FINNISH NATIONAL SECURITY AUTHORITY

National Security Auditing Criteria

(KATAKRI) version II, 2011

Confederation of Finnish Industries

Finnish Communications Regulatory Authority

MINISTRY FOR FOREIGN AFFAIRS OF FINLAND

MINISTRY OF THE INTERIOR

Puolustusministeriö
Försvarsministeriet
Ministry of Defence

This translation of the Finnish KATAKRI criteria has been slightly modified from the national version in order to keep it as simple as possible. Two notes for readers though:

- *Finnish legislation divides unclassified information, on the one hand, in what is required to be safeguarded and, on the other hand, in what needs to be classified. In the Criteria, however, only the term "classified" is used for both purposes in order to make things easier for international readers.*
- *The classification levels used in the Criteria are accordingly:*
  - *LEVEL IV (RESTRICTED)*
  - *LEVEL III (CONFIDENTIAL)*
  - *LEVEL II (SECRET)*

Puolustusministeriö
Försvarsministeriet
Ministry of Defence

PL 31, 00131 HELSINKI

www.defmin.fi

Translation: Katri Suvanto / Ministry of Defence
Layout: Tiina Takala/ Ministry of Defence

ISBN: 978-951-25-2247-7 print
ISBN: 978-951-25-2248-4 pdf

Contents

PREFACE

The first important goal of the national security auditing criteria is to harmonise official measures: when an authority conducts an audit in a company or an organisation to verify their security level. The authorities may complement the audit, when necessary, with a security assessment and, in some cases, with consulting. These measures do not belong, however, to the actual auditing. In this 2011 version of the security auditing criteria the focus is solely on security.

The second important goal is to support companies and other organisations as well as authorities with their service providers and subcontractors to work on their own internal security. This is why the criteria contain recommendations that are separate and outside of the official requirements; it is hoped that useful security practices will be chosen and applied, thus progressing to the level of official requirements.

The security auditing criteria fall into four main areas: administrative security (security management); personnel security; physical security; and information security. When an audit is conducted, the requirements of all the four areas shall be taken into account; they were not built to be independent elements. Each consists of a tripartite classification of requirements, corresponding to the security level concepts that are currently being widely introduced: the base level, the increased level and the high level. These are complemented by the above-mentioned recommendations for the industry. The criteria have been created from the perspective of absolute requirements and they do not include a marking system which is used in some criteria. The aim here is to make sure that at the end of an audit there would not be possibly unidentified but critical risks. The chosen approach means specific demands for the personnel conducting security audits and, as a result, high enough training level requirements are set to satisfy these demands.

The state administration already uses and is preparing a number of requirements which are related to securing the functions vital to society. For their part they complement the security auditing criteria which are now introduced. The work on the criteria has aimed at taking these views into account. The guidelines for comprehensive information security and preparedness which have been prepared in particular under the leadership of the Ministry of Finance constitute an important parallel material. In addition, this 2011 version of the security auditing criteria has taken into account, as far as possible, the definitions of policy in the Government Decree on Information Security in Central Government and in the new security regulation of the European Union which were prepared at the same time. The criteria contribute both to international information security obligations and to the procedures contained in the acts regulating security reports.

The steering group

Foreword for the first version of the Criteria

Puolustusministeriö
Försvarsministeriet
Ministry of Defence

1325/50.01.00/2009
FI.PLM.20009-4910
20.11.2009

Ministry of the Interior

INTERNAL SECURITY PROGRAMME II, Measure 6.4 (2), NATIONAL SECURITY AUDITING CRITERIA

The Government adopted a Resolution concerning the Internal Security Programme (STO II) on 8 May 2008. The Ministry of Defence was designated as the responsible ministry for the second measure under paragraph 6.4 of the Programme which aimed at creating national security auditing criteria. A steering group was set up on 12 September 2008 and the start-up seminar was held on 5 December 2008. The work was set to be finished by the end of 2009; the work is ready to be submitted on the given date.

The aim of the measure was to create a set of national security auditing criteria for the authorities and the business community to harmonise common security procedures and independent monitoring and to improve auditing. To cover the areas of responsibility of the measure, the steering group decided to set up four working groups and, in addition, a separate follow-up group to receive feedback at the different phases of the work.

The defence administration, with the Defence Forces in the forefront, has for a long time taken care of the official obligations of the security authority which have been necessary to address because of international agreements and other practices to safeguard the security level of companies. For its part, the administration of internal affairs took on the responsibility for these obligations in 2009. There was a notable contribution by the Finnish authorities, organisations and the business community to prepare the national security auditing criteria: more than a hundred people participated. Amidst at times heated debates, the significant work resulted in a set of criteria where national and international commitments have been taken into account. The completed set of criteria is not all-inclusive; this means that the work needs to be continued. This is noted also in the recommendations of the steering group.

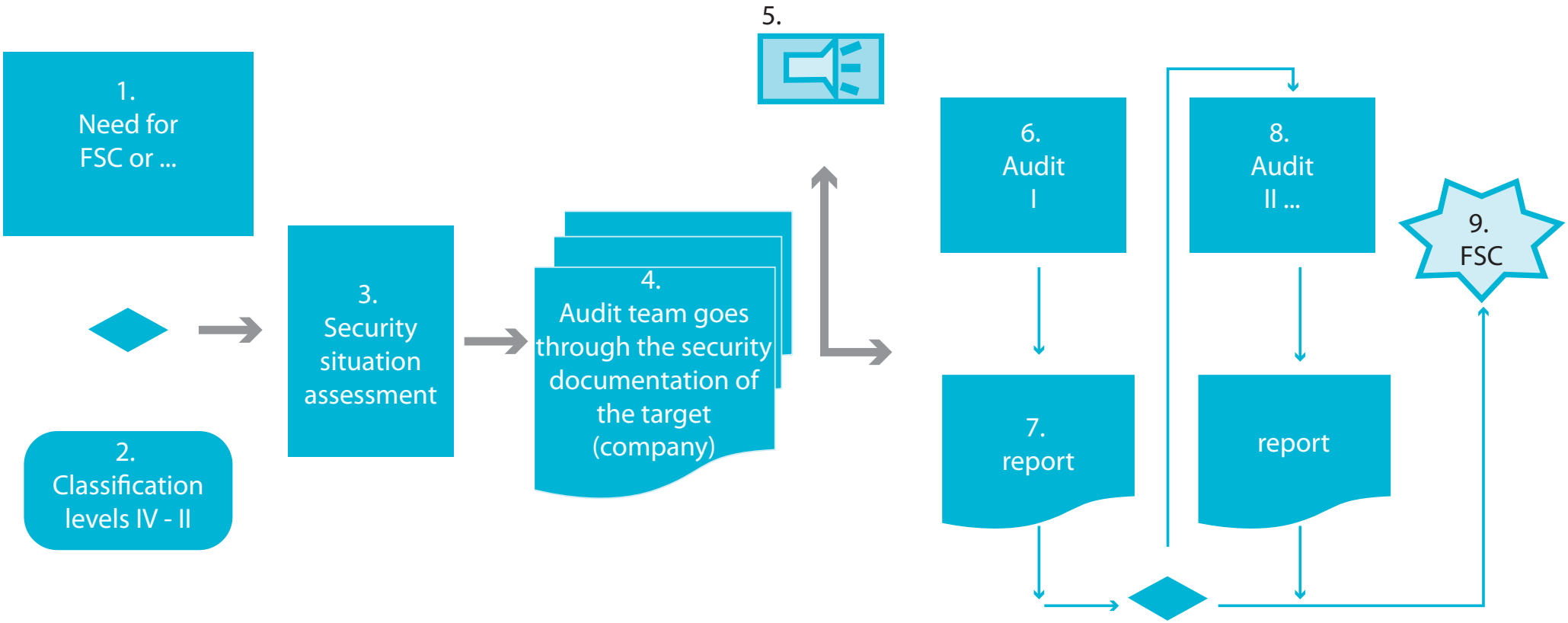
I hereby present the national security auditing criteria to the Ministry of the Interior to be introduced as the basis of security auditing that the authorities conduct in the companies.

Permanent Secretary Kari Rimpi

Security audit as a technical procedure (example)

FUNCTION

1. Recognition of the need for an audit
2. Definition of the classification level (CONFIDENTIAL/SECRET)
3. Building up a general image of the target to be audited
4. Security Assessment based on the security documentation of the target
5. Comments of fatal deficiencies/findings (optional, not part of actual auditing)
6. First audit
7. Audit report
8. Further audits and reports
9. Approval (Facility Security Clearance)



A Administrative Security

Contents

Introduction

For this subdivision of the criteria, administrative security work has been looked at as security management. The security management system and the minimum level required for auditing its subdivisions in protective levels II (high level), III (increased level) and IV (base level) are dealt with as a whole. In the field of security management, the criteria also include recommendations for independent security work to be carried out by the business community.

