibilities are typically related only to secure configuration and use of the service.

Security of the settings and secure use of the service configuration

Possibilities to establish different service configurations vary considerably depending on the service provider and the functionality of the service configuration in question. For instance, the access rights management of users of the service configuration as well as choices of authentication procedures are typically the customer's responsibility. In addition, the customer is responsible for the security of the terminal devices used for the configuration of the service settings.

Annex 2: Assessment and accreditation by the competent authority

Background

Pursuant to the Act on the Assessment of the Information Security of Public Authorities' Information Systems and Telecommunications Arrangements (1406/2011)[17], the authorities may use only the Finnish Transport and Communications Agency Traficom, or an Information Security Inspection Body accredited by Traficom, for the assessment of its information system security[18]. PiTuKri can be used as a tool when assessing how a cloud computing-based information system used or planned for the use of the authorities fulfils the national or international security requirements[19].

This Annex describes different PiTuKri use cases in the assessment of cloud computing-based information systems. The description focuses on the use cases of facility security clearance and assessment of authorities' information systems, in which Traficom is the competent authority. The description covers the assessment and accreditation processes as well as the accreditation by a compenent authority. The description does not address other use cases, such as use as part of the organisation's internal security work.

Assessment process

Assessment process for the security of information systems (L 1406/2011) begins when the target of the assessment submits an assessment request to Traficom. Other main phases of the assessment process are planning of assessment, inspections and reporting. The assessment process is visualised in a simplified form in Figure 2. The assessment process may be used for purposes such as supporting the internal security work of the target organisation, with the addressing of residual risks completely within the responsibility of the target organisation. The assessment process is described in more detail in the guideline on the NCSA's information security assessments from the customer organisation's perspective (in Finnish only)[20].

Figure 2. Simplified assessment process

[17] Act on the Assessment of the Information Security of Public Authorities' Information Systems and Telecommunications Arrangements (1406/2011), https://www.finlex.fi/fi/laki/alkup/2011/20111406. Laki liikenne- ja viestintäministeriön hallinnonalan virastouudistuksen täytäntöönpanoa sekä virastojen tehtävien uudelleenorganisointia koskevan lainsäädännön voimaanpanosta (937/2018) (Act on the execution and implementation of certain reforms and reorganisation within the administrative branch of the Ministry of Transport and Communications), https://www.finlex.fi/fi/laki/smur/2018/20180937.

[18] Act on Information Security Assessment Bodies (L 1405/2011), https://www.finlex.fi/fi/laki/ajantasa/2011/20111405.

