Katakri 2015 Finland

Information security audit tool for authorities

Contents

ISBN: 978-951-25-2778-6 pdf

Helsinki, FINLAND

The revision work was coordinated by a steering group which comprised the following members:

Maarit Jalava, Ambassador, Ministry for Foreign Affairs (chair)
Aku Hilve, Information Security Adviser, Ministry of Finance (vice chair)
Kai Knape, Deputy Security Director of the Defence Administration, Ministry of Defence
Laura Vilkkonen, Director of Unit, Ministry of Transport and Communications
Richard Wunsch, Lieutenant Commander, Defence Command Finland
Tapio Aaltonen, Chief Information Officer, deputy member **Samuli Bergström**, Head of Information Security, Ministry of the Interior
Juha Ilkka, Head of Information Security, Prime Minister's Office
Rauli Paananen, Finnish Communications Regulatory Authority (Ficora)
Lauri Holmström, Senior Specialist, Finnish Security Intelligence Service
Aki Tauriainen, Finnish Communications Regulatory Authority (Ficora)
Pekka Ylitalo, Major (eng.), Defence Command Finland
Jyrki Hollmén, Chief Policy Adviser, Confederation of the Finnish Industries
(as of 1.1.2015 Policy Adviser **Mika Susi**)
Kari Santalahti, Chief Security Officer, National Police Board
Mikko Viitasaari, Corporate Security Director, UPM
Tuomas Hyvärinen, Legal Adviser, Ministry for Foreign Affairs (secretary)
(as of 1.8.2014 Legal Adviser **Johanna Erkkilä**)
Kimmo Janhunen, Senior Adviser, Ministry of Finance (secretary)
(as of 1.8.2014 Senior Adviser **Kirsi Janhunen**)

In addition, different subdivisions within Katakri were prepared in separate sub-working groups. Katakri 2015 Security Audit Tool was approved by the NSA coordination group on 26.3.2015. To avoid constant revising, the goal was to make Katakri a tool which stands better the tests of time. An updated Katakri is available in an electronic format.

1. Foreword

The first Katakri - or the national security audit criteria - was produced in 2009 as part of the government's Programme for Internal Security. The work was led by the Ministry of Defence in close cooperation with other authorities and the business community. On completion, the Ministry of the Interior took on the responsibility for further managing and updating Katakri. The first updated version of Katakri was published in 2011.

The premise for revising Katakri for the second time was to increase its usability, scalability, risk-based approach, increasing the transparency of requirements and facilitating partial audits. As the changes were significant and they have resulted in a change in Katakri's structure it is no longer possible to talk about an updated version of Katakri. The term Katakri is, however, so established and so well known that it was decided to maintain it also in the future as a name for an audit tool for authorities.

2. Introduction

As an auditing tool for authorities, Katakri can be used to assess the ability of an organisation to protect Classified Information. Katakri itself does not set mandatory requirements on information security. It brings together the minimum requirements which are based on national legislation and international information security obligations. In this context, the most important piece of national legislation is the Government Decree on Information Security in Central Government (681/2010), which will be referred to as the Decree on Information Security and which is followed to protect both national and international Classified Information. An important international source here is the Council Decision on the Security Rules for protecting EU Classified Information (2013/488/EU) which lays down the basic principles and minimum standards of security for protecting EU Classified Information (EUCI). To ensure transparency, a source reference is always given in connection with the requirements presented in Katakri.

The structure of Katakri

The requirements in Katakri are divided into three subdivisions. The aim of the subdivision on security management (T) is to ensure that the organisation has sufficient security management abilities and skills. The organisation needs to fulfil the requirements for the basic level which are described in this subdivision. The subdivision on physical security (F) describes the security requirements for the physical environment of Classified Information. On the basis of the handling and storage needs of Classified Information, the physical areas of an organisation can be divided into administrative area, secured area and technically secured area. In the subdivision on Information assurance (I), the security requirements for the IT environment are given. On the basis of the information handled, this subdivision is further divided into three protection levels IV, III, II, equaling internationally used classification levels RESTRICTED, CONFIDENTIAL and SECRET.

Requirements have been set to allow different implementation options. The implementation of these requirements is supported by examples which are not, however, binding. Examples can be found in the section Additional Information. They describe recommendations and best practices which are found, for example, in VAHTI instructions[1] and policies and guidelines that complement the EU's Security Rules.

Using Katakri

Katakri can be used as an audit tool to assess for a Facility Security Clearance (FSC) how a company's security arrangements are implemented and to assess the authorities' information assurance. In addition, it can be used to support and develop security measures of companies, organisations and authorities. Katakri can be used to ensure that the organisation has introduced sufficient security arrangements to prevent unauthorised disclosure of Classified Information in all the environments where such information is handled. A further goal is to ensure that security requirements are taken into account in security management procedures.

By planning and implementing security arrangements it is possible to ensure that in view of possible threats an acceptable security level is reached. The organisation shall be able to demonstrate in a reliable manner that sufficient security arrangements are in place. This shall be based on systematic risk assessment. Security risk management shall be used to implement a combination of security measures which will create a satisfactory balance among user requirements, costs and residual risks.

Katakri is used to assess the general ability of an organisation to protect official classified information. Therefore FSCs carried out with the help of Katakri can be used in both domestic and international projects.

1 VAHTI instructions are a compilation of Finnish government instructions for secure handling of information.

Although the requirements laid down by the Council's Security Rules which are described in Katakri apply only to the EU Classified Information (EUCI) they reflect the fundamental principles jointly approved and implemented by the EU member states to protect Classified Information in Europe. They therefore provide a good basis for protecting Classified Information also in Finland. The member states follow the EU security rules in accordance with their national legislation and so, in addition to the EU requirements, also the Decree on Information Security is followed in Finland to protect the EUCI. The Decree on Information Security and the Council's Security Rules do not significantly differ. The source references in Katakri indicate if a requirement applies to the EUCI only.

As the subdivisions are drawn up as independent entities they can also be used separately. An example of this is an FSC which can be carried out partially when the activities of a company change or when an audit is conducted on a determined subdivision (FSC without safeguards, FSC with safeguards and FSC with safeguards including CIS[2]).

Katakri as such is not meant to be used as a security requirement in public procurement. For public procurement, accurate security requirements should be defined separately by taking into account procurement related risks and special needs. A single procurement may involve other requirements than those collected for Katakri about handling and protecting Classified Information. The implementation of these requirements is not assessed with the help of Katakri in case an organisation is committed to follow them on the basis of an agreement.

2 Communications and Information Systems

3. Subdivision T

SECURITY MANAGEMENT

This subdivision deals with the methods through which security and its management are implemented to be part of the entire organisation's activities. Security management which comprises both administrative security and personnel security aims at a well-functioning security management system and sufficient methods to ensure that the personnel handles Classified Information in an appropriate manner.

To facilitate interpretation, examples of implementation have been compiled in the field Additional information. This field contains examples of how to fulfil the minimum protection requirements in most of the cases. The examples given may be replaced by other protection means of anequal protection level. Requirements or given examples do not describe protection measures for every single environment or for every special case.

Security management should be an integral part of an organisation's management. On the basis of risk assessment, security management procedures should be seen in relation to the protection of Classified Information and the organisation's activities.

Reviewing of security management should be focused on that part of the organisation which has a direct or indirect impact on how Classified Information is handled. This may be a part of the organisation which manages the IT environment such as a subsidiary or equivalent. Especially when requirements for personnel security are assessed it should be noted that sufficient implementation may vary from one organisation to another. For example, the contents of the instructions for personnel handling information in protection level II generally varies significantly from instructions meant for the entire organisation.

Here a competent authority refers to the authority who in the case in question grants approval or issues a certification.

Administrative security

T 01

Security management

Security principles

Requirement	Source (681/2010)	Source (2013/488/EU)
1) Approved by the senior management, the organisation has introduced security principles which describe how their security measures are linked to the organisation's activities. 2) Security principles are comprehensive and appropriate for the organisation and for the protection of Classified Information. 3) Security principles provide guidance for security measures. Implementation of the security principles is reported and there is a frequent follow-up.	Sections 4 and 6	Article 9(1)

Additional information

General

One of the goals of the organisation's security principles is that the management is committed to security, which in turn supports the organisation's activities. The security principles are communicated to the personnel and, where necessary, to stakeholders. The principles can be presented in many ways, for example as a single document or as a part of the organisation's set of instructions.

Other sources of information

ISO/IEC 27002:2013 5.1.1; ISO/IEC 27001:2013 5.1; ISO/IEC 27001:2013 5.2; ISO/IEC 27001:2013 5.3; ISO/IEC 27001:2013 9.3; VAHTI 2/2010

T 02

Security management

Defining the tasks and responsibilities of the security management

Requirement	Source (681/2010)	Source (2013/488/EU)
The organisation has defined the tasks and responsibilities of security management.	Section 5(1)(3)	Article 7(5)

Additional information

Example of implementation

1) The organisation has defined the tasks and responsibilities of security management at least for the following areas:
   a) security administration
   b) personnel security
   c) physical security
   d) information assurance
2) This includes the responsibilities of the owner of the handling environment for Classified Information and other security related responsibilities.
3) Responsibilities are defined for monitoring the coverage of the security documentation and ensuring that it is up-to-date. Accessible on a need-to-know basis, the documentation covers the processes of and the handling environments for Classified Information during the entire life cycle of information.

General

The goal of defining the security tasks and responsibilities is to ensure that responsible people are designated for key subdivisions and that they are aware of their responsibilities and competences.

Other sources of information

ISO/IEC 27002:2013 6.1.1; ISO/IEC 27001:2013 5.1; ISO/IEC 27001:2013 5.2; ISO/IEC 27001:2013 5.3; VAHTI 2/2010

T 03

Security management

Resources of security management

Requirement	Source (681/2010)	Source (2013/488/EU)
There is a sufficient level of expertise in the organisation to ensure information security.	Section 5(1)(2)	Annex IV (4)

Additional information

A sufficient level of expertise ensures that the goal of information security is achieved and the measures are introduced in a cost-effective way. Sufficiency of resources is regularly assessed.

Other sources of information

ISO/IEC 27001:2013 7.1; ISO/IEC 27001:2013 7.2; ISO/IEC 27001:2013 5.1; VAHTI 2/2010

T 04

Security management

Security risk management

Requirement	Source (681/2010)	Source (2013/488/EU)
1) The organisation has a risk management process in place. Risk management must be a regular, continuous and documented process. 2) In risk analysis, a proven, transparent and fully understandable method shall be used in a systematic way. 3) Also external participation in risk management should be considered. 4) Risk management must cover at least the subdivisions of security management, physical security and information assurance. As for specific stakeholders, identified risks shall be taken into account. The organisation must ensure that the requirements for protection of Classified Information are met also in situations where information is handled by sub-contractors. 5) The risk management process and its results are taken into account when setting security goals for the organisation, assessing the impact of security deviations, planning security measures, in change management and, where applicable, in procurement. 6) Security measures are scaled by taking into account the information's protection level, amount, format, rationale for classification and the designated handling environment for the information in relation to an estimated risk of a hostile or criminal activity. 7) The organisation documents the most important parts of monitoring and security measures.	1) Sections 4, 5 and 6 2) 3) Sections 4, 5 and 6 4) Sections 4, 5 and 6 5) Sections 4, 5 and 6 6) Sections 4, 5 and 6 7) Sections 4, 5 and 6	1) Article 5, Annex IV (4) 2) Annex IV (4) 3) Annex IV (4) 4) Annex IV (4) 5) Annex IV (4) 6) Article 5, Annex IV (4-7) 7) Article 5d(2) 8) Annex IV (12)

Additional information

Example of implementation

1) The principles of risk management are described.
2) Targets to be protected have been identified.
3) The owner/responsible persons are designated for protected targets.
4) The risks related to the protected targets are identified and assessed.
5) Protection methods are proportioned to the identified risks.
6) A systematic method is used for risk management and analysis.
7) A description of security arrangements is maintained in the organisation. The conclusions of the risk management process are taken into account in the organisation's security documentation.

General

Implemented by the management and personnel, risk management is a process incorporated into the organisation's management and activities and applied to the extent deemed sufficient to all activities in the organisation (such as processes, relations to clients). Its aims are to identify and manage factors that may threaten the organisation's operational preconditions and to reduce the risks to such levels that the organisation's activities and objectives are not threatened.

Risk management refers to all measures taken in the organisation to mitigate risks and damage. It means assessment of situations, planning and concrete action, in which each member of personnel participates in their professional role. By its very nature, good risk management is anticipatory, conscious, planned and systematic.

T 04

Risk management means avoiding negative and detrimental incidents (influencing the likelihood of an incident) or minimising the consequences of incidents (influencing the extent of consequences). It also means identifying, analysing and benefiting from potential opportunities.

Risk management for the protection of Classified Information

Risk management measures must be focused on the environment where Classified Information is to be handled. The handling environment generally includes personnel, premises and information systems.

Taking account the principle of defence-in-depth in risk management

The multilevel nature of security arrangements (defence-in-depth) must be addressed in risk management. In risk assessment, it is essential to acknowledge that it is not possible to introduce full protection with any of the security arrangements. As to single risks, a sufficient protection can be achieved with a single or several security measures. For example, it is possible to improve physical security by using technical security systems and, in view of the risks involved, achieve a sufficient combination of security arrangements.

Methods for risk management and analysis

Each risk management method has its strengths and weaknesses. In many of the systematic methods, activities are based on identifying threats and vulnerabilities, assessing likelihoods and influence, defining measures necessary to reduce risks, assessing residual risks and for the follow-up of corrective measures.

Risk management in situations requiring approval by a competent authority

Managing the risks, which threaten the organisation's security, provides the basis for correctly scaled security arrangements. The competent authority adjusts the requirements to the threat environment and to security measures (controls) proposed by the organisation. However, the risk assessments of the competent authority and the organization may differ.

In situations where an organisation applies for an accreditation from an authority, the organisation needs to take into account the threat factors or an assessment of the sufficiency of security arrangements defined by a competent authority, before presenting an implementation plan. Through its risk management process, the organisation needs to be able to show to the competent authority its justification for the chosen security arrangements and their sufficiency. It is recommended that the organisation discusses its risk identification and security measures planning with the competent authority at an early phase to ensure that the assessment of both the organisation and the competent authority on the risks in the environment in question can be taken into account already in security measures planning. The threat factors assessed by the competent authority may result in a need to increase protection requirements.

T 04

Assessment of threat factors by the competent authority

For its assessments, the competent authority takes into account, for example, the basis for classification, protection level, handling format, significance and an assessment whether the information is interesting for state or criminal actors. Based on this assessment, the competent authority approves the security measures and implementation models chosen by the organisation.

Other sources of information

ISO/IEC 27001:2013 6.1.2; ISO/IEC 27001:2013 6.1.3; ISO/IEC 27001:2013 6.2; ISO/IEC 27001:2013 8.2; ISO/IEC 27001:2013 8.3; ISO/IEC 27001:2013 9.1; ISO/IEC 27001:2013 9.3; ISO/IEC 27001:2013 10.1; ISO/IEC 27002:2013 8.1.1; ISO/IEC 27002:2013 8.1.2; ISO/IEC 27002:2013 18.1.1; ISO/IEC 27002:2013 18.2.2; ISO/IEC 27002:2013 18.2.1; ISO/IEC 27005:2011; ISO 31000:2009; OCTAVE Allegro; SRHY risk management; VTT – Risk analysis methods; VAHTI 2/2010.

T 05

Security management

Continuity

Requirement	Source (681/2010)	Source (2013/488/EU)
1) Recovery and continuity assurance in view of operation requirements have been taken into account in planning. 2) Preventive and recovery measures must be incorporated into business continuity plans to minimise the effects of significant disruptions and exceptional incidents on handling and storing Classified Information. 3) The observations on deviations are made a part of risk assessment and, on the basis of these, recovery and continuity planning are updated when necessary. 4) To prevent unauthorised access to information, disclosure or loss of integrity and availability, the need to protect information in emergency situations has been taken into account in business continuity planning.	1) Section 5 (1)(4) 2) Section 5 (1)(4), Section 4 3) Section 5 (1)(4), Section 4 4) Section 5 (1)(4), Section 4	1) Article 5(4) 2) Article 5(4) 3) 4) Article 5(3)

Additional information

General

Dependencies on external factors have been identified in the organisation as well as their effects on its functions. The effects of organisation's activities on others have been identified.