The guidelines will be applied to the sub-contractor chain in such a way that the organisation can, on the basis of the assignment, allocate work to sub-contractors. The organisation will be responsible for auditing the same principles in the sub-contractor companies.

Security policy, the measures guiding security action and definitions, subdivision A100

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 101.0 **Has the organisation's management defined and approved the security policy? Has the policy been reviewed at regular intervals?** *What the question assesses: the maturity level of the organisation's security management*	The organisation has laid down the basic facts about security as a separate document or as part of general goals.	The organisation has laid down the security policy as approved by the top management or an equivalent definition that guides security action.	The organisation has a valid and published document carrying the name of 'security policy', for which training is arranged. It is a top-level security document, which is approved by the top management. Security policy is reviewed at least annually and the reviews are documented and approved by the top management. The security policy of the organisation guides the following entities: annual security programme; goals of security work; assessment and controls of risk identification; security organisation and responsibilities; accidents, danger situations, security incidents and preventive measures; security documentation and its management; security training and increasing awareness; reviews of knowhow, reporting and the management.	The organisation has laid down the basic facts about security as a separate document or as part of general goals.		

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 102.0 **What are the security components that security policy and/or security management cover in the organisation?** *What the question assesses: the comprehensiveness and systematic nature of security work*	The security documentation covers at least the following subdivisions: premises security, information assurance and personnel security.	The security documentation covers at least the following subdivisions: premises security, information assurance and personnel security and the clear organisation of security management as defined in the security policy.	The security documentation provides the basis for a broad and comprehensive approach. The concept of security, for example, covers the following: security management; security of production and operations; occupational safety, environmental safety; rescue work; management of emergency situations; information assurance; personnel security; premises security; security of foreign operations; and prevention of crime.	The security documentation covers at least the following subdivisions: premises security, information assurance and personnel security.		
A 103.0 **Does the organisation's security documentation reflect the scope of operations and products, the mode of operation and related security risks?** *What the question assesses: the level of the security policy*	The organisation has laid down the basic facts about security as a separate project document or as part of general goals.	The security documentation addresses the organisation in question and takes into account changes in its operations.	The organisation's security documentation consists of and covers all procedures that are part of the organisation's operations. Risk management is an integral part of the operations of the organisation.	The organisation has laid down the basic facts about security as a separate project document or as part of general goals.		

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 104.0 **Do all levels of the organisation function in line with the security policy?** *What the question assesses: introducing security policy matters to all levels of the organisation*	No requirements.	The organisation has a clear programme for monitoring activities that are based on the security policy. The results of the monitoring can be presented.	The organisation can prove, based on the results of internal and external audits, that it is committed to the requirements of security work and to implementing them on all levels.	The organisation can verify that the implementation of obligations is monitored as part of other control or as separate security auditing.		
A 105.0 **Does the security policy take into account the obligations of general legislation and of local security requirements?** *What the question assesses: knowledge of security legislation and supervision of the application of legislation*	The legislation on security work and legal requirements are known and taken into account in security guidelines.	The legislation on security work and legal requirements are known and taken into account in security guidelines. A person or a function has been designated in the job description of the organisation to observe the security legislation.	A person or a function is responsible for observing the security legislation that concerns the organisation. The application and observing of the security guidelines have also been defined in job descriptions.	The legislation on security work and legal requirements are known and taken into account in security guidelines.		

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 105.1 **The main question:** **Have the statutory requirements of activities been taken into account?** *Additional questions:* *How are the statutory requirements followed and how are they taken into account in activities? For example, are the handling processes of personal data on the level required by the Personal Data Act?*	1) Legislation and contract-based requirements of activities are identified and met. 2) The classification, distribution and handling of national classified documents are conducted in accordance with national handling rules, the requirements set by the material and/or a separate contract. 3) The classification, distribution and handling of international classified documents are conducted in accordance with national handling rules, the requirements set by the material and/or a separate contract.	1) Legislation and contract-based requirements of activities are identified and met. 2) The classification, distribution and handling of national classified documents are conducted in accordance with national handling rules, the requirements set by the material and/or a separate contract. 3) The classification, distribution and handling of international classified documents are conducted in accordance with national handling rules, the requirements set by the material and/or a separate contract.	1) Legislation and contract-based requirements of activities are identified and met. 2) The classification, distribution and handling of national classified documents are conducted in accordance with national handling rules, the requirements set by the material and/or a separate contract. 3) The classification, distribution and handling of international classified documents are conducted in accordance with national handling rules, the requirements set by the material and/or a separate contract.	1) Legislation and contract-based requirements of activities are identified and met. 2) The classification, distribution and handling of national classified documents are conducted in accordance with national handling rules, the requirements set by the material and/or a separate contract. 3) The classification, distribution and handling of international classified documents are conducted in accordance with national handling rules, the requirements set by the material and/or a separate contract.	ISO/IEC 27002 15.1, ”Handling instructions for international classified material” by the National Security Authority, VAHTI 8/2006, http://www.finlex.fi/fi/laki/ajantasa/1999/19990523, http://www.finlex.fi/fi/laki/alkup/2004/20040588, http://www.finlex.fi/fi/laki/alkup/2010/20100885, http://www.finlex.fi/fi/laki/ajantasa/1999/19990621, http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/pdf/ Tietoturvakartoitus_kysymyslista.pdf, http://www.tietosuoja.fi/tulostus/5940.htm, VAHTI 2/2010. In practice, ch.6 of the Personal Data Act (523/1999) and the requirements it sets for the purpose of handling personal data, personal registers and data protection during the entire life cycle of data in all of its forms concern all organisations. Cf. The handling rules of classified information pertaining to the requirements of data security.	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 106.0 **The main question: has all personnel been informed of the content of the security policy so that they have a clear idea of their security-related duties and responsibilities?** *Additional question: is the documentation on the security policy always accessible to all personnel?* *What the question assesses: introducing the content of the security policy on all levels of the organisation and basing the every-day work on the requirements of the policy.*	The entire personnel have been trained in the security policy or the security guidelines which can easily be gone through again, for example by means of the information system or a billboard.	The entire personnel have been trained in the security policy, and the training is well documented. It is repeated, for example, as part of other training. The policy is easy to go through for example by means of the information system or a billboard. Representatives of relevant stakeholders have been trained in the organisation's security policy.	The entire personnel have been trained in the security policy of the organisation as part of the introductory training. Knowledge of the policy has been ensured by repeating it as part of other training. It is easy to go through the policy training again e.g. by means of the information system or a billboard. The comprehensiveness of the security policy training has been documented as far as the participants and the content are concerned. Also representatives of relevant service providers and sub-contractors have trained in the security policy of the organisation.	The entire personnel have been trained in the security policy or the security guidelines which can easily be gone through again, for example by means of the information system or a billboard.		

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 107.0 **Does the security policy require that the entire personnel are committed to constantly improving the security situation?** *What the question assesses: the comprehensiveness of the content of the security policy*	No requirements.	The security policy underlines the importance of personal commitment.	The security policy describes the importance of the commitment of the management and the employees to the security policy, underlining that, apart from being an obligation for each individual it also guarantees that operations and work continue undisturbed. Security is acknowledged as the quality and competitive factor of the organisation.	The security policy and/ or the security guidelines underline the importance of personal commitment.		
A 108.0 **Have the central security goals been defined in the security policy?** *What the question assesses: the comprehensiveness of the security policy's content.*	The central goals have been described in the security policy or in the security guidelines.	The central goals have been described in the security policy.	The central security goals are described in the organisation's security policy; they deal with the elements that ensure the quality and competitive factors of the organisation.	The central goals have been described in the security policy or in the security guidelines.		

The annual security action programme, subdivision A200

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 201.0 **Has the organisation a written and documented action programme to manage security and to achieve the goals of security work?** *What the question assesses: the ability of the organisation to recognize the entity of security, own strengths in activities and the areas where improvements are needed.*	No requirements.	The organisation has an action programme which covers the areas to be developed in security management, personnel security, information assurance and premises security. The action programme is a separate document or a part of the action plan of the organisation.	The organisation has an action programme which covers all the subdivisions of security. It comprises measures, responsibilities, schedules and measurable results. Based on the same principle, the action programme also addresses the development of security management.	The organisation has an action programme which covers the areas to be developed in security management, personnel security, information assurance and premises security. The action programme is a separate document or a part of the action plan of the organisation.		
A 202.0 **Has the action programme specified procedures, responsibilities and schedules to achieve the goals?** *What the question assesses: how detailed is the programme?*	No requirements.	The organisation has an action programme for security in which the goals, responsibilities and schedules required for the development of at least security management, personnel security, information assurance and premises security are described. The action programme is a separate document or a part of the action plan of the organisation.	Based on the job descriptions of the organisation, the annual action programme for security includes a plan to constantly improve the administrative subdivisions of security. The goals, responsibilities and measurable goals are given in the annual plan.	The organisation has an action programme for security in which the goals, responsibilities and schedules required for the development of at least security management, personnel security, information assurance and premises security are described. The action programme is a separate document or a part of the action plan of the organisation.		