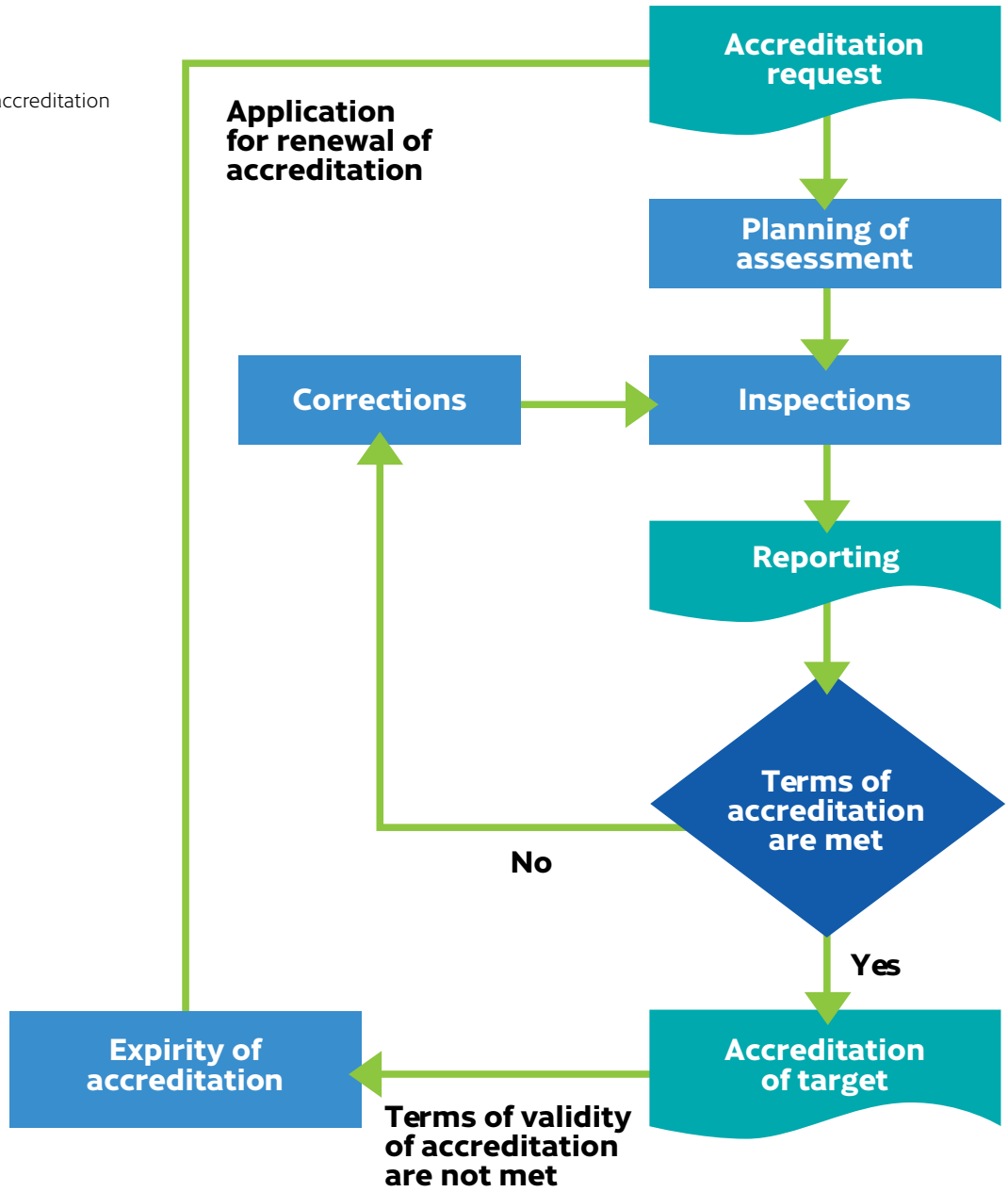
[19] Act on International Security Obligations(588/2004), https://www.finlex.fi/fi/laki/alkup/2004/20040588. Security Clearance Act (726/2014), https://www.finlex.fi/fi/laki/alkup/2014/20140726.

[20] National Cyber Security Centre. 2018. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-NCSA-toiminnon-suorittamat-tietoturvallisuustarkastukset.pdf.

Accreditation process

An accreditation process aiming for accreditation by the Finnish Transport and Communications Agency Traficom (L 588/2004, L 726/2014 or 1406/2011) begins when the target organisation submits an accreditation request to Traficom. The accreditation process is similar to the assessment process except that any deviations observed in the inspections must be corrected and the corrections verified before the accreditation can be issued. The accreditation process is shown in a simplified form in Figure 3. The accreditation process may be utilised, for instance, when the target organisations wants to demonstrate the adequacy of its protections by an accreditation issued by Traficom. In the accreditation process, risk assessment is carried out using the assessments by the target organisation and Traficom alike. The accreditation process is described in more detail in the guideline on the NCSA's information security assessments from the customer organisation's perspective (in Finnish only).

Figure 3.
Simplified accreditation process



Accreditation by a competent authority

The Finnish Transport and Communications Agency Traficom may issue the accreditation to a system that processes national or international classified information and meets the requirements. An accreditation may be issued only in the event that the target of the assessment undertakes to maintain the approved security level. Typically, it is also required that the entire system is governed under Finnish legislation.

The validity of the accreditation expires if any significant changes that affect the security of the inspected target occurs. Major changes to the network structure, personnel, security procedures or premises are examples of such changes. Changes caused by normal maintenance, such as installations of software security updates, do not lead to expiry of a valid accreditation. Case-specific terms for the expiry of accreditation are specified in connection with issuing the accreditation. Approvals for any significant changes must be requested in advance from Traficom.

Traficom may issue the accreditation to a system on the basis of an assessment performed by an accredited Information Security Inspection Body (L 1405/2011). The main prerequisites for issuing the accreditation are that the scope of the assessment performed match the scope of the request for the accreditation, as well as the adequacy of the inspection reports delivered. When necessary, before issuing the accreditation, Traficom performs additional assessments or requests the customer organisation to provide further information to ensure that the target meets the applicable security requirements.

Finnish Transport and Communications Agency Traficom
National Cyber Security Centre Finland
PO Box 320, FI-00059 TRAFICOM
tel. +358 (0)29 534 5000
traficom.fi