Other sources of information

ISO/IEC 27002:2013 17.1.1; ISO/IEC 27002:2013 17.1.2; ISO/IEC 27002:2013 17.2.1; ISO/IEC 27002:2013 12.3.1; ISO/IEC 27002:2013 16.1.2; ISO/IEC 27002:2013 16.1.6; VAHTI 2/2009; VAHTI 2/2010

T 06 Security management Management of security events	Requirement	Source (681/2010)	Source (2013/488/EU)
	1) The organisation has a set of procedures in place to handle security events. 2) The organisation has defined the persons/actors to whom to report on (possible) security events.	Section 5(1)(4)	Article 5(4), Article 14(3)

Additional information

Example of implementation

Management of security events is
1) planned,
2) provided with instructions/training,
3) documented on a sufficient level in view of the handling environment of the information,
4) practised, and in particular,
5) communication practices and responsibilities have been agreed on.

General

Through security event management it is ensured that the organisation is able to function efficiently in exceptional situations by minimising damage and restoring the situation to normal. Effective management of security events requires sufficient allocation of resources.

Originators of Classified Information (for example the EU) as well as existing approvals or certifications by authorities may require that there is an immediate notification of compromises or suspected breaches regarding Classified Information.

Other sources of information

ISO/IEC 27002:2013 16.1.1; ISO/IEC 27002:2013 16.1.2; ISO/IEC 27002:2013 16.1.4; ISO/IEC 27002:2013 16.1.5; ISO/IEC 27002:2013 6.1.3; VAHTI 2/2010

T 07

Security management

Classification of information

Requirement	Source (681/2010)	Source (2013/488/EU)
Information has been classified on the basis of statutory requirements: a) Classified Information (including drafts) are marked to indicate the protection level. b) A document is marked to indicate the highest protection level of its parts (e.g. Annexes). c) If the protection level of the main document and annexes is not the same, this must be indicated in the document.	Chapter 3, Sections 8 and 9	Annex III (2, 6, 7)

Additional information

General

The purpose of classification is to identify and scale correctly the security measures on the basis of protection needs. Depending on the information, handling environment and users, classification may be indicated in various ways. By classifying handling environments according to Classified Information it is possible to indicate clearly the security measures related to each IT environment.

Other sources of information

ISO/IEC 27002:2013 8.2.1; ISO/IEC 27002:2013 8.2.2; VAHTI 2/2010

Personnel security

T 08	Requirement	Source (681/2010)	Source (2013/488/EU)
Personnel security Taking into account the different phases of employment	The organisation has a procedure in place to ensure security in different phases of the employment. Particular attention must be paid to measures at recruitment, changing tasks and ending employment.	Section 5(1)(8), Section 13	Annex I (29, 31)
	Additional information		
	General Security awareness generally requires that the personnel has received security training and has been made aware of the relevant of security instructions. Instructions can be divided into entities for example according to the phases of the employment. Instruction entities include, for example, instructions for recruitment, induction training, carrying out changes during employment, ending employment, and for more detailed measures such as changes in user and access rights. *Other sources of information* ISO/IEC 27002:2013 7.1; ISO/IEC 27002:2013 7.2; ISO/IEC 27002:2013 7.3; VAHTI 2/2008; VAHTI 2/2008; VAHTI 2/2010		

T 09	Requirement Classified Information	Source (681/2010)	Source (2013/488/EU)
Personnel security Assessment of the trustworthiness and reliability of the personnel	The trustworthiness and reliability of individuals handling Classified Information is determined, if necessary, by means of security clearance methods in accordance with the relevant level.	Section 5(1)(8)	Annex I (2c, 2b, 29)
	Additional information		
	General The trustworthiness and reliability of an individual handling the EUCI and Nato's Classified Information requires at the level of CONFIDENTIAL and above that security clearance has been granted. *Other sources of information* ISO/IEC 27002:2013 7.1.1; act on security clearances (726/2014); act on international information security obligations (588/2004)		

T 10

Personnel security

Non-disclosure agreement and confidentiality commitment procedure

Requirement	Source (681/2010)	Source (2013/488/EU)
Non-disclosure agreement or confidentiality commitment is in place.	Section 5(1)(8,9)	Annex I (29)

Additional information

ISO/IEC 27002:2013 7.1.2; ISO/IEC 27002:2013 13.2.4

T 11

Personnel security

Security education and awareness

Requirement	Source (681/2010)	Source (2013/488/EU)
1) Security instructions cover the processes and handling environments that are related to Classified Information during the entire life cycle of information. 2) Personnel receive instructions for and education in the correct handling of Classified Information. 3) The education in the handling of Classified Information takes place on a regular basis and participants are documented. 4) It is controlled that security instructions are followed and the needs to change the instructions are assessed regularly.	1) Sections 4, 5 and 6 2) Section 5(1)(9) 3) Section 5(1)(10) 4) Section 5(1)(10)	Annex I (29-31); Annex IV (21-22)

Additional information

Example of implementation

1) All individuals who handle Classified Information have been made aware of security instructions and procedures concerning protection of information. Handling the EUCI and Nato's Classified Information requires that the individuals also acknowledge in writing their obligations to protect such information.
2) Security education and instructions are carried out in view of the needs that the personnel experience in their work.
3) There is a regular follow-up on the coverage and up-datedness of security instructions and this is made accessible for relevant actors.
4) The contents of security education are documented.

General:

One of the goals of security documentation is to ensure that the key security procedures are appropriate and consistent. Documentation also ensures that the work does not depend on certain individuals. Cf. the role of documentation in change management and in the ability to observe deviations (I 20).

Other sources of information:

ISO/IEC 27002:2013 7.2.2; ISO/IEC 27002:2013 5.1.1; ISO/IEC 27002:2013 5.1.2; ISO/IEC 27002:2013 12.1.1; ISO/IEC 27001:2013 7.5; VAHTI 4/2003; VAHTI 2/2008; VAHTI 2/2010

T 12 Personnel security Need-to-know and access rights	Requirement	Source (681/2010)	Source (2013/488/EU)
	1) A list of tasks which require handling of Classified Information is maintained in the organisation. 2) Access to Classified Information can only be granted after an individual's task-based need-to-know has been determined. 3) A list of handling rights for each protection level of Classified Information is maintained in the organisation.	Section 13	Annex I (2a)
	Additional information		
	General: It is easier to determine the need-to-know when the organisation has described the principles to Classified Information and processes for granting task-based access and managing it in changing situations. In determining handling rights, tasks and roles it should be ensured that dangerous role combinations are not created. *Other sources of information:* ISO/IEC 27002:2013 9.1.1; ISO/IEC 27002:2013 9.1.2; ISO/IEC 27002:2013 6.1.2; VAHTI 2/2008; VAHTI 2/2010		

4. Subdivision F

PHYSICAL SECURITY

In Katakri, physical security is approached from the point of protecting the Classified Information and ensuring that Classified Information is protected from unauthorised disclosure. The aim of physical safeguards is to deny surreptitious or forced entry by intruders, to deter, impede and detect unauthorised actions and allow for segregation of personnel in terms of access to Classified Information on the need-to-know basis. Such safeguards shall be determined on the basis of the risk management process. In subdivision F, premises and groups of premises are divided into three areas: administrative area, secured area and technically secured area. A need to establish any of these areas is based on the protection level of Classified Information which is stored or handled in the area. The division into physical areas is based on the security rules of the Council of the European Union but a similar division, based on security zones, is used also on a national level.

Physical security measures are chosen and appropriately scaled on the basis of a threat survey and risk assessment. Requirements can be met with different implementation models. The effectiveness of physical security measures should be monitored as a part of risk management in the organisation. In situations where the aim is to apply for an approval or certification for the premises from a competent authority, the implemented security measures need to be sufficient.

The field Additional Information contains examples of how to fulfil the minimum protection requirements in most of the cases. The examples given may be replaced by other protection means of equal protection level. Requirements or given examples do not describe protection measures for every single environment or every special case.

Physical security is based on design. The following should be addressed when designing and using premises and buildings:

1) In which physical environments Classified Information is handled and what protection level does it belong to?
2) In which part of the building is Classified Information handled?
3) Security arrangements and structures in a building or physical environment.
4) Protecting Classified Information in a physical environment (creating, receiving, using, storing and destroying information)
5) Which systems are used for handling Classified Information in the particular physical environment?
6) The amount of information; accumulating Classified Information may require that stricter security requirements are applied (for example, a large amount of protection level IV (RESTRICTED) information may aggregate a protection level III (CONFIDENTIAL) entity)
7) As a rule, information is handled in premises where security is sufficient considering the protection level of the information
8) The need for classification of of the building's security documentation has been agreed on with the planning and maintaining organisations.

Requirements on premises and equipment

F 01

Requirements on premises

Physical security measures

Requirement	Source (681/2010)	Source (2013/488/EU)
Physical security measures are implemented according to the principle of defence-in-depth	Section 14	Annex II (4)

Additional information

Defence-in-depth means implementing a number of security measures which complement each other. If possible, areas form zones which are within each other so that the innermost areas are the ones with the highest protection level. Access to zones is under control. Security measures are designed as an entity which takes into account the protection level and amount of Classified Information and the environment and structure of buildings. In addition, the risks identified by means of risk management such as sabotage, terrorism, intelligence and criminal offences are addressed.

The design of buildings and premises, structural protection solutions, security systems and devices as well as the procedures maintaining security constitute physical qualities which protect information. Based on risk assessment, security solutions are planned as combinations of different security controls.

Example of defence-in-depth:

A building is designed in a way that the walls, ceiling and floor form the first protection layer. Access into the building is controlled and managed. Information of a higher protection level is handled in the inner areas of the building so that intrusion is deterred. The technical solutions complement the structural security solutions. Windows, doors and other openings are taken into account in the design phase.

F 01

By applying the concept of defence-in-depth and on the basis of a risk management process, an organisation shall define a relevant combination of physical security measures which may involve the following:

a) Defence-in-depth: a physical barrier defending and locking the boundary of an area requiring protection;
b) a storage unit or storage area: a locked piece of office furniture, security container, strong room, vault;
c) intrusion detection system: to improve defence-in-depth in rooms and buildings instead of security personnel or in support of it;
d) physical access control: electric or electro-mechanical, carried out by security personnel and/or receptionist or with other physical means;
e) access rights management: protection of documents is ensured by granting access to documents only on the need-to-know basis;
f) security personnel: trained, supervised and when necessary security-cleared;
g) CCTV: security personnel are able to use a CCTV surveillance system;
h) security lighting: to enable the security personnel to monitor the area effectively, either directly or by means of a camera system; and
i) other relevant physical measures which aim at detecting and preventing unauthorised entry or preventing a loss of or damage of Classified Information.

Other sources of information:

ISO/IEC 27002:2013 11.1.3; VAHTI 2/2013

F 02	Requirement	Source (681/2010)	Source (2013/488/EU)
Requirements on areas	1) Areas where Classified Information is stored or handled are protected with appropriate locking systems, access control or other measures to prevent unauthorised access to the premises.	1) Section 14 2) Section 5 (1)(7)	
	2) Environments where Classified Information is handled or stored are sufficiently controlled and protected.		
Areas needed to provide physical protection for information	3) Necessary physically protected areas (see I 21) are set up to protect Classified information.		3) Annex II (12)
	Administrative area		
Administrative areas, secured areas and technically secured areas	4) A visibly defined perimeter has been established which allows individuals and, where possible, vehicles to be checked		4) Annex II (14a)
	5) unescorted access shall be granted only to individuals who are duly authorized. All other individuals shall be escorted at all times or be subject to equivalent controls		5) Annex II (14b-c) 6) Annex II (24)
	6) If Classified Information is stored in the area there is an approved storage solution for the information in question.		7) Annex II (23b)
	7) If Classified Information is handled in the area, access by unauthorised individuals to the information is deterred.		
	Secured area		
	8) A visibly defined and protected perimeter has been established through which all entry and exit is controlled by means of access control or personal recognition system.		8) Annex II (15a) 9) Annex II (15b-c)
	9) Unescorted access is granted only to individuals who are security-cleared and specifically authorised to enter the area on the basis of their need-to-know. All other individuals are escorted at all times or they are subject to equivalent controls.		10)Annex II (22) 11)Annex II (22, 24, 26)
	10) The structures defining the area form a complexity which in view of risks offers sufficient protection against unauthorised entry.		12)Annex II, item 19
	11) If Classified Information is stored in the area there must be an approved storing solution.		
	12) Secured areas which are not occupied by duty personnel on a 24-hour basis shall be inspected at the end of regular working hours and at random intervals outside regular working hours unless an intrusion detection system is in place.		

F 02	When entry into a secured area constitutes, in all practical purposes, direct access to Classified Information contained in it, the following additional requirements are applied: 13) The individual handling information shall be aware of the level of highest security classification of the information stored in the area. 14) All visitors shall require specific authorisation to enter the area. They shall be escorted at all times and shall be appropriately security-cleared unless steps are taken to ensure that no access to Classified Information is possible.		13) Annex II (16a) 14) Annex II (16b)
	A set of security operating procedures is drawn up for each secured area stipulating the following: 15) the highest protection level or security classification which can be handled in the area 16) control and protection measures to be applied 17) unescorted access is granted only to individuals who are security-cleared and specifically authorized to enter the area on the basis of their need-to-know 18) procedures concerning the escorting of individuals 19) any other relevant measures and procedures.		15-19) Annex II (21)
	Technically secured area In addition to the requirements on the secured area: 20) the area is equipped with an intrusion detection system (IDS) 21) the area is kept locked when not occupied and guarded when occupied 22) keys are controlled 23) all persons and material entering such an area are controlled 24) such an area is regularly inspected to detect unauthorised communication lines, unauthorised communication devices and other electronic equipment 25) there are no unauthorised communication lines or equipment in the area.		20-25) Annex II (17)
	Additional information An area can refer, for example, to a room, server room, storehouse, archives, an entity comprising all of these or to another specific part of building. Both buildings and premises may include areas belonging to a number of different security zones. A secured area may contain several areas. A secured area can be created without an administrative area. Information of protection levels IV-II can be handled in a secured area. Such information can also be handled in an administrative area if unauthorised access to information is deterred. Information of protection level IV can be stored in an administrative area whereas information of protection levels III-II shall be stored in a secured area. See I 21 and I 14.		

F 02

Perimeter of the administrative area:

There are no special requirements for the structures of the fence defining the area or for the walls, ceiling, floor, windows, doors and other openings of the buildings. The perimeter of the administrative area and the perimeter defining the handling and storage unit of Classified Information should be locked with keys that are granted patent protection and thus cannot be copied.

Perimeter of the protected area:

- Protection level III

If Classified Information is stored in the area using an approved storage unit, the structures of the walls, ceiling, floor, windows, doors and other openings of the buildings defining the area shall provide structural protection which delays and makes attempts to enter the area difficult.

If Classified Information is kept in the area without using an approved storage unit, the structures of the walls, ceiling, floor, windows, doors and other openings of the buildings defining the area shall provide structural protection equivalent to the approved storage unit for the relevant protection level. A SFS-EN-14450 class S2 security container or equivalent is such a storage unit. Similar structural protection is provided by, for example, a SFS-EN-1627 class 4.

- Protection level II

If Classified Information is stored in the area using an approved storage unit, the structures of the walls, ceiling, floor, windows, doors and other openings of the buildings defining the area shall provide structural protection which significantly delays and makes attempts to enter the area highly difficult.

If Classified Information is stored in the area without using an approved storage unit, the structures of the walls, ceiling, floor, windows, doors and other openings of the buildings defining the area shall provide structural protection equivalent to the approved storing unit for the relevant protection level. A SFS-EN-1143-1 class EII safe or equivalent is such a storage unit. Similar structural protection is also offered by SFS-EN-1627 class 5. An equivalent structural protection can also be realised in such a way that the structures defining the secured area constitute a protection level equivalent to SFS-EN-1627 class 3 and, in addition, the structures of the area defining the storage unit constitute a protection level equivalent to SFS-EN-1627 class 4.

F 02

Intrusion detection system (requirement 11):

There should be sufficient surveillance in secured areas in view of intrusion-related risks. Examples of these include:

a) intrusion detection system and a unit responding to alarms; or
   - the intrusion detection system covers the protected perimeter of the secured area
   - the intrusion detection system and alarm transmission system are tested once a month
   - the organisation has designated an individual responsible for managing the intrusion detection system which monitors the protection level II information

b) duty personnel are placed in the immediate vicinity of the storage area on a 24-hour basis.