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 203.0 **Is the action programme regularly reviewed?** *What the question assesses: does the organisation take into account possibly changing situations and is the annual action programme updated, when necessary, to reflect the changes.*	No requirements.	The review of the programme is part of the continuous management procedure.	A regular process is established in the organisation (e.g. the meeting procedure of the steering group or of the security steering group) where the progress of the security action programme items are presented by a responsible actor and the possible need to develop the programme goals, responsibilities or the schedule are brought up.	The review of the programme is part of the continuous management procedure.		
A 204.0 **Does the organisation have a documented programme to manage information assurance and to reach the goals of security work?**	The organisation has an information assurance plan or a plan of action (equivalent) and the related instructions if necessary. It is required that 1) the plan includes descriptions of at least administrative, physical and ICT information assurance, 2) the plan takes into account the legislation that regulates activities (including information assurance), 3) the guidelines for the plan are adequate in relation to the organisation and the asset.	The organisation has an information assurance plan or a plan of action (equivalent) and the related instructions if necessary. It is required that 1) the plan includes descriptions of at least administrative, physical and ICT information assurance, 2) the plan takes into account the legislation that regulates activities (including information assurance), 3) the guidelines for the plan are adequate in relation to the organisation and the asset.	The organisation has an information assurance plan or a plan of action (equivalent) and the related instructions if necessary. It is required that 1) the plan includes descriptions of at least administrative, physical and ICT information assurance, 2) the plan takes into account the legislation that regulates activities (including information assurance), 3) the guidelines for the plan are adequate in relation to the organisation and the asset.	The organisation has an information assurance plan or a plan of action (equivalent) and the related instructions if necessary. It is required that 1) the plan includes descriptions of at least administrative, physical and ICT information assurance, 2) the plan takes into account the legislation that regulates activities (including information assurance), 3) the guidelines for the plan are adequate in relation to the organisation and the asset.	PCI DSS 12.2, COBIT 4.1 PO, COBIT 4.1 DS5, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/ guidelines/ guidelines_pdf.pdf	

Defining the goals of security, subdivision A300

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 301.0 **Do the organisation's business activities and the supporting security policy and security programme provide the basis for setting the goals of security work?** *What the question assesses: do the policy, programme and goal-setting form a whole?*	The goals of security work have been set in line with the policy, in a clear and measurable way.	The goals of security work have been set in line with the policy, in a clear and measurable way.	The areas covered by the security policy have been taken into account in the goals of the action programme in a comprehensive way.	The goals of security work have been set in line with the policy, in a clear and measurable way.		
A 302.0 **Has the organisation set security goals for the various hierarchical levels and/or the functions of the organisation?** *What the question assesses: the concrete goal-setting as well as understanding the significance of the various sub-goals for the various parts and hierarchical levels of the organisation.*	No requirements.	The organisation has clear and documented security goals which cover the subdivisions of security in line with the programme and, itemized, the elements and levels required in the organisation's operations.	The organisation has defined clearly measurable goals for the whole, parts and levels of the organisation according to the requirements of operations. The goals have been documented and they form a part of the management system of the organisation.	The organisation has clear and documented security goals which cover the subdivisions of security in line with the programme and, itemized, the elements and levels required in the organisation's operations.		

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 303.0 **Have the goals been set in such a way that achieving them can be measured?** *What the question assesses: the concrete and realistic goal-setting and incorporating qualitative measurements into the goals.*	The goals of security work have been set in a concrete and measurable way.	The goals of security work have been set in a concrete and measurable way.	The goals of security work have been set in such a way that measurable goals have been set for the various parts and hierarchical levels of the organisation. For example, measurability is described as the comprehensiveness of the provided training, reducing the number of security incidents or other equivalent clear goal.	The goals of security work have been set in a concrete and measurable way.		
A304.0 **Has a timeline been set for achieving the goals?** *What the question assesses: concrete and realistic goal-setting.*	A timeline has been set for achieving the goals.	A timeline has been set for achieving the goals.	A timeline has been set for achieving the goals.	A timeline has been set for achieving the goals.		

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 305.0 **Have the following factors been taken into account when goals have been set:** **a. identified risks** **b. requirements from the organisation's own operations and/or business activities** **c. technical requirements and possibilities** **d. economic requirements** **e. requirements from other interest groups (e.g. clients, authorities)** **f. requirements from the legislation and/or other guidelines as well as agreements** *What does the question assess: when the goals were set, were the above requirements, possibilities and limiting factors identified.*	No requirements.	The goals to be set include, where necessary, a description of the goals in relation to the identified risks, technical and economic requirements as well as possibilities, requirements from the organisation's own operations and/or business activities, other interest groups and/or the legislation and/or other guidelines taking into account the factors a), b), c), e) and f).	When setting the goals, the factors a), b), c), d), e) and f) were taken into account.	The goals to be set include, where necessary, a description of the goals in relation to the identified risks, technical and economic requirements as well as possibilities, requirements from the organisation's own operations and/or business activities, other interest groups and/or the legislation and/or other guidelines taking into account the factors a), b), c), d), e) and f).		

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 306.0 **Is the entire handling environment of the classified information protected in accordance with the information assurance principles of the organisation and the significance/classification of the information?** *Additional questions: do protections cover all the logically connected information networks and systems where the classified information is handled? Do protections also cover the information networks and systems where information is exported or imported over the air gap by means of memory stics, for example?*	All information handling environments of protection level IV have been protected at least in accordance with the requirements of authorities.	All information handling environments of protection level III have been protected at least in accordance with the requirements of authorities.	All information handling environments of protection level II have been protected at least in accordance with the requirements of authorities.	All information networks and systems where the classified information is handled are protected according to the information assurance principles of the organisation.	”Handling instructions for international classified data” by the National Security Authority, VAHTI 2/2010, VAHTI 3/2010. The main goal of the requirement is to ensure that the entire handling environment of the classified information will be adequately protected and that there is no unauthorised access to the information via an auxiliary system connected to the main system, for example. A secondary goal is to ensure that there is no unauthorised access to the information, for example via a temporary network, trial network or a network which is installed without authorisation. As far as classified data is concerned, the entire handling environment of such information must be protected and approved in accordance with the relevant protection level. The requirement covers, for example, all other networks/ systems that are connected to the network/system as well as all handling environments where information is imported or exported. Cf. I 401.0).	

Identifying, assessing and controlling risks, subdivision A400

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 401.0 **Does the organisation have methods to identify and assess security risks?** *What the question assesses: does the organisation prioritise its security work by assessing the risks?*	The organisation assesses the risks in relation to security as a whole and risk assessment is the basis of prioritising security work. The procedure is regular and the results are documented.	The organisation assesses the risks in relation to security as a whole and risk assessment is the basis of prioritising security work. The procedure is regular and the results are documented.	Risk assessment is a continuous process which includes risk identification, assessment of likelihood and effectiveness, necessary measures, responsibilities and timelines. The best experts in the organisation carry out risk assessments. Risk assessment is the basis of prioritising security work.	The organisation assesses the risks in relation to security as a whole and risk assessment is the basis of prioritising security work. The procedure is regular and the results are documented.		
A 401.1 **Main question:** **Have the assets (functions, information, systems) been identified?** *Additional questions:* *What kinds of threats are made at them? Have the persons responsible for the assets been designated?* *(ex I 103.0)* *For additional information, see annex 1 (A401.1)*	1) The assets are identified. 2) The threats to the assets are identified. 3) A person responsible for/the owner of the assets is designated. 4) The protection methods for the assets are proportioned to the assets and the relevant risks (cf. A 401.2).	1) The assets are identified. 2) The threats to the assets are identified. 3) A person responsible for/the owner of the assets is designated. 4) The protection methods for the assets are proportioned to the assets and the relevant risks (cf. A 401.2).	1) The assets are identified. 2) The threats to the assets are identified. 3) A person responsible for/the owner of the assets is designated. 4) The protection methods for the assets are proportioned to the assets and the relevant risks (cf. A 401.2).	1) The assets are identified. 2) The threats to the assets are identified. 3) A person responsible for/the owner of the assets is designated. 4) The protection methods for the assets are proportioned to the assets and the relevant risks (cf. A 401.2).	ISO/IEC 27002 7.1, COBIT 4.1 PO9, VAHTI 8/2006, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines_pdf.pdf	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 401.2 **How are the risks to the assets assessed?** *(ex I104.0)* *For additional information, see annex 1 (A 401.2)*	1) The risks to the assets are systematically assessed. 2) Assessment is carried out at least annually and in connection with significant changes. 3) The chosen protection methods are appropriately proportioned to the assets and to the risks. 4) The management of security risks is an integral part of the definition, development, use and maintenance of the communications and information systems of the asset. 5) The management has approved the chosen protection methods and residual risks.	1) The risks to the assets are systematically assessed. 2) Assessment is carried out at least annually and in connection with significant changes. 3) The chosen protection methods are appropriately proportioned to the assets and to the risks. 4) The management of security risks is an integral part of the definition, development, use and maintenance of the communications and information systems of the asset. 5) The management has approved the chosen protection methods and residual risks..	1) The risks to the assets are systematically assessed. 2) Assessment is carried out at least annually and in connection with significant changes. 3) The chosen protection methods are appropriately proportioned to the assets and to the risks. 4) The management of security risks is an integral part of the definition, development, use and maintenance of the communications and information systems of the asset. 5) The management has approved the chosen protection methods and residual risks.	1) The risks to the assets are systematically assessed. 2) Assessment is carried out at least annually and in connection with significant changes. 3) The chosen protection methods are appropriately proportioned to the assets and to the risks. 4) The management of security risks is an integral part of the definition, development, use and maintenance of the communications and information systems of the asset. 5) The management has approved the chosen protection methods and residual risks.	ISO/IEC 27001 luku 4, ISO/IEC 27002 7.1, COBIT 4.1 PO9, "Handling instructions for international classified material" by the National Security Authority, VAHTI 8/2006, VAHTI 2/2010:n annex 5 (TTT), the EU code of security 6952/2/11 REV2 /1.4.20115. artikla, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/ guidelines/guidelines_pdf.pdf	
A 402.0 **Do these methods cover normal operations, special situations, accidents and emergencies?** *Are the subcontractors and service providers taken into account?* *What the question assesses: the comprehensiveness of risk assessment.*	Risk assessment covers at least security management and personnel security, information security and premises security. These have been assessed as far as relevant subcontractors and service providers are concerned.	Risk assessment covers at least security management and personnel security, information security and premises security. These have also been assessed as far as exceptional situations and relevant subcontractors and service providers are concerned.	Risk assessment covers at least security management and personnel security, information security and premises security. These have also been assessed as far as exceptional situations and relevant subcontractors and service providers are concerned.	Risk assessment covers at least security management and personnel security, information security and premises security. These have been assessed as far as relevant subcontractors and service providers are concerned.		

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 403.0 **Are the results of risk assessments documented and updated on a regular basis?** *What the question assesses: does the organisation have a verifiable system of recorded risk assessments*	No requirements.	Risk assessment is carried out at least annually and when the organisation's situation changes so that it is appropriate to update the assessment made. Risk assessments are recorded in such a way that they can be verified.	Security risk assessment is defined as part of the management process of the organisation and it is recorded as part of the documentation system of the organisation.	Risk assessment is carried out at least annually and when the organisation's situation changes so that it is appropriate to update the assessment made. Risk assessments are recorded in such a way that they can be verified.		
A 404.0 **Are the findings in risk assessment taken into account when the goals for security work are set?** *What the question assesses: is risk assessment part of high-quality security work, which aims at continuously improving the level of operations*	The results of risk management are taken into account in the goal-setting of security work.	The results of risk management are taken into account in the goal-setting of security work.	The risk assessment tool includes the measures required for managing risks as well as responsibilities and timelines. These are useful in the goal-setting of the organisation's security work. The risk assessment process is described.	The results of risk management are taken into account in the goal-setting of security work.		

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 405.0 **Is it possible to prioritise the risks on the basis of the results of risk assessment?** *What the question assesses: do the results provide the basis for choosing risk management measures, order of importance and urgency?*	The results of risk assessment are grouped by the order of importance.	The results of risk assessment are grouped by the order of importance.	Risk assessment is based on assessing the likelihood and effectiveness of the risk in such a way that the result is risk rating which can be used to define the need to remove a risk, improve risk management or diminish the effect	The results of risk assessment are grouped by the order of importance.		
A 406.0 **Does risk assessment provide the basis for security training requirements?** *What the question assesses: is risk assessment also a tool for supporting the planning of training as a means to diminish the effect of a risk*	The results of risk assessment influence the content of planned training. Training is seen as a means to influence risk management.	The results of risk assessment influence the content of planned training. Training is seen as a means to influence risk management.	The results of risk assessment influence the content of planned training. Training is seen as a means to influence risk management.	The results of risk assessment influence the content of planned training. Training is seen as a means to influence risk management.		

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 407.0 **Does the organisation have methods to control the implementation and effectiveness of the measures carried out on the basis of risk assessment?** *What the question assesses: do the measures chosen on the basis of risk assessment give the desired effect?*	No requirements.	The security management process includes the implementation of the measures carried out on the basis of risk assessment and assessment of effectiveness.	In the risk management cycle, the correct nature and scope of the measures planned on the basis of risk assessment and their effectiveness are processed.	The security management process includes the implementation of the measures carried out on the basis of risk assessment and assessment of effectiveness.		
A 408.0 **Main question: How is the information security of the organisation assessed?** *Additional question: Are operations developed on the basis of observations?* **(ex I 105.0)**	The information assurance level of the asset is continuously monitored, assessed and developed.	1) The information assurance level of the asset is systematically assessed and measured. 2) An independent review is conducted at planned intervals on the asset and always when significant changes take place in security implementation.	1) The information assurance level of the asset is systematically assessed and measured. 2) An independent review is conducted at planned intervals on the asset and always when significant changes take place in security implementation.	The operational mode of the organisation's information assurance and the practical implementation of information assurance are continuously monitored, assessed and developed.	ISO/IEC 27002 6.1.8, ISO/IEC 27004, VAHTI 8/2006, Fulfilling requirements can be verified for example by asking examples of how information assurance has been monitored, assessed and developed. In particular, fulfilling the requirements of protection level III can be verified by requesting a description of the used systematic method and the results it has given. On protection level III, a report produced by an external reviewer can be requested for inspection.	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 409.0 **How is information assurance observed in subcontracting, service contracting and other similar co-operation contracts?** *(ex I 106.0)*	1) Identified security requirements will be taken care of before clients are granted access to classified information or assets. 2) All data of protection level IV is submitted to the subcontractor (equivalent) with discretion in line with the need-to-know principle. The recipient of data is given instructions for how to handle data of the protection level in question. 3) The services handling sensitive information of the organisation are entitled to carry out checks on information assurance. 4) The risks relating to external actors such as outsourcing partners have been identified and relevant security mechanisms have been implemented. 5) Services have been defined with SLA. 6) Procedures have been agreed for information assurance incidents with service providers that process outsourced data.	The data of protection level III is not submitted to the subcontractor (equivalent) without prior permission from authorities.	The data of protection level II is not submitted to the subcontractor (equivalent) without prior permission from authorities.	1) Information assurance requirements are attached to invitation for tenders. 2) The risks relating to external actors such as outsourcing partners have been identified and relevant security mechanisms have been implemented. 3) Services have been defined with SLA. 4) Procedures have been agreed for information assurance incidents with service providers that process outsourced data.	ISO/IEC 27002 6.2.1, ISO/IEC 27002 6.2.2, ISO/IEC 27002 10.6.1, ISO/IEC 27002 12.1.1, COBIT 4.1 AI5, COBIT 4.1 DS1, COBIT 4.1 DS2, "Handling instructions for internationally classified data" by the National Security Authority, VAHTI 8/2006, the EU code of security 6952/2/11 REV2 /1.4.201111. article, the EU code of security 6952/2/11 REV2 /1.4.2011liite V Pledges of secrecy, non-disclosure or other secrecy clauses must also be observed (P 407.0). Subcontractors (equivalent) can be requested to submit reports, on a case by case basis, on the current level of information assurance, (for example, the observations, attacks, incidents, and so on, on a monthly basis). Part of international data must not be submitted to subcontractors (equivalent) without prior permission from authorities even on protection level IV. This must be ensured on a case by case basis.	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 410.0 **What action is taken in the organisation when information security incidents occur?** *Additional question:* *How is the management of security assurance incidents implemented in practice?* *(ex I 107.0)*	The management of information assurance incidents is 1) planned, 2) provided with instructions/training, 3) in view of the environment, documented to an adequate degree and in particular 4) communication procedures and responsibilities are agreed on.	1) The management of information assurance incidents is documented. 2) Occurred or suspected information assurance incidents are immediately reported to a security authority or to a formally recognised body.	1) The management of information assurance incidents is documented. 2) Occurred or suspected information assurance incidents are immediately reported to a security authority or to a formally recognised body.	The management of information assurance incidents is 1) planned, 2) provided with instructions/training, 3) in view of the environment, documented to an adequate degree and in particular 4) communication procedures and responsibilities are agreed on.	ISO/IEC 27002 13.2.1, PCI DSS 12.9, COBIT 4.1 DS8, the EU security code 6952/2/11 REV2 /1.4.2011 13. artikla, VAHTI 3/2010, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines_pdf.pdf - Cf. I 408.0. For some of the international data, a planned and documented incident handling model that is provided with guidelines is requested already on protection level IV. Who the incidents are reported to depends on the owner of the information. It can be, for example, NCSA-FI, CERT-FI, an element within the defence administration or a CERT actor within the European Union.	