Other sources of information

ISO/IEC 27002:2013 11.1.1; ISO/IEC 27002:2013 11.1.2; VAHTI 2/2013

F 03

Security systems and equipment to provide physical protection for information

Requirement	Source (681/2010)	Source (2013/488/EU)
Security systems and devices meant for providing physical protection for information (such as security containers, strong rooms, physical access control systems, intrusion detection systems, alarm systems and surveillance systems) are in line with the approved technical standards or minimum requirements. Systems and devices must be tested and kept in working order.	Sections 14 and 6	Annex II (8, 10) Annex IV (8)

Additional information

Storage solutions and security systems should meet the requirements of the following standards or, as to the required qualities, an equivalent standard approved in Europe:

- Strong rooms: tested and certified, for example, in line with SFS-EN 1143-1 or other equivalent standard;
- Prefabricated strong rooms: tested and certified, for example, in line with SFS-EN 1143-1 or other equivalent standard;
- Security containers: tested and certified, for example, in line with SFS-EN-14450 or other equivalent standard;
- Locks and fittings: tested and listed and certified, for example, in line with SFS 7020 / SFS 5970 or other equivalent standard;
- Doors and openings: tested and certified, for example, in line with SFS-EN 1627 or other equivalent standard;
- System requirements and application instructions for alarm systems (intrusion detection and theft detection systems) for example in line with standards SFS-EN 50131-1 + A1, SFS-EN 50131-1/A1 and SFS-CLC/TS 50131-7 or equivalent
- General requirements and application instructions for alarm systems (alarm transmission systems and equipment): for example in line with standards SFS-EN 50136-1 and SFS-CLC/TS 50136-7 or equivalent
- System and component requirements and application instructions for physical access control systems: for example in line with standards SFS-EN 50133-1 + A1, SFS-EN 50133-1/A1, SFS-EN 50133-2-1 and SFS-EN 50133-7 or equivalent
- System requirements and application instructions for CCTV surveillance systems: for example in line with standards SFS-EN 50132-1, SFS-EN 50132-7, SFS-EN 62676-1-1 and SFS-EN 62676-1-2 or equivalent
- Introduction and delivery inspection of CCTV surveillance systems may be carried out for example by the K method of the Federation of Finnish Financial Services. K method comprises a set of technical requirements through which the camera system is tuned into either detect or to identify the monitored object
- Shredders: see I 19.

In addition:

- if information classified for protection level IV is stored in a locked cabinet it must be ensured that intrusion will leave a trace
- information classified for protection level III must be stored in a SFS-EN 14450 level security container S2 or equivalent
- information classified for protection level II must be stored in a SFS-EN 1143-1 level safe EII or equivalent.

Other sources of information

ISO/IEC 27002:2013 11.1.1; VAHTI 2/2013

Deterring unauthorised access

F 04

Deterring unauthorised access

Management of access rights

Requirement	Source (681/2010)	Source (2013/488/EU)
1) Access right management is organised so that unauthorised access to classified information is denied. 2) Access to premises containing classified information is only allowed on the need-to-know basis.	Section 14	Annex II (2)

Additional information

Recommendation to implement access rights:

- ID cards with photo or equivalent visible identifiers are used in the organisation
- A designated person in the organisation grants access rights to the administrative area and secured area (also technically secured area)
- There are documented instructions on the procedures of the management system for access control:
  - a designated person maintains the document on granted physical access rights.
  - physical access rights are granted only on the basis of the need-to-know.
  - the rationale for access rights is documented and only designated persons have an access to such an area
  - access rights are kept up-to-date
  - lists of the personnel and visitors are kept separate
  - physical access rights are reviewed on regular intervals, for example every 6 months by a designated person
  - management of the physical access control system may be outsourced. Managing access control to a secured area from work stations must be disabled for unauthorised users.
- Only authorised persons have access to secured area. Access to a secured area must be verified afterwards.
- Only authorised persons have access to handling and storage areas of Classified Information at the protection level II and the identification must be always used when entering and leaving the area. It must be possible to verify later any access to the area.

Procedures for visitors:

- Personnel has received training in managing visits and visit procedures which are supported by a designated person in the organisation:
  - the host must belong to the personnel
  - visitors must never be left alone in the areas where Classified Information is handled
  - visitors wear a visible identifier, for example a visitor's badge
  - the personnel have been instructed to react to anyone who is not wearing a badge.

F 04

Maintenance in the administrative area and secured area

- maintenance work in the administrative area is carried out only by authorised individuals or under the supervision of the personnel
- maintenance work in the secured area is carried out only by security-cleared individuals who have been granted special permission to enter the area or who are under the supervision of the personnel
- as to the intrusion detection system, physical access control system and other control systems for the premises where the information of protection level III is stored or the area limiting it, all maintenance work, installation and cleaning of the technical rooms and the equipment in them can only be carried out by security-cleared individuals who have been granted special permission to enter the secured area or who are under the supervision of the personnel
- as to the intrusion detection system, physical access control system and other control systems for the premises where the information of protection level II is handled and stored and the secured area limiting it, all maintenance work, installation and cleaning of the technical rooms and the equipment in them can 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.

Handling classified information during maintenance work and visits:

Classified Information is not handled in the premises while maintenance work, installation and cleaning are conducted.

Other sources of information

ISO/IEC 27002:2013 11.1.5; VAHTI 2/2013

F 05

Deterring unauthorised access

Management of keys and combination settings

Requirement	Source (681/2010)	Source (2013/488/EU)
1) Management procedures for keys and combination settings for offices, rooms, strong rooms and security containers are sufficient to deter unauthorised entry. 2) Combination settings have been given to as few individuals as possible and they know them by heart. 3) Combination settings to security containers and strong rooms are changed a) when receiving a new container b) always when a person knowing the combination changes tasks or leaves employment in the organisation c) always when a compromise has occurred or is suspected d) when a lock has undergone maintenance or repair and at least every 12 months.	1) Section 5 (1) (7), Section 14(1)	1) Annex II (30) 2) Annex II (31) 3) Annex II (31)

Additional information

Key management system:

- The procedures for key management are instructed and documented
  - The organisation has designated a person responsible for key management and the person has a list of all keys, a blueprint of the locking system and a key card.
    - The reason for submitting a key is documented.
    - Keys can be handed over only to individuals with physical access rights.
    - Changes in the personnel are reflected in key management rights.
    - Key management rights are regularly reviewed.
- A master key to a public area must not provide access to an administrative area. It is forbidden to remove a master key or a similar identifier from the premises. Kept in a safe place, a master key shall be retained in an envelope which is securely sealed and bears the date of closing and signature.
- A master key to a public area or an administrative area must not provide access to a secured area. It is forbidden to remove a master key or a similar identifier from the premises. Kept in a safe place, a master key shall be retained in an envelope which is securely sealed and bears the date of closing and signature. Handing over the key requires a signature and is based on duties of the person involved. The procedure is described in security management instructions.
- When guards, building maintenance and service personnel are outsourced, the keys to the secured area which are to be handed over to them shall be sealed away for exceptional situations. If the alarm goes off, two persons are expected to arrive at the premises at the same time.
  - The keys to the security containers shall not be handed over to outsourced guards, building maintenance and service personnel not even in exceptional situations.

F 05	
	Access rights management system (security of information processing systems, see I 06, I 07 and I 08) ■ The procedures for access rights management system are instructed and documented • A document is drawn up of the granted access rights (keys and combination settings) to the storage room or storage unit (security containers, strong rooms, vaults and server rooms) of Classified Information. The document is maintained by a designated person in the organisation. • access rights can be granted if the person is entitled to access Classified Information or if there is some other need to access the premises which in practice means direct access to Classified Informatio and the person is security-cleared. • the rational for granting access rights is documented • access rights are kept up-to-date • access rights are reviewed at regular intervals. *Other sources of information* VAHTI 2/2013

Protection from unauthorised observation and eavesdropping

F 06	Requirement	Source (681/2010)	Source (2013/488/EU)
	Protection is provided against unauthorised observation and overlooking.	Section 14(1), Section 5(5)	Annex II (6)
Protecting information Protection from unauthorised observation and overlooking	Additional information *Preventing unauthorised observation and overlooking:* ■ Irrespective of the format of information, Classified Information is handled in such a way that it is protected from unauthorised observation and overlooking. ■ Portable computers have a display privacy filter. ■ The windows of the handling area are provided with visual obstruction such as blinds. There must not be a visual connection from outside when Classified Information is handled in the area. In a technically secured area an additional technical security inspection is conducted before the area can be taken into use (cf. F 02 item 24). See I 14. *Other sources of information* ISO/IEC 27002:2013 11.1.3; VAHTI 2/2013		

F 07	Requirement	Source (681/2010)	Source (2013/488/EU)
Information protection Protection from eavesdropping	Protection against eavesdropping is ensured.	Section 14(1) Section 5(5)	Annex II (17)
	Additional information		
	Sound insulation in an administrative area and in a secured area: Attenuation must be sufficient to prevent vocal discussions to be heard outside the respective area. In a technically secured area an additional technical security inspection is conducted before the area can be taken into use. (cf. F 02 item 24) *Other sources of information* ISO/IEC 27002:2013 11.1.3; VAHTI 2/2013		

Continuity management

F 08	Requirement	Source (681/2010)	Source (2013/488/EU)
Ensuring business continuity	Preventive and recovery measures must be incorporated into business continuity plans to minimise the effects of significant disruptions and exceptional incidents on handling and storing Classified Information.	Section 5(1)(4)	Article 5
	Additional information		

	Functional requirements on critical server and equipment rooms:
	
	■ Critical servers and equipment are identified and secured in line with operational requirements.
	  • if functional requirements on the system are high, the usability of systems shall be secured against theft, vandalism, fire, heat, gases, dust, shaking, water and disruptions in electricity supply
	  • remote access is denied to the HPAC automation management to monitor critical server and equipment rooms
	  • environmental sensors of critical server and equipment rooms are protected and controlled.
	
	Other sources of information
	
	ISO/IEC 27002:2013 11.2.1; ISO/IEC 27002:2013 11.2.2; VAHTI 2/2013		

5. Subdivision I

INFORMATION ASSURANCE

Information Assurance, one of the subdivisions in the Finnish Government Security Audit Tool (KATAKRI), provides requirements for appropriate protection when handling classified information in electronic format. This subdivision also works as a supplement to other subdivisions for the protection of information in paper format. Requirements have been divided in four chapters; communications security, systems security, data security and operations security. Subdivision consists of the requirements, of the examples for fulfilling the requirements and of additional support information. Some specific themes (e.g. management connections, wireless networks, remote use and backup procedures) have their particular requirements.

The correct use of the Information Assurance subdivision of this criterion requires the use of risk assessment results focusing on the dedicated environment subject to the audit. The field "Additional Information" contains examples of how to fulfil the minimum protection requirements in most of the cases. The examples given may be replaced by other protection means of equal protection level. Requirements or given examples do not describe protection measures for every single environment or for every special case.

In case the organisation to be audited is aiming at system accreditation by a competent authority, the protection measures have to fulfil the risk assessment findings of both the organisation itself and of the government authority. Especially in cases when compensatory controls are used, the organisation to be audited has to be able to address that the necessary protection level has been reached.

In order to stay in control of expenses, it is recommended to pay special attention to correct classification of the information, as well as how to limit the handling environment of the classified information to its minimum. For example, when separating the handling environment of CONFIDENTIAL (Finnish protection level III) information from the environment of RESTRICTED (Finnish protection level IV) information, the protection requirements set for CONFIDENTIAL level do not need to be taken into count in the RESTRICTED environment.

In majority of the cases the authority auditing information systems in Finland will be the Finnish Communications Regulatory Authority (FICORA). Audit cases for information processing systems have been described more in detail in the Annex II.

When assessing the handling environment of the Classified Information as a whole, it is necessary to take into account all requirements set in the Information Assurance subdivision. In cases when the audit is targeted solely to the information processing system handling information in an electronic format, only requirements set for electronic information handling are to be audited. In such cases the handling requirements concerning the information in paper format - for example (especially I 16, I 17, I 18, I 19) - will be taken into account only when applicable. When assessing the fulfilment of certain requirements (especially I 12 and I 14) the acceptable method is depending on whether the system will be used for handling national or international Classified Information.

Communications Security

I 01

Secure interconnection of CIS

- Security of the network architecture

Requirement	Source (681/2010)	Source (2013/488/EU)
Protection level IV 1) The information processing environment has been separated from other respective environments 2) The connection of the information processing environment to the one(s) of another protection level requires the use of a firewall in minimum. 3) Data traffic exceeding the perimeter of a controlled physical security area has been encrypted using an encryption solution approved by the Crypto Approval Authority (CAA) for the respective level (see I 12 and I 15). *Protection levels III-II* In addition to requirements 1 and 3 above: 4) The connection of the information processing environment to the one(s) of another protection level requires the use of a boundary protection service approved by the competent authority for the respective level.	1) Section 5(1)(6); Section 16 2) Section 5(1)(6); Section 16 3) Section 5(1)(6); Section 16 4) Section 5(1)(6); Section 16; Section 19	1) Annex IV (32-35) 2) Annex IV (32-35) 3) Article 9(4), Annex IV (32-35) 4) Annex IV (32-35)

Additional information

General

By default the information processing environments are considered to be mutually untrustworthy also in situations where information processing environments administered by different organisations are connected to each other. Information processing environments of the same protection level may be connected through an encryption solution approved by the CAA (e.g. interconnection of physically separated information processing environments of the same organisation through a public network).

Note: when the management traffic (see I 04) exceeds the protection level a gateway solution approved by the respective authority for the upper protection level is to be used. In most of the cases the use of the management traffic is limited to the same protection level.

I 01

Examples

The protection level IV information processing environment may be connected to information processing environments of other protection levels through firewall technology and by limiting the traffic of security critical services (web-browsing, e-mail etc.), which use lower protection level environment, by directing it through separate proxy servers, which filter their content. It is possible to connect the information processing environments of the protection level IV to Internet or other untrustworthy networks, as long as other requirements set for the protection level are fulfilled. A typical use of the protection level IV information processing environment is to use it as a part of the office network of the information processing environment, which may consist of e.g. workstations and data management systems and of the structures used for their protection (firewalls, access control etc.).

From protection level III onwards the connections to environments of different protection level may be done using gateway solutions approved by respective authorities. Design principles and general solution models for gateway solutions which may be approvable have been described in detail in Finnish Communications Regulatory Authority Guidelines for Gateway Solutions; "Ohje hyväksyttävien yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista" (www.ncsa.fi > Asiakirjat > Yhdyskäytäväratkaisuohje). The document is only available in Finnish.

The protection level III information processing environments are separated from untrustworthy networks or systems using a multi-layer logical or physical separation. The definition "physical separation" stands here for the separation put into effect on the physical layer of the OSI-model.

Protection level III information processing environments are normally not connected to other networks/systems. When the end user, based on given duties, has to have access to Internet or to systems/networks of other protection levels, the most reasonable way to achieve this tends to be the use of a separate computer, which has not been connected to the protection level III network. The competent authority may, case by case, accept the connection of the protection level III information processing environment to a network or system, which has been audited and approved before the interconnection will be done. These separately approved networks/systems can be roughly divided into four different use cases:

A. Data transfer systems

Protection level III system or network may be a data transfer system between two or more physical points. In this case each of these points should fulfil the requirements of the level. In most of the cases the network interface is of the form [physically separated network/work station] – [hardware or software firewall] – [crypto device approved to the level] – [hardware or software firewall] – [Internet] – [hardware or software firewall]- [crypto device approved to the level] – [hardware or software firewall] -[physically separated network/work station]. Similar arrangement may be used for protection level II solutions.

B. Service systems

Level III system or network can be e.g. database service used from several physical points. In this case the network level interface follows the case A.

Protection level II information processing environments are by default physically separated entities, to which the data transfer crossing the protection level limits has to go through data diodes or via similar one-way flow regulators operating on physical level of the OSI-model.

I 01

C. Gateway solutions

C1. It is possible to transfer data to level III information processing environment from the one of the lower level through a one-way flow regulator, like a data diode. Similar arrangement may be used for protection level II solutions.

C2. The lower protection level data may be transferred from the protection level III environment to a lower protection level environment using a content filtering solution. The prerequisite for using a content filtering solution is to identify the information content on the upper protection level environment, in order to let only the lower protection level information be transferred from the upper to the lower protection level environment.