Security organisation and responsibilities, subdivision A500

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 501.0 **Have the responsibilities of security work been defined? Do the definitions cover the various levels of the organisation?** *What the question assesses: have the responsibilities of security work been laid down so that all functions and levels of the organisation are covered*	The security organisation covers at least personnel security, information security and premises security. The responsible persons have been designated.	The security organisation covers security management and personnel security, information security and premises security. The responsible persons have been designated and trained and the task is part of the person's job description.	The responsibilities of security work have been defined for the subdivisions in security management and the security policy as well as for the functions and levels of the organisation. The responsible persons have been designated and trained and the task is part of the person's job description.	The security organisation covers at least personnel security, information security and premises security. The responsible persons have been designated.		

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 501.1 **Does the management support the organisation's information security? How does the support manifest in the activities of the organisation?**	The management supports the organisation's information security. The minimum requirements are the following: 1) Responsibilities are clearly set in information security (responsibilities of the management; responsibilities for maintaining the information management systems; responsibilities of the basic user, and so on) 2) The organisation has principles and practices for information security that are approved by the management 3) The entire organisation is made aware of the principles and practices for information security 4) The principles and practices of information security are reviewed always when significant changes happen. 5) It is required by the management that employees, suppliers and external handlers of information work in line with the information security principles of the organisation. 6) In view of operational requirements, necessary resources are available for information security.	The management supports the organisation's information security. The minimum requirements are the following: 1) Responsibilities are clearly set in information security (responsibilities of the management; responsibilities for maintaining the information management systems; responsibilities of the basic user, and so on) 2) The organisation has principles and practices for information security that are approved by the management 3) The entire organisation is made aware of the principles and practices for information security 4) The principles and practices of information security are reviewed always when significant changes happen. 5) It is required by the management that employees, suppliers and external handlers of information work in line with the information security principles of the organisation. 6) In view of operational requirements, necessary resources are available for information security.	The management supports the organisation's information security. The minimum requirements are the following: 1) Responsibilities are clearly set in information security (responsibilities of the management; responsibilities for maintaining the information management systems; responsibilities of the basic user, and so on) 2) The organisation has principles and practices for information security that are approved by the management 3) The entire organisation is made aware of the principles and practices for information security 4) The principles and practices of information security are reviewed always when significant changes happen. 5) It is required by the management that employees, suppliers and external handlers of information work in line with the information security principles of the organisation. 6) In view of operational requirements, necessary resources are available for information security.	The management supports the organisation's information security. The minimum requirements are the following: 1) Responsibilities are clearly set in information security (responsibilities of the management; responsibilities for maintaining the information management systems; responsibilities of the basic user, and so on) 2) The organisation has principles and practices for information security that are approved by the management 3) The entire organisation is made aware of the principles and practices for information security 4) The principles and practices of information security are reviewed always when significant changes happen. 5) It is required by the management that employees, suppliers and external handlers of information work in line with the information security principles of the organisation. 6) In view of operational requirements, necessary resources are available for information security.	ISO/IEC 27002 5.1.1, ISO/IEC 27002 5.1.2, ISO/IEC 27002 6.1.1, ISO/IEC 27002 6.1.3, ISO/IEC 27002 7.1, ISO/IEC 27002 8.2.1, PCI DSS 12.1, PCI DSS 12.3.1, PCI DSS 12.4, PCI DSS 12.5, COBIT 4.1 PO4, COBIT 4.1 PO6, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/ guidelines/ guidelines_pdf.pdf It is recommended that, in addition to the maintenance responsibility, also owners for the systems are specified. It is recommended that technical maintenance is not the same as the owner.	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 502.0 **Has information been given about the roles, responsibilities and implementation powers within the organisation and to those external parties who need to know the structure of the security organisation?** *What the question assesses: are the persons responsible for the various subdivisions of security and who can provide support in a problem situation known in the organisation?*	The personnel have been given training in the security organisation and updated information is available, for example, by means of the information system or a billboard.	The personnel have been given training in the security organisation and updated information is available, for example, by means of the information system or a billboard.	The entire organisation has been given training in the structure and responsibilities of the security organisation and the updated information is constantly available including the relevant service providers and subcontractors.	The personnel have been given training in the security organisation and updated information is available, for example, by means of the information system or a billboard.		
A 503.0 **Have enough resources been allocated to security work to carry out, control and improve the work? The resources should cover:** • **personnel** • **special competence** • **technical resources** • **economic resources** *What the question assesses: does security work have realistic chances of succeeding?*	No requirements.	Trained and experienced personnel are responsible for security work. Their competence level is maintained according to a plan on a regular basis. Security management covers, for example, the assessment of personnel resources, technical resources and adequate economic resources. These components have been incorporated into the continuous improvement of security work.	Trained and experienced personnel are responsible for security work. Their competence level is maintained according to a plan on a regular basis. The continuity of competence is secured by good personnel planning. High-quality security technology is used as part of security management with relevant integration.	Security management covers, for example, the assessment of personnel resources, technical resources and adequate economic resources.		

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 504.0 **Has the top management designated a person who is responsible for developing and managing security action and for ensuring that security work covers the needs of all the levels of the organisation?** *What the question assesses: is the person responsible for security supported by the management and does (s)he have appropriate powers? Is the scope of the task wide enough for the management of the whole? The task may be part of the person's job description.*	The organisation has designated a person responsible for security with sufficient powers to direct security action and to manage at least the subdivisions of personnel security, information security and premises security. The tasks may also be divided if that is appropriate for the functioning of the organisation.	The organisation has designated a key person responsible for security with sufficient powers to direct and co-ordinate security action and to manage at least the subdivisions of personnel security, information security and premises security.	The organisation has designated a person with the overall responsibility for developing and managing security as part of the organisation's management. The job covers the subdivisions of security and the parts and levels of the organisation.	The organisation has designated a person responsible for security with sufficient powers to direct security action and to manage at least the subdivisions of personnel security, information security and premises security. The tasks may also be divided if that is appropriate for the functioning of the organisation.		

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 505.0 **Does the designated person responsible for security work have powers to secure that the security management system is established according to the requirements of the goals?** *What the question assesses: can the person directing security work influence the management system in such a way that the security goals are achieved?*	The person responsible for security has such a position in the organisation that (s)he can influence how security is implemented. This has to be specified in the process description of the organisation and/or in his/her job description.	The person responsible for security has such a position in the organisation that (s)he can influence how security is implemented. This has to be specified in the process description of the organisation and/or in his/her job description.	The person responsible for security is on such a level in the organisation that (s)he can influence how security is implemented. This has to be specified in the process description of the organisation and/or in his/her job description.	The person responsible for security is on such a level in the organisation that (s)he can influence how security is implemented as part of the regular management of the organisation. This has to be specified in the process description of the organisation and/or in his/her job description.		
A 506.0 **Is the organisation's management committed to security goals and to achieving them as well as to the continuous improvement of security?** *What the question assesses: the commitment to security on every level of the organisation. The example set by the organisation's management is a crucial factor.*	No requirements.	The organisation's management is involved in the goal-setting of security work, choosing the methods and assessing the follow-up of the goals. The model has to be specified in the process description of the organisation.	The organisation's management shows its commitment concretely by observing security requirements and taking part in development work. The management takes up the goals, methods and achievements of security as part of the overall management.	The organisation's management is involved in the goal-setting of security work, choosing the methods and assessing the follow-up of the goals.		

Accidents, danger situations, security incidents and preventive measures, subdivision A600

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 601.0 **Does the organisation have a business continuity management in place?** *What the question assesses: has the organisation identified the disturbances that threaten operations and is it prepared for those that may slow down or prevent the organisation from achieving the main goals?*	No requirements.	In managing the organisation's activities, preparedness is in place for incidents disturbing or disrupting business operations and preparedness plans and business recovery plans have been made for the core functions of the organisation. The need for resources is specified and their availability is planned. The implementation of continuity management is monitored and assessed.	In managing the organisation's activities, preparedness measures are in place against incidents disturbing or disrupting business operations and appropriate preparedness plans and business recovery plans have been made. The resources have been specified and reserved, the methods are tested and relevant training has been done. The implementation of continuation management is monitored and assessed. Continuation management is introduced throughout the organisation and covers the processes of the organisation. The mode of operation has been documented. Interruption risks have been insured against as planned.	The organisation has identified the major threats against continuation and is prepared for them by protecting, verifying, duplexing and other methods. The organisation has taken a statutory insurance cover.		

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 602.0 **Has the organisation designated the people responsible for dealing with and investigating accidents, danger situations and security incidents?** *What the question assesses: has the organisation taken into account the possibility of security incidents and is the incident management specified and organised? Is co-operation with authorities planned?*	No requirements.	The organisation has defined that the management of exceptional situations is part of organising security. The responsibilities are given in the job descriptions. The responsible persons are well aware of the division of powers and responsibilities between the organisation and the authorities.	The people responsible for dealing with and investigating accidents, danger situations and security incidents are designated, taking into account the scope of operations and the parts and levels of the organisation. They are well aware of the division of powers and responsibilities between the organisation and the authorities.	The organisation has defined that the management of exceptional situations is part of organising security.		
A 603.0 **Are the responsibilities specified to diminish in advance the effects of crisis situations, accidents, danger situations and deviations from security?** *What the question assesses: has the organisation taken into account in advance the emergence of irregular situations and is diminishing risks specified and organise*	No requirements.	The organisation has defined that managing exceptional situations is part of organising security. Powers and responsibilities are given in the job descriptions.	The organisation has defined that managing exceptional situations is part of organising security. Powers and responsibilities are given in the job descriptions. The description also includes the responsibility for diminishing risks.	The organisation has defined that managing exceptional situations is part of organising security. Powers and responsibilities are given in the job descriptions.		

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 604.0 **Does the organisation employ methods to identify security incidents and to carry out protective and corrective measures?** *What the question assesses: does the organisation employ methods to monitor the security situation and are there methods and preparedness in place to carry out protective and corrective measures*	There has to be an established method in the organisation to report on the security incidents.	There has to be an established method in the organisation to report on the security incidents. The emergence of these has to be monitored.	The organisation has a documented system with which to monitor and report on the security incidents for all subdivisions of security. The monitoring system is constant. The organisation has specified responsibilities and powers to carry out protective and corrective measures.	There has to be an established method in the organisation to report on the security incidents. The emergence of these has to be monitored.		
A 605.0 **Does the organisation follow procedures to ensure that protective and corrective security measures are effective and correctly targeted?** *What the question assesses: are the measures correct to ensure security?*	No requirements.	The effect of security measures is assessed and the organisation has a clear idea of the input-output ratio.	The desired and achieved effects of security measures are compared. The organisation has a clear idea of the input-output ratio.	The effect of security measures is assessed and the organisation has a clear idea of the input-output ratio.		

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 606.0 **Does the organisation follow procedures to assess the risks which are caused by the planned corrective measures?** *What the question assesses: when security systems are changed, is it ensured that this will not lead to new threats or danger situations*	No requirements.	The security action process includes an assessment of the negative effects of changes.	The security action process includes an assessment of the negative effects of changes.	The security action process includes an assessment of the negative effects of changes.		
A 607.0 **Does the organisation follow procedures to analyze the effects of security measures?** *What the question assesses: does the organisation document and analyse the security measures and their effects?*	The organisation observes the effects of security measures.	The organisation analyzes the effects of security measures at least annually. For example, statistics provide a way to observe changes in the frequency of a danger situation.	The organisation follows a process which, in addition to documentation, analyses the security measures on a regular basis and their effects on the security level and activities at least annually. The analyses benefit the development of security work.	The organisation observes the effects of security measures.		

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 608.0 **Is there a procedure in place in the organisation to ensure that significant changes in the information processing environment take place in a controlled way?** *(ex I 109.0)* *Note! The required mode of implementation depends of the asset.* *For additional information, see annex 1 (A 608.0)*	A change management procedure is in place for changes related to data processing.	A change management procedure is in place for changes related to data processing.	A change management procedure is in place for changes related to data processing.	A change management procedure is in place for changes related to data processing.	ISO/IEC 27002 Luku 12 ja 10.1.2, PCI DSS 6.4, COBIT 4.1 AI6, VAHTI 2/2010, VAHTI 3/2010, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/ guidelines/guidelines_pdf.pdf	

Security documentation and its management, subdivision A700

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 701.0 **Does the organisation have established processes or modes of operation about** • **security files/security registers or documentation methods?** • **specification and tracing of information in security documentation?** • **the storage time, place and responsibilities of security documentation?** *What the question assesses: is there a system in place with which to manage the above-mentioned factors?*	The organisation has a system in place which contains own guidelines and registers the security incidents.	The organisation has a system in place which contains own guidelines and registers the security incidents. The system fulfils the requirements laid down by legislation (incl. a file description).	The organisation has a user-friendly and comprehensive information management system which has been extended to all levels of the organisation. The system includes security registers (such as permits) and other documents (such as guidelines). When saving information, it is possible to specify and trace events. As for the confidentiality of the information and the storage time, the requirements laid down by legislation are met.	The organisation has a system in place which contains own guidelines and registers the security incidents.		
A 702.0 **Do the registers also include information about the level of security goals to be achieved?** *What the question assesses: has the goal-setting been clear and is it easy to use the system to verify the achievement of the goals?*	No requirements.	The organisation can show the level of the achieved security goals at least annually.	The organisation has an information management system which can produce updated information. The reports can be identified and are comparable as for time, place and topic.	The organisation can show the level of the achieved security goals at least annually.		

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 703.0 **Do the security registers contain information about the provided security training?** *What the question assesses: is security training registered in such a way that their adequacy and validity can be verified? Have the set requirements been achieved?*	The organisation runs a training register with which to verify the given training and its content.	The organisation runs a training register with which to verify the given training, its content and period of validity.	The organisation runs a training register on the various areas of security as a separate or integral part of the overall training register. With the given information it is possible to monitor that training has been provided for all the tasks requiring training. When the training has become outdated, refresher training or continuing training can be provided.	The organisation runs a training register with which to verify the given training and its content.		
A 704.0 **Can it be verified, on the basis of the documentation, that the level of security training is high enough?** *What the question assesses: have quantitative and qualitative requirements been set for security training and is the completion registered?*	No requirements.	Level requirements have been entered into the organisation's training register and, to ensure their completion, the job will not be started before the training requirement has been met.	Level requirements have been entered into the organisation's training register and, to ensure their completion, the job will not be started before the training requirement has been met.	Level requirements have been entered into the organisation's training register and, to ensure their completion, the job will not be started before the training requirement has been met.		

Security training, increasing awareness and knowhow, subdivision A800

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 801.0 **Are all the personnel aware of the importance of observing security requirements and the correct modes of operation?** *What the question assesses: the maturity level of the organisation's security culture and the commitment of the management to constantly improve security through training.*	The personnel participating in separate projects have been trained according to the project-related requirements.	The entire personnel in the organisation have been trained in the requirements for personnel security, premises security and information assurance. The personnel working on projects have been trained according to the project-related requirements.	The entire personnel in the organisation have been trained in the requirements for security. The personnel working on projects have been trained according to the project-related requirements.	The entire personnel in the organisation have been trained in the requirements for security. The personnel working on projects have been trained according to the project-related requirements.		
A 802.0 **Has it been ensured that the personnel know the security risks in connection with their own job?** *What the question assesses: has the risk assessment of security been implemented in such a way that the personnel is involved in making assessments and knows the security risks in connection with their work.*	In connection with risk assessment at least the following is dealt with: personnel security, premises security and information assurance. The personnel are told about the security risks in connection with their jobs.	In connection with risk assessment at least the following is dealt with: personnel security, premises security and information assurance. The personnel are told about the security risks in connection with their jobs.	In connection with risk assessment, the matters pertaining to all subdivisions of security are dealt with. The personnel take part in led risk management.	In connection with risk assessment at least the following is dealt with: personnel security, premises security and information assurance. The personnel are told about the security risks in connection with their jobs.		