D. Other information processing environments

Other level III information processing environments are normally research and development networks of the particular organization, or other level III information processing environments. Connections to such systems may only be from the ones which serve this dedicated environment, such as an update server. Update server may be allowed to deliver security updates or fingerprints of malware with certain restrictions. The deliverable updates or fingerprint bases can be imported to the update server through an airgap or e.g. through a data diode.

Aggregate of Classified Information

An aggregate of Classified Information in information processing environments may warrant a level of protection corresponding to a higher classification than that of its individual components. In the majority of these cases a large amount of protection level IV information in a compiled form creates a protection need equalling the one used to protect level III information. In such a case the protection measures for this information processing environment should follow the requirements set for the level III information processing environment. According to this procedure the access to the information should be limited, following the need-to-know principle, to give access only to the necessary parts of the information. The procedure should also detect unauthorised access attempts to the part of the Classified Information where no need-to-know can be recognised.
When using Katakri as an audit tool this aggregate effect should be interpreted to require the use of a higher protection level physical security measures, such as I 13 (application layer security), I 10 and I 11 (traceability and detection performance), as well as I 06 (separation of duties). It is worth noticing that in cases where the protection level of the pool of information has risen with one level there is no need for an approved gateway solution between the pool of information (e.g. level III) and the terminal equipment (e.g. level IV).

Other sources of information

Finnish Communications Regulatory Authority's Guidelines for Gateway Solutions; "Ohje hyväksyttävien yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista" (www.ncsa.fi > Asiakirjat > Yhdyskäytäväratkaisuohje). The document is only available in Finnish; SANS Critical Security Controls (v5) / 10; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; ISO/IEC 27002:2013 13.1.1; ISO/IEC 27002:2013 13.1.2; VAHTI 3/2012 chapter 2.4 (only in Finnish).

I 02	Requirement	Source (681/2010)	Source (2013/488/EU)
Principle of least privilege – Segmenting of the communication network and the filtering rules within the protection level	The segmenting of the communication network and the filtering rules has to be done following the principles of least privilege and defence-in-depth.	Section 5(1)(6)	Annex IV (16, 18, 19 and 33-34)
	Additional information		
	Example On protection levels IV to II this requirement may be fulfilled by the carrying out the following: 1) communications network has been divided within the protection level into separate network areas (zones, segments) 2) traffic between network areas is monitored and limited in a manner where only such pre-authorised traffic, which is essential for the operation, is allowed (default-deny). 3) information processing environment has been prepared to stand general level network offensives. *General* The division of the communications network into separate network areas (zones, segments) may mean e.g. separating the workstations and servers within the project. The traffic monitoring and limitation between the network areas may be carried out on the boundary of the protection level IV network by e.g. denying all incoming attempts for establishing a connection and by limiting the outgoing connections to web-browsing and email traffic through a proxy server. In networks of all protection levels the adequate consideration of the least privilege principle typically requires that within the protection level only the necessary connections between the network areas are allowed (source-target-protocol) and that other connection attempts are detected. Every connected IT system should be considered untrustworthy and one should be prepared for general network offensives. Preparation for general network offensives includes e.g. that only the necessary functions are kept on. This means that every functionality which is kept on, should be justified by the operation. The functionality should be limited to the narrowest subset which fulfils the operational requirements (e.g. the limitation of the visibility of functionalities). In addition such things as prevention of spoofing and limitation of visibility of networks should be taken into account. At protection level IV also the possibility of a denial of service should be kept in mind in cases where the system will be connected to an untrustworthy network. The filtering should be based on the least privilege principle and it should let through only such traffic which has been approved (default-deny). The functionalities of different protocols (e.g. IPv4, IPv6, GRE, VPN tunnels, routing protocols) should also be taken into account. Unnecessary protocols should be inactivated in all such systems (workstations, servers, network devices etc.) where they have no real operational use. In addition the traffic denial (network, workstation and service levels) should be ensured by filtering rules of the firewalls. In case workstations, servers, network devices and in other similar systems e.g. IPv6 feature is used, the consequences should be taken into account especially in the filtering (firewalls should cover the IPv6 traffic) and routing of traffic. Effects of connecting and multi-use solutions (e.g. IPv4-IPv6 solutions, NAT-64, Teredo) of different protocols should be taken into account in general planning of the network or the system security.		

I 02

Other sources of information

BSI IT-Grundschutz-Catalogues - 13th version - 2013; SANS Critical Security Controls (v5) / 10; SANS Critical Security Controls (v5) / 11; SANS Critical Security Controls (v5) / 13; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; CPNI - Spear Phishing - Understanding the Threat; ISO/IEC 27002:2013 13.1.1; ISO/IEC 27002:2013 13.1.2; ISO/IEC 27002:2013 13.1.3; VAHTI 3/2010 chapter 11; VAHTI 2/2010 Annex 5, chapter 2.5

I 03

Security of information processing environment throughout the life cycle

– Management of filtering and monitoring systems

Requirement	Source (681/2010)	Source (2013/488/EU)
1) The appropriate operation of filtering and control systems will be taken care of throughout the life cycle of the information processing environment. 2) Amendments, changes or removals in the setup of filtering and controlling systems has been organized and tasked. 3) The documentation of the network and the respective filtering and controlling systems is maintained through its life cycle as an inseparable part of the process for administrating modifications and setups. 4) The setup and the desirable operation of the systems filtering and controlling the traffic will be checked periodically during the operation and maintenance of the information processing environment and in exceptional situations.	1) Section 5(1)(2,6) 2) Section 5(1)(2, 6) 3) Section 5(1)(6) 4) Section 5(1)(6)	1) Annex IV (8-12) 2) Annex IV (9) 3) Annex IV (12) 4) Annex IV (11)

Additional information

General

Systems filtering and/controlling the traffic are typically firewalls, routers, IDS/IPS-systems and the ones with similar functionalities (network devices/servers/applications).

To set up an adequate documentation usually requires e.g. the description of the network structure, including the network areas (zones and segments) precisely enough, so that the approval of the network is possible taking into account the structural requirements set by authorities.

In order to ensure the usability and an adequate documentation it is often reasonable to take care of the backups of firewall configurations and to store these backups according to their protection level.

The frequency of inspections for setups and the required actions depends especially on the frequency of the amendments and of the scale of the inspected target. For instance the firewall code of the organisation using a protection level IV information processing environment may be vast and the need for changes may be frequent. In such environments a sufficient inspection frequency could be e.g. after every quarter of the year or twice a year.

On the other hand, in such small scale environments where filtering code does not need constant fine tuning a yearly inspection might do.

Other sources of information

SANS Critical Security Controls (v5) / 10; BSI IT-Grundschutz-Catalogues - 13th version - 2013; ISO/IEC 27002:2013 18.2.1; ISO/IEC 27002:2013 18.2.3; VAHTI 3/2010 chapter 16; VAHTI 2/2010 Annex 5, chapter 2.5

I 04

Secure interconnection of CIS

– Management connections

Requirement	Source (681/2010)	Source (2013/488/EU)
1) Management connections have been segmented on the basis of the protection level, unless a gateway solution approved by the competent authority for the particular protection level is used. 2) In case classified information is embedded to the management traffic and if the traffic has been routed through a lower protection level environment, the classified information has been encrypted using a crypto solution approved by the competent authority. 3) In case the management traffic flow will stay inside the same protection level, the lower protection level encryption or unencrypted transfer may be used based on the results of the risk management process and the exceptional approval by competent authorities. 4) Management connections have been limited according to the least privilege principle.	1) Section 5(1)(6) 2) Section 5(1)(6) 3) Section 5(1)(6) 4) Section 5(1)(6)	1) Annex IV (32-35) 2) Article 9(4); Article 10(6); Annex IV (25) 3) Annex IV (31) 4) Annex IV (16, 18, 19)

Additional information

Example

On protection levels IV to II the requirement can be fulfilled by putting into force the following:

1) There is no connection to the management connections of the information processing environment from the environments of other protection levels unless the gateway solution has been approved by competent authorities (see I 01).
2) The workstation used for management is connected to the device or interface through a crypto solution approved by the competent authority (see I 12) to the respective protection level in situations, where the management traffic is routed through a lower protection level environment
3) In situations where the management traffic will stay within the respective protection level,
   a) the management workstation of the respective protection level is connected to the device or interface physically (with e.g. console cable), or
   a) the traffic channel of the management connection of the respective protection level has been protected in some other reliable way (e.g. cabling within a technically protected area), or
   a) the management workstation of the respective protection level is connected to the device or interface using a lower level crypto solution (e.g. SSH, HTTPS, SCP) to protect the connection
4) Only the management contacts from the sources following the least privilege principle are allowed to the devices or interfaces.

I 04

General

In this context the devices or interfaces mean systems where the management rights should be limited only to the personnel responsible for the maintenance or similar duties. These include typically the firewalls, routers, switches, wireless base stations, servers, workstations, ILO-management interfaces and management interfaces of Blade enclosures.

When assessing the protection of management connections, especially the risk of the disclosure of classified information through the management connection should be taken into account. Most of the management connection means make it possible to access classified information either directly (e.g. database management usually has access to the content of the database) or indirectly (e.g. network device maintenance usually can change the firewall settings). Especially in situations where the management connection provides a direct or indirect access to classified information the management connection and the terminals connected to it should be kept on the same protection level as the information processing environment.

The management of a lower protection level environment may in certain cases be possible from the upper protection level management environment, if at the boundaries of the protection levels a gateway solution approved by the competent authority for the respective protection level is used to block the information flow from the upper protection level to the lower level environment. Due to the security critical nature of the management traffic, by default it is not possible to manage the upper protection level environment from the lower protection level environment. From the upper protection level environment it is possible in some cases, through a gateway solution approved by competent authorities, to offer a read-only control access for the environment which is on one protection level lower.

In order to achieve an adequate traceability within the protection level it is possible to use the so called jump machine procedure, in which all management actions are executed and registered (into logs) through the jump machine. The prerequisites of remote management are described more in detail in the requirement I 24.

Other sources of information

FICORA document “Ohje hyväksyttävien yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista”, in Finnish only; SANS Critical Security Controls (v5) / 10; SANS Critical Security Controls (v5) / 13; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; ISO/IEC 27002:2013 13.1.1; ISO/IEC 27002:2013 13.1.2; ISO/IEC 27002:2013 13.1.3; VAHTI 3/2010 chapter 16.

I 05	Requirement	Source (681/2010)	Source (2013/488/EU)
Exchange of classified information outside the physically protected areas - Wireless networks	The radio frequency interfaces of wireless networks are treated in a similar way as public networks.	Section 5(1)(6)	Article 9(4); Annex IV (33 and 35)

Additional information

Example

On protection levels IV to II the requirement can be fulfilled by putting into force the following:
The data traffic going through wireless network will be encrypted with the method which has been approved to the respective protection level by competent authorities (I 12).

General

Usage of radio frequency interface on wireless network connections (e.g. WLAN, 3G) will be interpreted as a dismissal from a physically protected area. This means that the use of the radio frequency interface will be judged equal to the traffic exchanged in public networks, which should be taken into account when choosing the encryption method (see I 12).

Other sources of information

SANS Critical Security Controls (v5) / 15; SANS Critical Security Controls (v5) / 7; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0;

System Security

I 06

The principle of least privilege

– Management of access rights

Requirement	Source (681/2010)	Source (2013/488/EU)
1) CIS users and automated processes shall be given only the access, privileges or authorisations they require to perform their tasks. 2) Unauthorised modifications or other unauthorised or inappropriate handling of classified information is prevented through access control management and the appropriate use of security controls within the IT system.	1) Section 5(1)(5,6) 2) Section 5(1)(6)	1) Annex IV (19) 2) Annex IV (16, 19, 32-35)

Additional information

Example

On protection level IV the requirement can be fulfilled by putting into force the following:

1) Usage rights management for systems has been tasked.
2) Users of the system have been listed.
3) When granting the usage rights for the system the target personnel has been verified to be part of the organisation or is authorised to use the system based on other facts.
4) Administration of user rights has been organised.
5) There is a clear and well-functioning way to handle the changes in the personnel by immediately informing all relevant players of the field to take action.
6) Every user right issuance is documented (electronically or in paper format.
7) User and access rights are regularly audited.
8) Classified information in the information processing system is separated according to the principle of least privilege by using user right definitions and handling regulation or other respective methods.
9) Within the information processing system classified information are kept separated from public information or from the information classified to another protection level, or the information mass is handled according to the requirements set for the highest respective protection level.
10) Information which may or will be a target for inspections performed by the originator or the owner of the information are kept separate from each other using the method approved by the competent authority for the respective protection level.

On protection levels III and II the requirement can be fulfilled by putting into force the following, in addition to the functions described above (1-10):

11) Tasks and areas of responsibility are separated from each other as well as possible in order to reduce the risk of unauthorized or accidental alterations or misuse of the classified objects. In case critical working combinations will be probable, they have to be under monitoring.
12) The classified information used in servers, workstations and in other storage media is stored using the encryption method approved for the particular technical environment (see I 12). The authority may, case by case, accept the use of a replacing method where the encryption solution will be replaced with the combination of physical and logical access control and by the use of trustworthy management of storage media (see F 02, points 6 and 11). Note! This replacing procedure cannot be used in situations where the information may or will be a target for inspections performed by the originator or the owner of the information, as the separation may be insufficient.

I 06

Verification on the validity of access rights

In order to verify the validity of access rights it is important to inspect the user and access rights on a regular basis, like every 6 months. When the characteristics in working positions change, which happens through promotions or resignations, these changes should be taken into account in a clear and well-functioning way. Such a clear manner can be the procedure where the foreman informs people responsible for managing access or user rights in advance. This may mean in practice that access and user rights are deleted or changed using a centralised managing system or by executing the changes in several systems one by one.

Separation of duties

An adequate separation of duties is largely depending on the use of the particular system. In most of the systems an adequate separation of duties may be achieved by separating the maintenance roles of the system (and users) from the ones of log (and user) surveillance. It is quite typical also to use several people for critical maintenance and other respective tasks (two man rule).

Taking the inspection rights into account in technical solutions

Owners of the classified information often reserve a possibility to inspect all such systems which handle their information. In many cases these inspections require both physical and logical access to the target under inspection, and therefore the inspectors often have a technical possibility to access the information itself. Especially in multiproject networks and in other demanding environments, where there is a need to handle the information belonging to multiple owners it should be verified that the system has been designed to make these inspections possible in a way where the inspectors don't have access to the information which don't belong to them.

Information belonging to different owners may be separated according to three main classes:

a) For the protection level IV information a logical level separation (like virtualisation of servers and user right separation of network storage media) is normally sufficient.
b) For the information belonging to protection levels IV and III the methods which are based on a reliable logical separation (like virtual machines with approved crypto on a dedicated, customer based disks and an approved encryption of the information or data flow on multiuse network devices
c) For the information belonging to protection levels IV, III and II a solution based on physical separation (dedicated physical devices) may be used.

Note: the requirement for the separation of information is not valid for the protection level IV in workstations or in other very limited data masses, taking into account that there is a reliable method in use to avoid the aggregation (see I 19, point 3). Information belonging to those who have reserved a right to inspect the handling procedure of their information may be kept unseparated in cases where all owners of the information have in advance given their written consent to accept the risks cumulating of this inspection right.

I 06

Other sources of information

SANS Critical Security Controls (v5) / 15; SANS Critical Security Controls (v5) / 3; SANS Critical Security Controls (v5) / 12; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; Finnish National Security Authority manual for handling International Classified Information (in Finnish only); ISO/IEC 27002:2013 6.1.2; ISO/IEC 27002:2013 9.1.1; ISO/IEC 27002:2013 9.1.2; ISO/IEC 27002:2013 9.2.1; ISO/IEC 27002:2013 9.2.2; ISO/IEC 27002:2013 9.2.3; ISO/IEC 27002:2013 9.2.4; ISO/IEC 27002:2013 9.2.5; ISO/IEC 27002:2013 9.2.6; ISO/IEC 27002:2013 12.5.1; VAHTI 2/2010 chapter 8.9; VAHTI 2/2010 Annex 5 chapter 2.7

I 07

Defence-in-Depth - Identification of actors of the information processing environment within a physically protected area

Requirement	Source (681/2010)	Source (2013/488/EU)
Reliable methods to identify the actors of the information processing environment have been taken into use.	Section 5(1)(5,6); Section 14, Section 20	Annex IV (16, 19)

Additional information

Example

On protection level IV this requirement may be fulfilled by using following procedures:

1) Individual user identifiers are in use.
2) All users are identified and authenticated.
3) In authentication and in identification a well-known and reliable technique is used or the requirement has been covered in another reliable way.
4) Too many false attempts in the identification will result in the locking of the identifier.
5) Maintenance identifiers for systems and applications are personal. In case this is not technically possible, documented and settled password management procedures are required for identifiers in used my multiple persons.
6) The authentication is done at least by the use of passwords. In case password authentication is in use, a) users have been notified about good practices in choosing and using the password, b) the application monitoring the usage sets up certain minimum requirements for the password and requires that the password will be changed regularly.