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 803.0 **Has it been ensured that the personnel can act correctly in situations where security is under threat?** *What the question assesses: in exceptional situations, the management of security risks, e.g., premises security for fires, the principles of information retrieval for information assurance*	There are documented operational models for the most important exceptional situations and exercises are organised about the most central ones.	The organisation is aware of the major security risks threatening it. There are documented operational models for the most important exceptional situations and exercises are organised about the most central ones on a regular basis.	The organisation has compiled documentation based on risk assessment and there is an action plan training for the most significant security risks. There are training for managing exceptional situations and exercises in the operational model.	The organisation is aware of the major security risks threatening it. There are documented operational models for the most important exceptional situations and exercises are organised about the most central ones.		
A 803.1 **How does the organisation control that the instructions for information assurance are observed?** *Additional question: has it been defined how to handle possible disclosure of classified information and what the consequences are?* *(ex I 206.0)*	1) The observance of the instructions for information assurance is controlled and breaches are addressed. 2) The handling and consequences of breaches of information assurance are defined. 3) The handling and consequences are the same for the entire personnel.	In addition to the base level requirements: the breaches of information assurance are looked into by authorities.	In addition to the base level requirements: the breaches of information assurance are looked into by authorities.	The observance of the instructions for information assurance is controlled and breaches are addressed.	ISO/IEC 27002 8.2.3, VAHTI 8/2006 Can be verified by clarifying a. how control is carried out in practice, b. what kind of breaches have emerged in recent years, and c. how breaches have been addressed.	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 804.0 **Does the organisation have a procedure to establish what kind of security training the personnel need for their tasks?** *What the question assesses: is there a process in place to assess the need for training taking into account legal requirements, central security matters and general security awareness requirements.*	No requirements.	The organisation has a function to define the requirement levels of security training at least for personnel security, premises security and information assurance.	The organisation has a function to assess the target groups of training and the content and quality of the provided training.	The organisation has a function to define the requirement levels of security training at least for personnel security, premises security and information assurance.		
A 805.0 **Does the organisation have a procedure to ensure that the personnel have the aptitude, security training, familiarity and experience required for their tasks?** *What the question assesses: the possibility to clarify the level of security training*	The security training register provides the information whether the person in question has had the training required for the job.	The security training register provides the information about the security training level required for the job.	The security training register provides the information about the security training level required for the job.	The security training register provides the information about the security training level required for the job.		

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 806.0 **Has the organisation made sure that there are adequate instructions, training and information?** *(ex I 204.0)*	The organisation has made sure that there are adequate instructions, training and information. 1) During introduction to duties the personnel have been instructed how to act in line with the security principles of the organisation. The instructions/training shall cover the major work situations (basic use, distant use, the use during work-related travel, maintenance, and so on) and work methods. 2) Employees who through their status could access classified information are given precise instructions right at the beginning and later on a regular basis about the necessity of security measures and their implementation methods. 3) Guidelines for secure use have been provided for the systems handling classified information. 4) Guidelines for the classification, handling (incl. encryption) and saving of information has been drafted and introduced. 5) The personnel have been instructed and obligated to report on information assurance incidents and threats. 6) Users will be informed of future security flaw updates of work stations with the level of accuracy needed to raise their awareness of what is required from them. 7) Users will be informed of the most significant current threats against the users in the organisation (for example, targeted attacks). 8) The maintenance personnel of the systems in questions have completed a manufacturer-specific/environment-specific security training, other generally accepted security training applicable to the environment, or the maintenance personnel have in other ways acquired adequate knowhow to safely maintain the systems in question.	In addition to the base level: the security training given to the personnel has been documented.	In addition to the base level: the security training given to the personnel has been documented.	The organisation has made sure that there are adequate instructions, training and information. During introduction to duties the personnel have been instructed how to act in line with the security principles of the organisation. The instructions/training shall cover the major work situations (basic use, distant use, the use during work-related travel, maintenance, and so on) and work methods.	ISO/IEC 27002 10.7.3, ISO/IEC 27002 13.1.1, ISO/IEC 27002 7.2.2, ISO/IEC 27002 8.2.2, PCI DSS 12.6, COBIT 4.1 DS7, “Handling instructions for nationally classified data” by the National Security Authority, VAHTI 8/2006, the EU code of security 6952/2/11 REV2 /1.4.2011liite I, VAHTI 2/2010, VAHTI 3/2010, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/ guidelines/guidelines_pdf.pdf Can be verified for example by asking a few randomly chosen users in connection with a review how they have been instructed to observe information assurance.	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 807.0 **Has the Acceptable Use Policy been defined for information and data processing services and are the personnel informed accordingly?** *(ex I 205.0)*	1) The AUP for assets related to information and data processing services has been defined and documented. 2) The AUP addresses at least the question of whether it is allowed to use the information systems of the organisation for personal matters (e-mail, disk space, the use of banking services, and so on). 3) The personnel have been clearly informed of the AUP. 4) The personnel have an easy access to the AUP.	1) The AUP for assets related to information and data processing services has been defined and documented. 2) The AUP addresses at least the question of whether it is allowed to use the information systems of the organisation for personal matters (e-mail, disk space, the use of banking services, and so on). 3) The personnel have been clearly informed of the AUP. 4) The personnel have an easy access to the AUP.	1) The AUP for assets related to information and data processing services has been defined and documented. 2) The AUP addresses at least the question of whether it is allowed to use the information systems of the organisation for personal matters (e-mail, disk space, the use of banking services, and so on). 3) The personnel have been clearly informed of the AUP. 4) The personnel have an easy access to the AUP.	1) The AUP for assets related to information and data processing services has been defined and documented. 2) The AUP addresses at least the question of whether it is allowed to use the information systems of the organisation for personal matters (e-mail, disk space, the use of banking services, and so on). 3) The personnel have been clearly informed of the AUP. 4) The personnel have an easy access to the AUP.	ISO/IEC 27002 7.1.3, PCI DSS 12.3, VAHTI 8/2006 Can be verified by checking the existence and contents of the AUP and, in addition, whether the personnel have an easy access to the policy. It will also be established how the personnel have been informed of the AUP.	

Reports and inspections by the management, subdivision A900

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 901.0 **Does the person responsible for security report directly to the organisation's top management about security-related matters?** *What the question assesses: the commitment of the management to security. Does the security management have a direct, fast and effective channel to the management of the organisation?*	The person responsible for security reports directly to the management on a regular basis in such a way that the steering group is aware of the security work level and security situation. It must be possible to immediately report significant incidents or changes to the management, e.g. by means of the crisis management procedure.	The person responsible for security reports directly to the management on a regular basis in such a way that the steering group is aware of the security work level and security situation. It must be possible to immediately report significant incidents or changes to the management, e.g. by means of the crisis management procedure.	The person responsible for security reports to the managing director, the vice managing director, the steering group or to a member of the steering group.	The person responsible for security reports directly to the management on a regular basis in such a way that the steering group is aware of the security work level and security situation. It must be possible to immediately report significant incidents or changes to the management, e.g. by means of the crisis management procedure.		
A 902.0 **Does the organisation's top management check on a regular basis (at least once a year) the functioning of the security system?** *What the question assesses: the commitment of the management to continuously improving the security work and to quality management.*	Reporting on security matters is incorporated into the management process.	As part of the organisation's management process, security matters are comprehensively presented, at least once a year, to the steering group. A member of the steering group has been designated to follow security-related matters as part of his/her job description.	As part of the organisation's management process, security matters are comprehensively presented, at least once a year, to the steering group, e.g. in the management review. A member of the steering group has been designated to follow security-related matters as part of his/her job description.	At least annually conducted reporting on security matters is incorporated into the management process.		

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 903.0 **When the top management carries out checks, are the suitability of the security system, sufficient resources and the effectiveness of activities assessed?** *What the question assesses: the quality and scope of reporting.*	No requirements.	The security goals of the organisation and achieving them are presented in a measurable form.	The security goals of the organisation and achieving them are presented in a measurable form.	The security goals of the organisation and achieving them are presented in a measurable form.		
A904.0 **Are the follow-up checks documented?** *What the question assesses: the systematic action taken by the organisation's management and the possibility to view the effects and effectiveness of the decisions taken on the basis of the follow-up.*	No requirements.	Follow-up checks are documented.	Follow-up checks are documented in the information management system of security.	Follow-up checks are documented.		