On protection levels III and II the requirement can be fulfilled by putting into force the following, in addition to the functions 1 to 5 described above:

7) A strong user identification method is required, based on at least two identification factors.
8) Terminals are technically identified (device identification, 802.1X or equal procedure) before allowing to access the network or the service, unless the access to the network has been limited with physical means (e.g. setting the server in a locked rack cabin inside a technically protected security area which has been approved by a competent authority for the respective protection level).

I 07	*General* Protection level IV environments, in which a threat of a Denial of Service is eminent (e.g. locking of identifiers on Internet connected identification services), the locking of the identifier may be replaced with some other method reducing the risk (e.g. methods of slow reply, filtering or a temporary locking). On protection level IV a terminal based technical identification is normally not necessary, as long as the users are identified. The methods of strong identification and identification of the device on protection levels III and II may in some cases be realised by limiting the access to the system only from a physically protected area (in most of the cases either a technically protected security area, a locked rack cabin or equivalent) with a strong access control system, based at least on two identification factors. In such a case the identification of the user of the information processing system may be based on the double method of user id and password. Setting up a reliable identification and authentication procedure contains at least i) the authentication method has been protected against man-in-the-middle manoeuvres ii) on the log in phase, before the actual authentication of the user, no additional information is revealed iii) the credentials used for authentication will always be on an encrypted format in cases where they will be sent over the network iv) the method of authentication is protected against repetitive transmission attacks v) the authentication method has been protected against brute force attacks. *Other sources of information* BSI IT-Grundschutz-Catalogues - 13th version - 2013; SANS Critical Security Controls (v5) / 15; SANS Critical Security Controls (v5) / 12; SANS Critical Security Controls (v5) / 1; SANS Critical Security Controls (v5) / 16; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; ISO/IEC 27002:2013 9.1.2; ISO/IEC 27002:2013 9.4.1; ISO/IEC 27002:2013 9.4.2; ISO/IEC 27002:2013 9.4.3

I 08

Principle of minimality and of least privilege

- Configuration with dedicated system parameters

Requirement	Source (681/2010)	Source (2013/488/EU)
1) Only the essential functionalities, devices and services to meet operational requirements shall be implemented in order to avoid unnecessary risks. 2) Organisation uses a procedure through which systems are installed and configured systematically, resulting on a hardened installation, following the configuration rules set by the organisation itself. 3) Configuration contains only such components, services, user and process rights which are mandatory in order to fulfil the operational as well as the security requirements.	Section 5(1)(6)	Annex IV (16, 18,19)

Additional information

Example

On protection level IV this requirement may be fulfilled by using following procedures:

Active components of the network

1) Default passwords have been changed to quality ones which fulfil the password policy of the organisation.
2) Only necessary network services are used and these services have been limited only to the necessary network connections.
3) Necessary security updates have been installed on software of network devices.
4) Management is not possible without user identification and authentication.
5) Time-out procedure should be used in management connections.
6) Configurations are based on trustworthy configuration guidelines or instructions.

Servers, workstations or equivalent

7) The services provided (especially network services) are set to minimum and limited only to the crucial ones. In addition a host-based firewall solution limiting the network traffic to the essential is in use.
8) The platform consists only of the software elements necessary for the system. User rights for the platform components, processes (e.g. server processes), directories and add-on software are set up according to the principle of least privilege.
9) Necessary security updates have been installed on the operating system and on application software.
10) Access rights to user accounts automatically created when installing the system (e.g. “administrator” and “guest”) are limited to minimum or removed from use.
11) Default passwords have been changed to quality ones which fulfil the password policy of the organisation.
12) The system lock up automatically, if not used for certain period (e.g. a password protected screen saver activates after 15 minutes of idling time).
13) User rights are set up according to the principle of least privilege (see I 06).

I 08

14) The known security risks of the operating system that use automatic running of programme code have been switched off (especially the automatic preview of PDF files and the autorun and autoplay functions, as well as the prevention of auto-start of USB and Firewire devices when the device is locked.
15) Software applications, especially web-browsers, PDF readers, office software and e-mail applications are configured in a secure manner. On application configurations the prevention of default run code (e.g. JavaScript and macros) should have special emphasis.
16) Access to the BIOS setup has been protected with a password (on protection level IV especially concerning NATO RESTRICTED information)
17) Additional security features supported by the system (e.g. DEP/ASLR/Applocker/SELINUX) are used.

On protection levels III and II this requirement may be fulfilled by using following procedures in addition to the points 1-17 above:

Active elements of the network

18) Unnecessary network plugs (or equivalent) have been removed from use.

Servers, workstations or equivalent

19) Operating systems and other programmes are configured to download updates only from the source specified for the purpose and all unnecessary network traffic is prevented in order to allow more efficient monitoring of anomalies.
20) BIOS-settings are set to meet the security requirements and the changing of the settings is prevented from unauthorised users. In addition to the use of password: a) boot up is allowed only from primary hard disk, b) unnecessary services and ports are removed from use.

General

Systems refer to servers, workstations, active components of the network and equivalent devices. Active network devices refer to firewalls, routers, switches, wireless base stations and equivalent devices / systems. Security configuring of the system means in general terms the changes to the setup in a way where the area of vulnerability of the system diminishes. In general only the essential functions, devices and services should be taken into use in systems. Respectively for instance automated processes should have access only to that part of data, privileges or authentications which are necessary for their tasks in order to limit the damages caused by accidental, erroneous or unauthorised use of system resources. The necessary security configuring of servers, workstations or equivalent devices can be done following, for instance USGCB or equivalent level (e.g. SSLF in Microsoft environment). In case the handling of classified information includes the use of network printers, phone systems etc., the principles mentioned above should cover also these systems.

Compensatory methods

When the control of the network device is not technically possible through the individual user ID, the procedure which allows the access to the password only through two simultaneous personal IDs has to be covered in user rules. When the size of the environment is considered to be large, the authentication is recommended to be done by using duplicated AAA-servers (especially TACACS+, RADIUS or Kerberos.

I 08

Other sources of information

SANS Critical Security Controls (v5) / 3; SANS Critical Security Controls (v5) / 10; SANS Critical Security Controls (v5) / 11; SANS Critical Security Controls (v5) / 13; SANS Critical Security Controls (v5) / 5; SANS Critical Security Controls (v5) / 6; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; The United States Government Configuration Baseline (USGCB); NATO Best Practice Configuration Guidance; IASE Security Technical Implementation Guides (STIGs); NIST Special Publications (800 Series); Microsoft Security Compliance Manager; Apache Security Tips; ModSecurity; Cisco Security Configuration; VAHTI 3/2012 chapter 4.2.1; VAHTI 3/2010 chapter 7

I 09

Defence-in-depth

– Protection against malware

Requirement	Source (681/2010)	Source (2013/488/EU)
Reliable methods for deterrence, prevention, detection, resilience and recovery measures of malware are used in the information processing environment in order to prevent unauthorised changes and other unauthorised use of the information.	Section 5(1)(6)	Annex IV (8, 9, 16, 18, 19, 21, 22)

Additional information

Example

On protection level IV this requirement may be fulfilled by using following procedures:
1) Malware prevention software (anti-malware) has been installed to all such systems which are vulnerable to malware infections.
2) Anti-malware is running and able to act.
3) Anti-malware produces logs of its functions and gives alarms.
4) Malware fingerprints (and respective) are updated regularly.
5) Users have been instructed about the threats caused by malware and about the procedures following the information assurance principles of the organisation.
6) Malware detection and alarms are monitored regularly and they cause reaction
7) Organisation filters malicious traffic at least on the gateways of e-mail and WWW-traffic.

On protection levels III and II this requirement may be fulfilled by using following procedures in addition to the points 1-7 above:
8) It is considered whether the use of USB-ports or other interfaces are needed.
9) If no essential reason can be found after a critical evaluation, the interfaces are removed from use.
10) In cases where a reason can be found after a critical evaluation, the estimation is done case by case to define the prerequisites and conditions for devices and media (like USB-sticks) to be connected to the system.

I 09	*General* Anti-malware may be left uninstalled in environments where the malware access has been prevented in a particular manner (e.g. systems without input/output interfaces or strictly limited interfaces in which a reliable validation or sanitation of the information is performed. *Environments restricted from public networks* In systems that are not connected to public networks the updates of malware fingerprints can be organized by using e.g. controlled and protected update download server, the fingerprint base of which is kept updated from e.g. a separate system connected to the Internet and by transferring the fingerprints manually (e.g. once a day) or by bringing in the fingerprints through an approved gateway solution (see I 01). Note: there should be a manner to verify the integrity of updates (source, checksums, signatures etc.). The requirement may be set on a case by case basis to ensure that USB-ports (or other respective interfaces) may be used to connect a specifically defined and approved USB-stick (or equivalent) to the system in case they are not connected to any other system. Case by case requirements may, for instance, include an arrangement where only such storage media which has been delivered by the ICT management of the organisation may be used, whereas the connection of all other storage media is prohibited or technically prevented. On cases where there is a specific need to import information from untrustworthy sources by using storage media, there prerequisite to use such an exceptional manner usually includes definitions of methods to decrease the risk. One possible method would be the connection of the storage media to an isolated inspection system from where the information would then be transferred after a temporary storage to a separate storage media, which would be used to import the information into the trusted system. On such arrangements on level III at least the memory area has to be inspected and from level II on also the controller level tailored threats are to be taken into account. *Other sources of information* SANS Critical Security Controls (v5) / 5; SANS Critical Security Controls (v5) / 17; SANS Critical Security Controls (v5) / 2; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; ISO/IEC 27002:2013 12.2.1; VAHTI 2/2010 Annex 5, chapter 2.8

I 10

Defence-in-depth

- Traceability of security events

Requirement	Source (681/2010)	Source (2013/488/EU)
In order to detect unauthorised changes or other unauthorised or inappropriate information handling within the information processing environment, reliable methods have been taken into use for tracing the security events.	Section 5(1)(6); Section 20	Annex IV (16), Annex III (18, 21)

Additional information

Example

On protection level IV this requirement may be fulfilled by using following procedures:
1) Logs make it possible to detect the security breaches or attempts to such afterwards.
2) Essential recordings are stored at least 6 months, unless laws and regulations or separate contracts define a longer storage period.
3) Log files and respective register services are protected against unauthorised access (user rights management, logical access control).
4) A policy document defining the generation, release, alarm and follow up of the logs have been taken into the actual use. This policy has been written taking into account the particular operational requirements.

On protection levels III and II this requirement may be fulfilled by using following procedures in addition to the points 1-4 above:
5) Essential recordings are stored at least from 2 to 5 years, unless laws and regulations or separate contracts define a longer storage period
6) Log files are backed up regularly.
7) Clocks of all relevant information processing systems within security domain must be synchronised to a single reference time source.
8) System covering the integrity of the logs has been taken into use.
9) Handling and usage of the log files are registered.

General

Essential recordings typically include the log data of fundamental network devices and servers. Also the log data of e.g. workstations etc. is often covered by the definition. The requirement of the coverage can in most cases be fulfilled by checking that at least the logging is on for workstations, servers, network devices (especially firewalls, but also for software barriers/walls in workstations). From network device logs it should be possible to confirm afterwards what kind of administrative functions the network device has gone through, when and by whom. Event logs should be gathered of the use of the system, of user activities, of functions and exceptions dealing with security. A recommended method to protect the logs is to forward all logging information in a centralised manner to a specific, strongly safeguarded logging server, the information content of which is periodically backed up.

I 10	On workstations and servers the implementation often needs the logging to be switched on and the default values of storage duration and mode to be changed. For instance in some of the Windows environments this usually means that on Audit Policy settings at least the following features have to be switched on (for unsuccessful and successful events): ■ audit account logon events ■ audit account management ■ audit logon event ■ audit object access ■ audit policy change ■ audit privilege use ■ audit system events. In the implementation to workstations and to servers it should be taken into account that the duration and storage capacity of the logs will be sufficient (normally needs to be increased). Recommendation: to reserve enough capacity based on the estimation according to the system environment. To define an adequate duration can be done by e.g. calculating the storage capacity sufficient for one month and using this information to determine the storage capacity needed for the storage duration. Note: it is advisable to reserve some buffer capacity, as situations change and because certain type of cyber-attacks increase log activities a lot. *Other sources of information* SANS Critical Security Controls (v5) / 14; SANS Critical Security Controls (v5) / 16; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; The United States Government Configuration Baseline (USGCB); ISO/IEC 27002:2013 12.4.1; ISO/IEC 27002:2013 12.4.2; ISO/IEC 27002:2013 12.4.3; ISO/IEC 27002:2013 12.4.4; ISO/IEC 27002:2013 18.1.3; VAHTI 3/2009

I 11

Defence-in-depth

- Incident detection and recovery

Requirement	Source (681/2010)	Source (2013/488/EU)
Reliable methods are taken into use in the information processing environment in order to detect attacks against the information processing environment, to limit the effect to a minimum amount of the information and to minimum resources of the information processing environment and to prevent other damages, as well as to restore the protected status within the information processing environment.	Section 5(1)(6); Section 20	Annex IV (16)

Additional information

Example

On protection levels IV to II this requirement may be fulfilled by using following procedures:
1) The base line of the network traffic (amount of traffic, protocols and connections) are known.
2) A procedure is in use to detect abnormal events in the network traffic (e.g. abnormal connections or intentions for such).
3) A procedure is in use to detect abnormal activities on logs (see I10). Especially an unauthorised attempt to start-up of the system has to be detected.
4) A procedure is in use to recover from the detected incidents.

General

There are numerous solutions how to solve the detection of the network traffic and to limit the detected attack, starting from the monitoring on the network node level down to workstation/server sensors and to their combinations. Regardless of the network devices or operators the actual capability to detect changes on the network level requires understanding of the normal status of the network traffic.

On protection level IV the detection capability on the network traffic level should cover specifically the outmost border of the network or the target. From the protection level III on the gateway solution should be used on the outer border, as well as the traffic inside the network or other object should be monitored.

To detect an attack or an intention of misuse, the use of automated detection and alarm tools can be seen as a requirement in most of the environments. Manual inspection of logs is sufficient only on environments where the log masses are very limited and there is enough manpower to study the logs.

To restore the protected status of the information processing environment in a decent time frame, planned, described, trained and rehearsed processes and technical methods are normally required.

Other sources of information

SANS Critical Security Controls (v5) / 14; SANS Critical Security Controls (v5) / 16; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; ISO/IEC 27002:2013 12.4.1; ISO/IEC 27002:2013 13.1.1; ISO/IEC 27002:2013 16.1.4; ISO/IEC 27002:2013 16.1.5; VAHTI 3/2009

I 12

Evaluation and approval of cryptographic products

- Crypto solutions

Requirement	Source (681/2010)	Source (2013/488/EU)
Competent authority has approved crypto solutions or products in current environment to the respective protection levels in order to safeguard and protect the information against unauthorised disclosure or loss of integrity.	Section 5(1)(6); Section 16; Section 19 §	Article 10(6), Annex IV (25)

Additional information

Example

On protection levels IV to II this requirement may be fulfilled by using following procedures:

1) The safeguards on a particular protection level have been implemented through a) crypto solutions approved by competent authorities are used according to the user policy and respective specifications, or b) case by case approvals and user policies or specifications set by competent authorities for crypto solutions which have not been accredited in advance.
2) Secret keys can be used by authorised users and processes only. Crypto management processes and practices have been documented and appropriately executed. Processes require at least a) cryptographically strong keys b) secure key delivery, c) secure storage of keys, d) regular key changes, e) changes of outdated or revealed keys, f) prevention of unauthorised key changes.

General

When evaluating crypto products several aspects are taken into account. In addition to verify the strength of the algorithm and the correct functioning of the crypto product, also the threat level of the user environment is taken into account. For instance on situations where the traffic will be transferred over internet the threat level differs a lot compared to the situation where the encryption is used to encipher the information handled inside a controlled physical area (e.g. transferring SECRET information through physical protection level III area from one physical area belonging to the protection level II to another similarly protected area. Other aspects which are taken into account while evaluating crypto products contain e.g. operative needs for the integrity or for the confidentiality period before disclosure is acceptable.

Crypto approvals of several international security authorities require that the correct functioning of the product will be evaluated, as well as the fulfilment of particular requirements concerning e.g. the delivery and evaluation of the source code, tampering and TEMPEST countermeasures. Pure software crypto solutions may typically be approved on protection level IV and in some cases on level III. For protection level II and usually also for level III reliability requirements for the technical platform are set.

The protection effect of encryption may be lost completely or partially in situations where the weaknesses of the crypto key management can be used by the unauthorised personnel.

Other sources of information

List of crypto products approved by the Council of the European Union; List of crypto products approved by NATO, List of crypto products approved by the national Crypto Approval Authority (FICORA); Finnish National Security Authority manual for handling International Classified Information (in Finnish only), SANS Critical Security Controls (v5) / 17; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; ISO/IEC 27002:2013 10.1.1; ISO/IEC 27002:2013 10.1.2; ISO/IEC 27002:2013 18.1.5; VAHTI 3/2010 chapter 12.

I 13

Defence-in-depth throughout the lifecycle

- Software based access control

Requirement	Source (681/2010)	Source (2013/488/EU)
1) Any CIS, including its technical and non-technical security measures, shall be subject to security testing during the accreditation process to ensure that the appropriate level of assurance is obtained and to verify that they are correctly implemented, integrated and configured. 2) In order to detect and prevent unauthorised changes of the information, as well as other unauthorised or inappropriate handling of the information within the information processing environment, reliable methods are to be used for the security of software based access control management.	Section 5(1)(6); Section 6	1) Annex IV (8, 9, 10, 16, 19, 33) 2) Annex IV (10,19)

Additional information

Example

On protection levels IV and III this requirement may be fulfilled by using following procedures:
1) Services/applications/systems should be accomplished in a way where the requirements of secure programming are met. The contractor should provide details of how these requirements have been taken into account in the development of the product.
2) Contractor of services/applications/systems will be given binding requirements to take corrective actions throughout the entire lifecycle of the service or the application, or there will be another way to correct the security related findings; and
3) Interfaces of the service/application/system have to be able to stand against the most common attacks without the confidentiality of the information used in services or applications would be endangered.

On protection level II information this requirement may be fulfilled by using following procedures in addition to the above mentioned points 1 to 3:
4) Each code having serious effect on the security of the service/application/system is available for the inspection (e.g. back doors, unsecure completions).

General

This requirement is valid especially in situations where the security of the implementation of access control to the classified information relies on a programme. Most of these cases are related to dedicated document management systems, web applications and similar cases. On protection level IV this requirement is valid in situations where the access to the service/application/system having a role in the protection of the information can be established from an untrustworthy network (e.g. internet). Same goes with service/application/system where the aggregate effect plays a role (typically e.g. information management and documentation storage systems). From protection level III on this requirement is valid also when the access is through trusted networks.

I 13	The following requirements may be set for the software producer: 1) Information assurance knowledge of software developers has been verified. 2) During the software development phase a risk analysis has been carried out and the potential risks have been dealt with (either controlled or deliberately accepted). 3) Interfaces (at least the external ones) have been tested with false input and with large quantity of feedings. 4) Depending on the developing environment there is a policy in use for such functions and interfaces which easily create problems and this policy is monitored (e.g. Microsoft has lists of denied functions). 5) Architecture and the source code are audited. 6) Programme code is inspected with automated static analysis. 7) Integrity of programme code version management and development tools has been verified. In addition it is recommended that the documentation of the programmes to be purchased is able to provide information at least of the network ports used by the programme and of dependencies to other programme components (like the toolkits used by the programme). It is recommended also that 1) applications use a small amount of designated ports 2) applications using dynamic ports use only a small port space, and 3) programmes don't require large user rights to function (i.e. programmes have to run with the rights of a basic user). Filtering functionalities of programmes may be supported and/or realised also with, e.g. web application firewalls (WAFs). See I 502.0. *Other sources of information* SANS Critical Security Controls (v5) / 6; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; CPNI - Development and Implementation of Secure Web Applications; CPNI - Security Questions to Ask Your Vendor; OWASP Top Ten Project; OWASP Application Security Verification Standard Project; CWE/SANS TOP 25 Most Dangerous Software Errors; The Building Security In Maturity Model; Software Assurance Maturity Model; ModSecurity; ISO/IEC 27002:2013 14.1.1; ISO/IEC 27002:2013 14.1.2; ISO/IEC 27002:2013 14.1.3; ISO/IEC 27002:2013 14.2.8; ISO/IEC 27002:2013 14.2.9; VAHTI 1/2013

I 14

Defence-in-depth – Electromagnetic radiation (TEMPEST)

Requirement	Source (681/2010)	Source (2013/488/EU)
Security measures shall be implemented to protect CIS handling classified against compromise of such information through unintentional electromagnetic emanations ('TEMPEST security measures'). Such security measures shall be commensurate with the risk of exploitation and the level of classification of the information.	Section 16; Section 5(1)(6)	Article 10(5)

Additional information

General

On protection level IV there are no defined requirements. On protection levels III and II the electromagnetic radiation which exceeds the limit will be set under control using the respective methods approved by competent security authorities.

In cases where EU classified information is concerned, the National TEMPEST Authority (NTA) is the Finnish Communications Regulatory Authority. On protection level III compensative protection measures may be more widely approved.

The adequacy of counter measures may be verified by facility zoning measurement or by shielded enclosure measurement.

Other sources of information

Finnish Communications Regulatory Authority Instruction on EMR Protection "Sähkömagneettisen hajasäteilyn aiheuttamien tietoturvariskien ehkäisyn periaatteet" (in Finnish only); BSI IT-Grundschutz-Catalogues - 13th version - 2013; ISO/IEC 27002:2013 11.2.3; VAHTI 2/2010 chapter 4.4; VAHTI 3/2012 chapter 3.2; VAHTI 2/2013 chapter 3.1.3

I 15

Exchange of classified information between physically protected areas

- Electronic transformation of the information

Requirement	Source (681/2010)	Source (2013/488/EU)
1) When classified information is transferred outside physically protected areas, the information or the traffic is enciphered with a method approved by the competent authority to the respective protection level. 2) When transmission of classified information is confined within physically protected areas, unencrypted transmission or encryption at a lower level may be used based on the outcome of a risk management process and subject to the approval of the competent authority.	1) Section 5(1)(6); Section 19 2) Section 5(1)(6)	1) Article 9(4) 2) Annex IV (31)

Additional information

Example

On protection levels IV to II this requirement may be fulfilled by using following procedures:

1) When transferring classified information outside physically protected areas approved for the level, the requirements set in I 12 and in 21 should be taken into account.
2) In situations, where classified information is transferred within physically protected areas,
   a) traffic channel of respective security level has to be physically protected (e.g. cabling which stays inside a physically protected area, perhaps within a single room, approved for the respective protection level) or
   b) information is encrypted with a lower level encryption product, based on a separate approval by the competent authority (e.g. HTTPS).

General

This requirement covers telephones, facsimiles, email, rapid messages and other similar information network based transfer methods. Requirements for the storage media (hard drives, USB-memories etc.) containing classified information are set on requirement I 22.

The use of radio-interface on wireless network connections (e.g. WLAN, 3G) is understood as a dismissal from the physically protected area. This means that the radio-interface of wireless networks should be handled in a similar manner as a public network. See I 05.

Other sources of information

SANS Critical Security Controls (v5) / 15; SANS Critical Security Controls (v5) / 17; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; Finnish National Security Authority manual for handling International Classified Information (in Finnish only); ISO/IEC 27002:2013 11.2.3; ISO/IEC 27002:2013 13.2.1; ISO/IEC 27002:2013 13.2.3; VAHTI 3/2010 chapter 12

I 16

Transfer of classified information between physically protected areas

- Delivery by mail or by courier

Requirement	Source (681/2010)	Source (2013/488/EU)
When transferring information between working units or office areas which are located outside of physically protected areas the following has to be taken care of: 1) As a general rule, classified information is transmitted by electronic means protected by cryptographic products approved by the competent authority over the data network. 2) In case the above mentioned method is not used, classified information is either carried a) with encrypted electronic storage media (USB-sticks, CD-disks, hard drives), or b) in all other cases following the instructions given by the respective authority.	Section 5(1)(6), Section 6; Section 18	Article 9(4)(4), Annex III (28-41)

Additional information

Example

On protection level IV this requirement may be fulfilled by using following procedures:
1) Classified material will be packed in an envelope or in other closable package. Packages are not marked with classification marking and they may not reveal from outside that they contain classified information (non-transparent envelopes or packages).
2) Classified material may be transferred within Finland by regular mail, in a registered form or by using a courier procedure approved for the particular protection level. Outside Finland regular mail is used only after an approval by the respective authority.
3) Internal mail handling chain within the organisation consists only of approved personnel.
4) Organisation has recognized the requirements for the transfer of items requiring special attention (e.g. crypto keys) and the required measures have been taken into use.

On protection level III this requirement may be fulfilled by using following procedures in addition to the point 4 above:
5) Classified information or material is carried as registered post in a non-transparent double envelope (or equivalent). The outmost envelope may not contain any sign of a classification and may not reveal from outside that they contain classified information.
6) Classified material may be transferred within Finland by registered mail in a registered form only after a separate approval of the authority in charge or by using a courier procedure approved for the particular protection level. Outside Finland mail may be used only after an approval by the respective authority.
7) Internal mail handling chain within the organisation consists only of security-cleared personnel.

On protection level II this requirement may be fulfilled by using following procedures in addition to the points 4 and 7 above:
8) Classified information or material is carried as registered post in a non-transparent double envelope (or equivalent). The outmost envelope may not contain any sign of a classification and may not reveal from outside that they contain classified information. The inner envelope has to be sealed. The receiver has to be instructed to inspect the integrity of the seal and to inform the sender if there is any doubt about the integrity.
9) Within and outside Finland a courier procedure approved for the particular protection level by the respective authority may be used.

I 16	*General* Classified material may also be delivered personally in case the transfer will take place within physically protected areas (in more detail: I 22), bearing in mind the requirements set for the particular protection level. Certain part of international or domestic classified information belonging to protection level III will never be delivered by mail. The approved methods have to be confirmed by the respective authorities. For instance NATO CONFIDENTIAL information may not be send by mail in a clear mode, not even in registered mail. It will be transferred either personally or by using the courier services approved by competent authorities. The National Security Authority will give further guidance when needed. Classified material may be transferred in an electronic format within Finland or outside Finland in a chosen manner in case the information has been encrypted inside protected environment, using a crypto product which has been approved for the respective protection level by the competent authority. *Other sources of information* BSI IT-Grundschutz-Catalogues - 13th version - 2013; Finnish National Security Authority manual for handling International Classified Information (in Finnish only); ISO/IEC 27002:2013 13.2.1

I 17	Requirement	Source (681/2010)	Source (2013/488/EU)
Security throughout the information processing environment lifecycle - Copying and printing of classified information	*Protection levels IV and III* 1) The security measures applicable to the original document shall apply to copies and translations thereof. *Protection level II* In addition to point 1 2) Copies produced of the material belonging to protection level II have to be listed or numbered.	1) Section 5(1)(6); Section 6; Section 13; Section 16; Section 17 2) Section 17	1) Annex III (27); Article 9(1); Article 7 (1); Article 8 (5) 2) Annex III, (13, 18, 19)

Additional information

Example:

On protection levels IV and III this requirement may be fulfilled by using following procedures:
1) Copies are handled in a similar way as the original document.
2) Copies can be further released only to people who have a right to access and need-to-know to the information-
3) A copy or a print-out is allowed to be produced only with the device approved for the respective protection level.

On protection level II this requirement may be fulfilled by using following procedures in addition to the points 1 - 3 above:
4) Information of copies is marked on a diary or registers or is listed in some other respective manner.

General

Printers and copy machines are considered to be information processing systems and therefore they should be subject to similar security measures in fulfilling technical, physical and administrative security requirements.

Other sources of information

BSI IT-Grundschutz-Catalogues - 13th version - 2013; VAHTI 2/2010 chapter 8.4

I 18

Security throughout the information processing environment lifecycle

- Registering of classified information in safeguarding purpose

Requirement	Source (681/2010)	Source (2013/488/EU)
Protection level IV 1) Administrative and technical measures are taken in the information processing environment aiming at safeguarding of classified information throughout the lifecycle in order to detect and prevent the disclosure of such information accidentally or on purpose. *Protection levels III and II* In addition to point 1 2) A registration point or a diary has been dedicated for departments or other units in the organisation which handle classified information. Registration points or diaries have been established on physically protected security areas. 3) Classified information is registered in registration points or in diaries when the classified information is received or will be sent out. 4) Handling of classified information will be registered either on electronic log, information processing system, document management system, manual diary, or document.	1) Section 20, Section 5(1)(6,7); Section 6; Section 14; Section 15; Section 17 2) Section 20; Section 5(1)(6,7); Section 6; Section 14; Section 15; Section 17 3) Section 20; Section 5(1)(6,7); Section 6; Section 14; Section 15; Section 17 4) Section 20	1) Annex III (1) 2) Annex III (17) 3) Article 9 (2); Annex III (18, 19, 21) 4) Annex IV (16); Annex III (18, 21)

Additional information

General

Registering or marking into a diary means the use of methods to register the life cycle of the material, including the delivery and disposal. In case of information system the registering may be accomplished using the processes in the system itself. On protection level IV the registration based on security requirements is not mandatory, unless sensitive personal or biometrical information belonging to protection level IV and registered in a personal data file are included.

In order to register the life cycle of the material means typically e.g. that assurance of tracing the incidents can be found. When handling classified information in an information system especially user identification and authentication should be taken into account (see I 07) as well as a reliable implementation of accountability (logging, see I 10).

Other sources of information

BSI IT-Grundschutz-Catalogues - 13th version - 2013; SANS Critical Security Controls (v5) / 14; SANS Critical Security Controls (v5) / 16; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0

I 19	Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Security throughout the information processing environment lifecycle – Disposal of data material containing classified information	*Protection level IV* 1) Classified documents shall be destroyed by methods which meet relevant standards or which have been approved by competent authorities in accordance with national technical standards so as to prevent reconstruction in whole or in part. 2) Classified material in electronic format shall be destroyed by methods which meet relevant standards or which have been approved by competent authorities in accordance with national technical standards so as to prevent reconstruction in whole or in part. 3) Temporary files which contain information, resulting from the normal use of an information system are destroyed regularly, unless they are destroyed automatically. *Protection level III* In addition to points 1-3 above 4) The registrar and the witness, where the presence of the latter is required shall sign a destruction certificate, which shall be filed in the registry. The registry shall keep destruction certificates for a period of at least five years. *Protection level II* In addition to points 1-4 above 5) Destruction shall be performed in the presence of a witness who shall be cleared to at least the classification level of the document being destroyed.	1) Section 6, Section 21 2) Section 6, Section 21 3) Section 6, Section 21 4) 5) Section 6, Section 21	1) Annex II (8); Annex III (46); Annex IV (8) 2) Annex IV (8, 37-38) 3) Annex IV (16) 4) Annex III (45) and Annex IV (8, 37-38) 5) Annex III (44) and Annex IV (8, 37-38)
	Additional information		
	Destruction using a shredder On protection level IV the material may be shredded following, for instance, requirements below: ■ remaining paper particles are not more than 30 mm2 (DIN 66399 / P5 or DIN 32757 / DIN 4), ■ remaining magnetic hard disk particles are not more than 320 mm2 (DIN 66399 / H-5), ■ remaining SSD-disk or USB-memory particles are not more than 10 mm2 (DIN 66399 / E-5), and ■ remaining optical media particles are not more than 10 mm2 (DIN 66399 / O-5). On protection level III the material may be shredded following, for instance, requirements below: ■ remaining paper particles are not more than 30 mm2 (DIN 66399 / P5 or DIN 32757 / DIN 4), ■ remaining magnetic hard disk particles are not more than 10 mm2 (DIN 66399 / H-6), ■ remaining SSD-disk or USB-memory particles are not more than 10 mm2 (DIN 66399 / E-5), and ■ remaining optical media particles are not more than 5 mm2 (DIN 66399 / O-6).		

I 19	On protection level II the material may be shredded following, for instance, requirements below: ■ remaining paper particles are not more than 10 mm2 (DIN 66399 / P6), ■ remaining magnetic hard disk particles are not more than 10 mm2 (DIN 66399 / H-6), ■ remaining SSD-disk or USB-memory particles are not more than 1 mm2 (DIN 66399 / E-6), and ■ remaining optical media particles are not more than 5 mm2 (DIN 66399 / O-6). When using particle sizes described above the remaining waste may be disposed in a similar manner as the normal office waste. This means e.g. that particles resulting from the destruction when using DIN 66399 / P5 shredders for level III material no more need to be disposed using the classified waste disposal procedure, e.g., including of outsourced metal boxes. *Destruction using combined methods* Destruction may be executed instead or in addition to shredding by using various other methods, which are secure enough to prevent the reassembly of destroyed information (burning shredded material or melting hard disks). The possibility to reassemble paper documents depends also from the amount of the shredded material (like one shredded paper sheet versus large quantities of shredded material). Encrypting the data in different parts of its life cycle also diminishes the risks. Destruction of electronic storage media has been covered more in detail in FICORA instructions (www.ncsa.fi > Asiakirjat > Ylikirjoitusohje; in Finnish only). *Details taken into account on the destruction of electronic media* Especially the reliable destruction of electronic material should cover all devices which have been used to store classified information at some part of their life cycle. One has to make it sure that the individual components of devices (hard drives, memory components, solid state disks etc.) containing classified information have to be destroyed in a reliable manner especially when the device will be delivered to service, becomes obsolete, or is taken into use as a part of a recycling process. In case a reliable deletion manner (like an overwriting procedure approved by competent authorities) cannot be used, the component containing classified information cannot be delivered for third party. In service situations where it is impossible to delete the memory content in a reliable way, the service should be carried out under supervision in order to ensure that classified information is not disclosed during the service. *To be taken into account on the destruction of temporary files* On the destruction of temporary files the overwriting procedure should be used for deleting temporary file folders of the operating system and of applications as well as the content of the trash bin. An overwriting procedure may be carried out for instance at start up or shut down of the system through the use of automated logon/logoff scripts. On servers or other systems which are not booted up on a daily basis it is recommendable to produce automated over writing scripts of temporary files, which will be run regularly, like once a day. More information about documenting the destruction procedure can be found at I 18. *Other sources of information* FICORA instruction on overwriting: Viestintäviraston ylikirjoitusohje (in Finnish only); Secure destruction of sensitive items - CPNI standard - 2014, BSI IT-Grundschutz-Catalogues - 13th version - 2013; ISO/IEC 27002:2013 8.3.2; ISO/IEC 27002:2013 11.2.4; ISO/IEC 27002:2013 11.2.7

Operations Security

I 20

Security throughout the information processing environment lifecycle

- Methods for change management

Requirement	Source (681/2010)	Source (2013/488/EU)
1) Ensuring security shall be a requirement throughout the entire CIS life-cycle from initiation to withdrawal from service. 2) Security assessments, inspections and reviews shall be performed periodically during the operation and maintenance of a CIS and when exceptional circumstances arise. 3) Security documentation for a CIS shall evolve over its life-cycle as an integral part of the process of change and configuration management.	1) Section 4; Section 5(1)(6); Section 6 2) Section 4; Section 5(1) (6); Section 6 3) Section 4, Section 5(1)(6); Section 6	1) Annex IV (8) 2) Annex IV (11, 16) 3) Annex IV (12

Additional information

Example

On protection levels IV and III the requirement may be fulfilled by using following procedures:

1) Modifications having effect on information processing should be handled through a modification management process. Modifications should be traceable.
2) Networks, systems and devices connected to them, programmes and settings have been documented in a way that modifications made to the approved setup can be confirmed by comparing the modifications to the documentation.
3) Information processing environments are kept under supervision in order to detect unauthorised changes and devices.

On protection levels II the requirement may be fulfilled by using following procedures in addition to points 1-3 above:

4) Systems are protected against connection of unauthorised devices (keyloggers etc.)

General

The documentation should consist at least of a network image, device and programme registers and of information about device and programme configurations.

In the protection of the system against the connection of unauthorised devices the following means may be used:

a) placing the devices on a security rack which is sealed and/or equipped with alarm
b) using devices which have been protected against tampering
c) using some other respective method (e.g. sealing of devices). When using the sealing method, inspection of the seals should be a regular process.

Inspection interval which can be accepted for verifying unauthorised modifications or devices depends on procedures implemented to limit and to supervise the access to the target of the inspection (a system, a physical area). In most of the environments a yearly or biannual inspection might do.

I 20

Other sources of information

SANS Critical Security Controls (v5) / 1 (); SANS Critical Security Controls (v5) / 2; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on Cyber-Security - The Critical Security Controls for Effective Cyber Defense Version 5.0; CPNI - Hardware Keyloggers; Finnish National Security Authority manual for handling International Classified Information (in Finnish only); ISO/IEC 27002:2013 8.1.1; ISO/IEC 27002:2013 12.1.1; ISO/IEC 27002:2013 12.1.2; ISO/IEC 27002:2013 12.5.1; ISO/IEC 27002:2013 14.2.2; ISO/IEC 27002:2013 14.2.8; ISO/IEC 27002:2013 14.2.9; ISO/IEC 27002:2013 18.2.3; VAHTI 2/2010 Annex 5 chapter 2.4

I 21

Handling of classified information within physically protected areas

- Physical security

Requirement	Source (681/2010)	Source (2013/488/EU)
Protection level IV 1) Physical security measures are carried out in all areas, offices, rooms and other such places where classified information is handled or stored, including the areas where information processing environments are located. 2) Handling of information is possible within security areas, in administrative areas or outside the administrative area in case methods approved by competent authorities are used. 3) Information may be stored within security areas and administrative area inside lockable office furniture or temporarily also outside the administrative area in case methods approved by competent authorities are used. *Protection levels III and II* n addition to point 1 above: 4) handling of classified information is possible within security areas approved by competent authorities. Handling of classified information is possible also in administrative area in case unauthorised personnel do not have access to classified information. 5) information can be stored within security areas approved by competent authorities in a safe or in a vault.	1) Section 5(1)7); Section 14; Section 15 2) Section 5(1)7); Section 14; Section 15 3) Section 5(1)7); Section 14; Section 15 4) Section 5(1)(7); Section 14; 15 § 5) Section 5(1)7); Section 14; Section 15	1) Article 8 (3) 2) Annex II (23); Article 8(3) 3) Annex II (24); Article 8 (3); Article 9 (4) 4) Annex II (25); Article 8 (4) 5) Annex II (22, 26); Article 8 (4)

Additional information

General

In situations where information belonging to protection levels III or II are temporarily handled inside the area that has been specified to one level less secure, additional measures - like TEMPEST - should be taken into account (see I 14) according to the protection level. Security procedures during lunch and coffee breaks and in other special circumstances should be planned; taking the classified material into safes in security areas, limiting the visibility to the area for instance by covering the windows and limiting the access only for accredited personnel. Requirements for administrative areas, security areas and e.g. for safes have been covered in detail in subdivision F of KATAKRI (see F 02 and F 03).

Other sources of information

BSI IT-Grundschutz-Catalogues - 13th version - 2013; CPNI - Security Advice - Physical Security; ISO/IEC 27002:2013 11.1.1; ISO/IEC 27002:2013 11.1.3; ISO/IEC 27002:2013 11.1.5; ISO/IEC 27002:2013 11.2.1

I 22	Requirement	Source (681/2010)	Source (2013/488/EU)
Handling and transfer of classified information between physically protected areas - Remote use and remote management	*Protection level IV* 1) Transferring and handling of classified information between physically protected areas is possible only by using compensative arrangements approved by competent authorities. 2) Personnel has been trained and instructed on secure remote use and management. 3) Unless the protection level IV classified information stored on electronic media (hard drives, USB-sticks etc.) has been encrypted using a method approved by competent authorities, storage media has to be stored securely enough to reach equal level of security as in a closed office furniture on level IV physically protected environment. If this is not possible, the storage media has to stay under constant supervision. 4) Remote use or management requires that the traffic will be encrypted by using a crypto product approved by competent authority to the respective protection level. *Protection levels III and II* in addition to points 1-2 and 4 above: 5) Unless the classified information stored on electronic media (hard drives, USB-sticks etc.) has been encrypted using a method approved by competent authorities, storage media has to stay constantly on possession of the authorised user in cases where it will be taken outside respective physically protected areas. Classified information may not be decrypted or read on public places. 6) Remote use or management of systems is limited to the physical areas approved by competent authorities.	1) Section 5(1)7,9); Section 14; Section 15; Section 16; Section 19 2) Section 5(1)(9) 3) Section 5(1)(6) 4) Section 5(1)6); Section 16; Section 19 5) Section 5(1)(6) 6) Section 5(1)(6); Section 14; Section 15.	1) Article 8(3); Article 9(4) 2) Annex IV (22) 3) Article 9(4); Annex III (28, 30,33 4) Article 10(6) 5) Article 9(4); Annex III (28, 30,33) 6) Annex II (25,26); Article 8(4).
	Additional information		
	General Remote use and management usually means that information processing systems are used of managed outside the office facilities of the organisation with a terminal dedicated for the use. In most of the cases the terminal used is a laptop computer, assigned to this use by the organisation. Remote use and management of classified information is basically possible only for protection level IV. From protection level III on the handling of classified information requires a physically protected environment approved by competent authorities for this particular use. In special cases this requirement may be compensated by the use of additional security measures (e.g. in the operative work carried out by authorities).		

I 22

Compensative arrangements on requirement 1 include on protection level IV the following:

a) only devices and remote connections approved by competent authorities for this particular environment are used
b) remote use or management requires a strong authentication based on at least two factors

On protection levels III and II an additional compensative control is required by the use of technically approved remote terminals (device authentication).

Protection of management connections is one of the most critical factors in the security of information processing systems (see I 04). However, especially systems belonging to protection level IV may be considered as subject to remote management. In cases where remote management is considered to be justified the security measures are recommended to be stricter than in pure remote use of the system. For instance, remote management connections may be limited to dedicated physical and logical locations.

Other sources of information

CPNI - Personnel Security in Remote Working; CPNI - Configuring & managing Remote Access for Industrial Control Systems; SANS Critical Security Controls (v5) / 13; SANS Critical Security Controls (v5) / 17; SANS Critical Security Controls (v5) / 10; SANS Critical Security Controls (v5) / 9; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; CPNI - Security Advice - Physical Security; ISO/IEC 27002:2013 6.2.1; ISO/IEC 27002:2013 6.2.2; ISO/IEC 27002:2013 7.2.2; ISO/IEC 27002:2013 8.3.1; ISO/IEC 27002:2013 8.3.3; ISO/IEC 27002:2013 11.1.1; ISO/IEC 27002:2013 11.1.3; ISO/IEC 27002:2013 11.1.5; ISO/IEC 27002:2013 11.2.1; ISO/IEC 27002:2013 11.2.3; ISO/IEC 27002:2013 11.2.5; ISO/IEC 27002:2013 11.2.6; ISO/IEC 27002:2013 12.1.1

I 23	Requirement	Source (681/2010)	Source (2013/488/EU)
Security throughout the information processing environment lifecycle - Management of software vulnerabilities	Reliable arrangements are established for the entire lifecycle of the information processing environment to manage programme vulnerabilities.	Section 5(1)(6); Section 6	Annex IV (8, 11,16)

Additional information

Example

On protection level IV this requirement may be reached by using following procedures:

1) Bulletins of authorities or device and programme manufacturers (etc.) are followed in order to estimate the need of security updates. Updates are installed in a controlled manner.
2) The network and its services, servers and workstations connected to the network, as well as laptops and other devices are inspected (vulnerability scan, CMDB etc.) at least annually and after every significant change or modification in order to detect such objects in the update process which need to be fixed. In addition to this, results of centralised update service installation processes are assessed regularly (e.g. on monthly basis).

On protection levels III and II this requirement may be reached by using following procedure in addition to point 1 above:

3) The network and its services, servers and workstations connected to the network, as well as laptops and other devices are inspected (vulnerability scan, CMDB etc.) at least biannually and after every significant change or modification in order to detect such objects in the update process which need to be fixed. In addition to this, results of centralised update service installation processes are assessed regularly (e.g. on monthly basis).

General

Management of vulnerabilities in programmes may be taken care of (e.g.) by the following:

1) information updates from CERT-community and from manufacturers are subscribed as e-mail. From these updates such information is picked up, which has impact to the security of the systems of the organisation. The integrity of programme downloads and updates (checksums, malware detection) are tested before bringing them to the production environment. Also the effects of updates should be tested before installing them to the production environment. Testing can be done in an isolated test environment or by a small user group.
2) The network and its services, servers and workstations connected to the network, as well as laptops and other devices are inspected (vulnerability scan, CMDB etc.) regularly and after every significant change or modification in order to detect such objects in the update process which need to be fixed. In addition to this, results of centralised update service installation processes are assessed regularly (e.g. on monthly basis).

Into ”significant changes” can be counted e.g. changes in network topology, new systems to be taken into use and / or service pack level updates to old systems, changes on filtering rules of firewalls etc.

Other sources of information: SANS Critical Security Controls (v5) / 4; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; CPNI - Good Practice Guide - Patch Management; ISO/IEC 27002:2013 12.6.1; VAHTI 2/2010 Annex 5 chapter 2.4

I 24

Security throughout the information processing environment lifecycle

- Backup copies

Requirement	Source (681/2010)	Source (2013/488/EU)
Backup copies containing classified information are kept under protection throughout their lifecycle using protection measures of at least equal level as what is used for safeguarding the original information.	Section 5(1)(6); Section 6; Section 20	Annex III (18,27); Annex IV (8,16)

Additional information

Example

On protection level IV this requirement may be reached by using following procedures:

1) Backup copies are handled and stored throughout their lifecycle on systems which fulfil at least requirements set for the protection level
2) When handling in the same backup system information belonging to different owners, who reserve the inspection rights (see I 06) to the handling of their particular information, separating methods making this possible in backup system interfaces and storage media have to be implemented following the requirements set for the protection level.
3) In case there is a need to transfer backup copies outside the physically protected area of the particular protection level, procedures described in I 15 (electronic transfer) and/or in I 16 and I 22 (transfer outside physically protected environment) are taken into account.
4) Backup media are destroyed according to the requirements set for the particular protection level (I 19).

On protection levels III and II this requirement may be fulfilled by using following procedure in addition to points 1-4 above:

5) Registers of backup copies are maintained and the handling of backups is documented on electronic log, on information system, on document management system, or on manual diary or document (see I 18).

General

Backup copying shall always be done according to the operational requirements. Backup copying that is considered adequate for the operational requirements takes into account at least the following:

1) Frequency for making backups is sufficient considering the criticality of the back upped information. This requires that a survey is done of how much of the data can be lost (recovery point objective, RPO).
2) The speed of the recovery process is sufficient for the operational requirements. This requires that a survey is done of how long the recovery may take (recovery time objective, RTO).
3) Correct functioning of the backup and recovery process is tested regularly.
4) The documentation of the recovery process is on an adequate level.
5) The physical location where backups are stored is separated from the actual system (in a separate sag/fire space, sufficient distance between backups and the system room, etc.). Note: backup copies should be protected with physical and logical access control methods following at least the requirements set for the respective protection level (taking into account the possible aggregate effect).
6) When handling in the same backup system information belonging to different owners, separating methods (see I 06) making inspection rights possible have to be implemented in backup system interfaces and storage media (e.g. dedicated and encrypted backup tapes which are stored in separate safes or closets).

Other sources of information: SANS Critical Security Controls (v5) / 8; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; ISO/IEC 27002:2013 12.3.1; VAHTI 2/2010 Annex 5 chapter 2.10

ANNEX I: Facility Security Clearance Procedure

Using KATAKRI in the Facility Security Clearance Procedure

Finnish national procedure for Facility Security Clearances has been set at the Act on Security Clearances (726/2014). Using the Facility Security Clearance (FSC) procedure the competent authority is able to assess, the capability of the company for taking care of given security responsibilities. This is achieved through the use of information sources listed in the Act as well as through vetting of personnel as well as trough audits of the security management and the premises of the company. Security arrangements which are audited are among others the safeguarding procedure of Classified Information, physical access control mechanisms and the security training of the personnel. Katakri can be used as a tool on the above mentioned assessment process.

The assessment process for the Facility Security Clearance can be seen in figure 1. This process scheme describes the tasks of the assessing security authority and the ones of the company at different stages of the assessment process. The process includes an audit to company's information systems in cases where this particular audit is part of the Facility Security Clearance process.

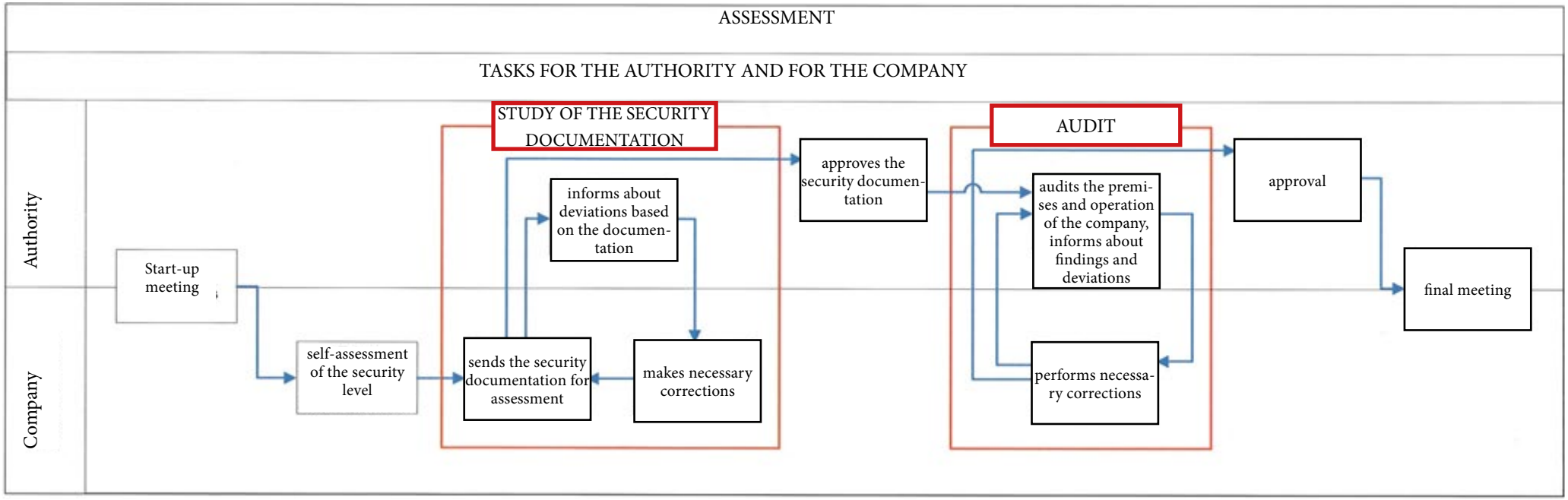

Figure 1 FSC assessment process.

It is possible to carry out the Facility Security Clearance procedure partially. In case there is no indication on the FSC application that the company should be capable to safeguard classified information which belongs to authorities in the premises of the company (”FSC without safeguards”), only Security Management subdivision of the criteria may be used. In case there is an indication on the FSC application that the company should be able to safeguard classified information belonging to authorities in the premises of the company (”FSC with safeguards”), assessment may be done using – in addition to the Security Management subdivision – the subdivision Physical Security and those parts of the Information Assurance subdivision, where requirements for handling paper documents are given. Assessment of the information system as a part of the FSC procedure has been described more in detail on Annex II.

Preparations for the audit

Before the actual process with authorities is ready to begin, the company has to conclude the security level and residual risks of the information handling environment to the level which can be accepted through the company risk management. Company then delivers risk management results for the authority together with a description of the conformity of security arrangements. There is no official model or form to report of the results or the conformity.

Risk management of the company

Risk management serves as a basis for the correct scaling of the security measures. The competent authority then sets the requirements in relation to the threat environment and those security controls which the company presents. The understanding of threats may, however, vary between the authority and the company.

Risk management process aiming at safeguarding information can be described on a simplified way with four phases:
1) identification of risks,
2) analysing risks to define the impact and probabilities,
3) assessment of risks in order to choose appropriate security measures
4) preparation for actualising risks through a follow up of the risk management process.

Coverage of the risk management and other requirements set for it are touched more in detail in subdivision T (especially T 04).
Company has to be able to present the rationale for chosen security measures and for their adequacy through the risk management process. It is recommended that the company discusses with the authority about their risk definitions and about security operating procedures at an early stage in order to have mutual understanding already at the security planning phase.

Description of the conformity of company´s security arrangements

The goal for the description of the conformity of company´s security arrangements is to have a compiled presentation of those security arrangements which the company thinks are essential when fulfilling the security requirements. The description is used especially on the planning and execution of the audit performed by the competent authority. On the table 1 (below) an example of the conformity of security arrangements is presented.

Table 1. Example of the description of the conformity of security arrangements.

T 11 Personnel security - Security awareness and training	1) Security instructions cover the processes and handling environments that are related to classified information during the entire life span of the information 2) Personnel receive instructions for and training in the correct handling of classified information 3) The training in the handling of classified information takes place on a regular basis and the participants are documented 4) It is controlled that security instructions are followed and needs to change the instructions are estimated regularly.	New employees are given the basic security training and instructions right after their employment. The entire personnel will have updated security training sessions annually. It is mandatory for the whole personnel to take part to the security training. Results of the training are followed through a test on the intranet. Passing the test is a prerequisite for issuing and maintaining personal access rights. Risk manager is responsible for the general security training. Task based training for safeguarding information is given to that part of the personnel who has the need to handle classified information. This task based training has been tailored for different task groups. It is mandatory to pass the training before the access rights to the classified information environment can be issued. Training register is used to record the attendance. Training is repeated annually and the training package has to be passed on Q1. Risk manager is responsible for the task based security training together with the security responsible named for each task based function. Maintenance of security instructions is on a responsibility of the risk manager. What comes to task based instructions, the risk manager is supported by the security responsible named for each of the task based functions.

Assessment of the authorities on the adequacy of security arrangements

In the assessment produced by competent authorities the protection level and the amount of the information is taken into account, as well as the form and the rationale for classifying. These details are put against the possible threat of hostile or criminal actions. When considering security measures it is important to note that the requirements described on different subdivisions of KATAKRI that the given examples may be replaced with compensating controls giving the same protection against the threat. For instance the implementation of strong user authentication is possible either through means of information technology or physical security. On the other hand it is usually impossible to find compensating controls for encryption in situations where the traffic will be routed outside a physically protected area.

In situations where the threat on which the requirement is based on is considered to be highly unlikely, the authority may decide that the requirement is not valid. For example in workstations of which all network interfaces have been physically reliably removed are normally not a subject of requirements set for firewalls or for the maintenance of their filtering rules. Authorities use given examples to assess whether the Katakri requirement is fulfilled or not, based on their risk analysis and of risk management measures taken to prevent risks and to diminish the possible consequences. Authorities normally use the method of administrative and technical inspections. Audit methods used for assessing the security arrangements of information systems have been described more in detail on Finnish Communications Regulatory Authority's instruction for Evaluation Agencies on Information Security[1].

1 Finnish Communications Regulatory Authority's instruction for Evaluation Agencies on Information Security. URL: https://www.viestintavirasto.fi/attachments/Ohje_tietoturvallisuuden_arviointilaitoksille.pdf.

ANNEX II Evaluation of information systems

According to the Act on the Evaluation of Government Information Systems and Data Transfer Arrangements (Act 1406/2011) it is possible to give the evaluation task to the Finnish Communications Regulatory Authority or to one of the Accreditation Agencies accredited by the Finnish Communications Regulatory Authority[2]. Katakri can be used as a tool when assessing how the information system used or planned for the use of the government fulfils the national or international security requirements. Also when used to assess the government information systems Katakri has to be used following the findings of organised risk assessment, resulting in the selection of safeguarding requirements chosen for the particular use and in the evaluation of their realisation based on given examples.

This Annex describes different use cases of KATAKRI when inspecting information systems. The description concentrates on cases where the topic is either a FSC inspection or an information system used (or to be used) by the government. In these cases the relevant competent authority is the Finnish Communications Regulatory Authority. This description has been divided into presentations of use cases, evaluation and accreditation processes and of the accreditation and clearance issuance. The description leaves out other user cases like the use of audits as a part of the internal security work of the organisation.

Use cases

KATAKRI use cases on information system inspections performed by the NCSA function of the Finnish Communications Regulatory Authority can be divided in five categories:

1. Systems which are in possession of the government or are intended to be purchased, and of which the governmental authority has issued an evaluation request for the Finnish Communications Regulatory Authority (Act 1406/2011).
    - system evaluation is based on the interest specified on the request; national interest, international interest or both, concerning the safeguarding of classified information.
2. Requests of the Ministry of Finance concentrating on general information security level of information systems or data transfer systems owned by government authorities (Act 1406/2011).
    - system evaluation is based on the interest specified by the Ministry of Finance on the request; national interest, international interest or both, concerning the safeguarding of classified information.
3. Systems owned by governmental authorities as long as they are part of fulfilling the international information security requirements (Act 588/2004[3]).
    - system evaluation is based on the interest concerning the safeguarding of international Classified Information .
4. Systems owned by companies when systems are part of the evaluation package, based on the request for a Facility Security Clearance, as long as the accreditation given by the competent NCSA authority is needed (Act 588/2004 and/or 726/2014[4]).
    - system evaluation is based on the interest concerning the safeguarding of international Classified Information .
5. Systems owned by companies when systems are part of the evaluation package, as long as the accreditation given by the competent NCSA authority is needed (Act 726/2014[5]).
    - system evaluation is based on the interest concerning the safeguarding of national Classified Information .

Use cases of information system inspections can be combined according to the wishes expressed by the organisation ordering the evaluation.

2 Act on Information Security Evaluation Agencies (L 1405/2011), https://www.finlex.fi/fi/laki/ajantasa/2011/20111405 (in Finnish).
3 Act on international information security obligations (588/2004), https://www.finlex.fi/fi/laki/alkup/2004/20040588 (in Finnish).
4 Act on Security Clearances (726/2014), https://www.finlex.fi/fi/laki/alkup/2014/20140726.
5 Act on Security Clearances (726/2014), https://www.finlex.fi/fi/laki/alkup/2014/20140726.

Evaluation process

Evaluation process for the security of information systems begins when the target of the evaluation sends an evaluation request to the Finnish Communications Regulatory Authority (competent authority). Other phases in the evaluation process are the planning of the evaluation, the inspections and the reporting. An evaluation process has been visualised in figure 1. An evaluation process may be used, e.g., as a part of the internal security work of the target organisation, perhaps in a manner where for instance residual risks are left completely on the responsibility of the target organisation. An evaluation process has been described more in detail in the Finnish Communications Regulatory Authority instruction "Information Security Inspections of NCSA – View of the Ordering Organisation" (in Finnish only) .

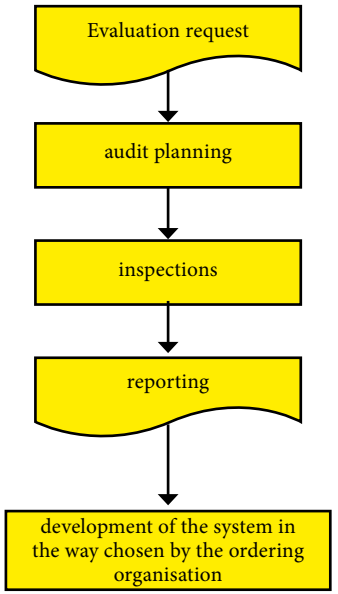

Figure 1. Simplified evaluation process.

Accreditation process

Accreditation process aiming at the accreditation of the Finnish Communications Regulatory Authority begins, when the target organisation of the evaluation sends a accreditation or certification request to the Finnish Communications Regulatory Authority. The accreditation process is similar to the evaluation process with the exception that the deviated findings of the inspection have to be corrected and verified before the accreditation or the certification can be issued. Accreditation process has been visualised in a simplified form in figure 2. Accreditation process may be used, e.g., when the target organisation wishes to proof the conformity of the protection of the information system by the accreditation or certificate issued by the Finnish Communications Regulatory Authority. In the accreditation process the risk assessment will be done using the assessments made by both the organisation itself, as well as the one of the competent authority (Finnish Communications Regulatory Authority). The accreditation process is described more in detail in the Finnish Communications Regulatory Authority instruction "Information Security Inspections of NCSA – View of the Ordering Organisation" (in Finnish only).

Accreditation and the certificate

The Finnish Communications Regulatory Authority may issue an accreditation for the system which handles international classified information and fulfils the requirements. For the system handling national classified information the Finnish Communications Regulatory Authority may issue a certificate of conformity. Prerequisite for issuing the accreditation or the certificate is the commitment of the target organisation to maintain the approved security level.

The validity of both the accreditation and the certificate will expire in case a significant change affecting the security of the inspected target will occur. Such changes could be for instance significant changes in the network architecture, personnel, security measures or premises. Changes resulting from normal maintenance procedures, such as security updates for programmes, will not cause revoking of the accreditation or the certificate. Conditions for revoking the accreditation or the certificate will be defined at their issuance. Approvals for major changes should be requested in advance from the competent authority (Finnish Communications Regulatory Authority).

The Finnish Communications Regulatory Authority is able to issue a certificate for the system which has been audited by an approved Evaluation Agency (Act 1405/2011). Prerequisite for the issuance is that the target for the audit has been confined to match with the definitions of the request for the certificate or for the accreditation, as well as the adequacy of the audit reports for the particular use. The Finnish Communications Regulatory Authority may carry out additional inspections or may ask for further information from the ordering organisation in order to ensure that the target fulfils the applicable information security requirements.

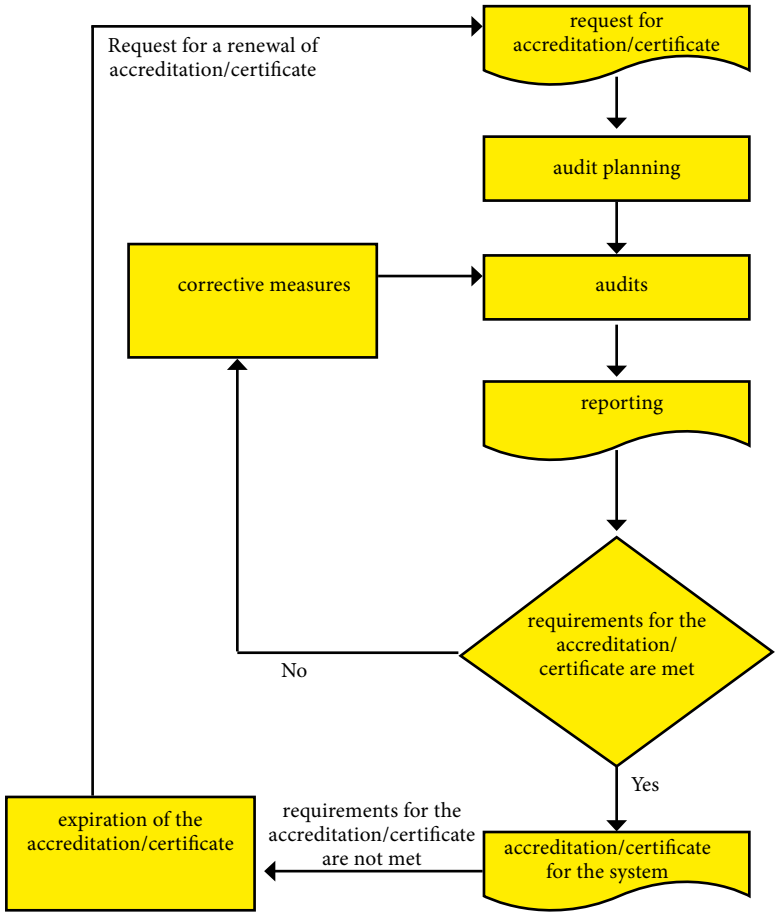

Figure 2. Simplified accreditation process.