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
A 905.0 **Do the follow-up checks provide the basis for continuous improvement, in other words, do they influence the content of policies and of goals?** *What the question assesses: can security management be considered as a high-quality action, where policies and goals, as well as operational models of security are constantly being improved.*	No requirements.	Security management includes a process where feedback from the management's review is used to reassess security policy and security goals.	The security work process of the organisation includes a function where the results presented in the management's review and the resulting conclusions are employed to reassess security policy and security goals.	Security management includes a process where feedback from the management is used to reassess the security policy and security goals.		

P Personnel Security

Content

Scope of application

In some tasks the personnel is required to deal with classified information of the authorities or with such sensitive information of the employer (business or trade secrets and professional secrets) where serious damage could be caused for the employer if such information were used against security regulations. The criteria aim to contribute to the selection process where the persons best suited for these tasks were chosen. The criteria can be used in security agreements between companies and with the authority.

The criteria for personnel security starts with a technical section which is the same for all protection levels. The aim is to manage the personnel who have access to sensitive or classified information.

The criteria then continue as a list of requirements divided by levels of confidentiality (IV-II) where the matters to be considered for recruitment or selection are dealt with. The list of requirements can be applied to new recruitments but, where applicable, also to selecting suitable professionals for a classified project from among the personnel. When external subcontractors are used it is useful to take up already in the contract negotiations that the personnel of the co-contractor who participate in the contract may be subjected to security clearance. Outside of requirements, also the personnel criteria contain recommendations for the business community.

Protection of privacy

When the annexed regulations are applied the Act on the Protection of Privacy in Working Life should be taken into consideration. In particular it should be remembered that the employer is allowed to only handle information which is directly relevant for the employment, which deals with the rights and duties of the parties or with the benefits that the employer offers to their employees or which is necessary because of the special nature of the employment. An example of this is the requirement of exceptional reliability.

As a rule the employer shall collect the information on the employee from the employee himself/herself or ask for his/her permission to collect the information elsewhere. When credit references are gathered to find out about the reliability of the person no permission is needed but the employee shall be informed of this and of the sources to be used. The employee shall be informed before a decision is taken when the information is collected from elsewhere than the person in question. In this respect the co-operation procedure should provide the basis for the contract of employment.

Instructions and guidelines

Useful instructions and guidelines for a good and safe personnel process are available for example by the Government Information Security Management Board (VAHTI) which has given out guidelines on personnel security as part of information security.

Technical criteria, subdivision P100

The purpose of the subdivision is the management of the personnel who have access to sensitive or classified information.

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
P 101.0 **Has a list been made of the persons taking part in the project?**	A list shall be made of the personnel taking part in the project; the list shall contain the following information: name and personal identity number, the job and the name and department of the company where the person is employed. The person responsible for security of the project shall approve the list of persons.	As on the base level.	As on the base level.	A list shall be made of the personnel taking part in the project; the list shall contain the following information: name and personal identity number, the job and the name and department of the company where the person is employed. The person responsible for security of the project shall approve the list of persons.		
P 102.0 **Have policies been established and is the contact person information valid?** *Additional question: Are the documents on personnel stored in an appropriate way?*	There shall be policy guidelines to immediately inform the person responsible for security in the project of any changes concerning personnel.	There shall be policy guidelines to immediately inform the person responsible for security in the project of any changes concerning personnel.	There shall be policy guidelines to immediately inform the person responsible for security in the project of any changes concerning personnel.	There shall be policy guidelines to immediately inform the person responsible for security in the project of any changes concerning personnel.		
P 103.0 **Does training documentation exist (markings of earlier training)?**	The personnel taking part in the project shall receive training in the project-related security.	The personnel taking part in the project shall receive training in the project-related security.	The personnel taking part in the project shall receive training in the project-related security.	The personnel taking part in the project shall receive training in the project-related security.		

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
P 104.0 **Does a list of visitors exist and is it kept in an appropriate way?** *Additional question:* *Are the hosting personnel aware of how to deal with visitors?*	Unnecessary visits to the premises used in the project shall be avoided. During any visits the data shall be stored so that persons not involved in the project cannot familiarise themselves with it. Visitors shall not be left in the said premises without the host or his/ her representative.	Unnecessary visits to the premises used in the project shall be avoided. During any visits the data shall be stored so that persons not involved in the project cannot familiarise themselves with it. Visitors shall not be left in the said premises without the host or his/her representative.	Unnecessary visits to the premises used in the project shall be avoided. During any visits the data shall be stored so that persons not involved in the project cannot familiarise themselves with it. Visitors shall not be left in the said premises without the host or his/ her representative.	Unnecessary visits to the premises used in the project shall be avoided. During any visits the data shall be stored so that persons not involved in the project cannot familiarise themselves with it. Visitors shall not be left in the said premises without the host or his/ her representative.		
P 105.0 **Are requirements followed in accordance with protection levels or security classification?**	Guidelines for recruitment procedures are applied.	Guidelines for recruitment procedures are applied.	Guidelines for recruitment procedures are applied.	Guidelines for recruitment procedures are applied.		

Securing sufficient competences, subdivision P200

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
P 201.0 **Has the candidate for employment been asked to produce key documents to prove current competences?**	The candidate for employment is asked to provide confirmation of claimed academic and professional qualifications; extract from a personal file (equivalent); recommendations and certificates.	The candidate for employment is asked to provide confirmation of claimed academic and professional qualifications; extract from a personal file (equivalent); recommendations and certificates.	The candidate for employment is asked to provide confirmation of claimed academic and professional qualifications; extract from a personal file (equivalent); recommendations and certificates.	The candidate for employment is asked to provide confirmation of claimed academic and professional qualifications; extract from a personal file (equivalent); recommendations and certificates.	Act on the Protection of Privacy in Working Life, section 4.	
P 202.0 **How is the authenticity of the information given in the interview verified?** *Justification: It is not rare to receive misleading references and certificates.*	The authenticity of the information is checked.	The authenticity of the information is checked.	The authenticity of the information is checked.	The authenticity of the information is checked	After auditing, guidelines are given, if necessary, how this is implemented.	
P 203.0 **Are the competences of the candidate for employment checked with expert questions?**	The authenticity of the background information about the candidate and his/her competences are checked in the interview.	The authenticity of the background information about the candidate and his/her competences are checked in the interview.	The authenticity of the background information about the candidate and his/her competences are checked in the interview.	The authenticity of the background information about the candidate and his/her competences are checked in the interview.		

Other suitability of the candidate for the task, subdivision P300

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
P 301.0 **Is it ensured in the interview that the candidate is able to act in accordance with the values of the company?**	In the interview it is ensured that the person does not face unreasonable choices in his/her tasks. Information is asked about former tasks that affect trust.	In the interview it is ensured that the person does not face unreasonable choices in his/her tasks. Information is asked about former tasks that affect trust.	In the interview it is ensured that the person does not face unreasonable choices in his/her tasks. Information is asked about former tasks that affect trust.	In the interview it is ensured that the person does not face unreasonable choices in his/her tasks. Information is asked about former tasks that affect trust.	Act on the Protection of Privacy in Working Life, section 3	**Also when selecting for a new project. Questions may be asked about restriction of competition contracts or secrecy contracts to test understanding.**
P 302.0 **Is a drug test available if it seems necessary?**	A drug test is required, if necessary.	A drug test is required, if necessary.	A drug test is required, if necessary.	A drug test is required, if necessary.	Act on the Protection of Privacy in Working Life, sections 6, 7, 8, 9 and 14. Act on Co-operation within Undertakings, section 19, paragraph 2 (334/2007).	
P 303.0 **Is the capability of the candidate to perform tasks requiring outstanding reliability verified with tests run by experts?**	Selection and aptitude tests.	Selection and aptitude tests.	Selection and aptitude tests.	Selection and aptitude tests.	Act on the Protection of Privacy in Working Life, section 13.	

Measures after the decision to recruit, subdivision P400

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
P 401.0 **When recruiting for this task, are the pledge of secrecy and the pledge of confidentiality used and if so, what is their exact content?**	The pledge of secrecy and the pledge of confidentiality are used.	The pledge of secrecy and the pledge of confidentiality are used.	The pledge of secrecy and the pledge of confidentiality are used.	The pledge of secrecy and the pledge of confidentiality are used.		**Also when selecting for a new project.**
P 402.0 **Is a probation period used in recruitment and if so, how long is it?**	A probation period is used.	A probation period is used.	A probation period is used.	A probation period is used.	Employment Contracts Act Chapter 1, section 4; chapter 2, section 4.	
P 403.0 **For what tasks is it seen as necessary to establish the information on responsible persons and company connections?** *Additional question: how is the information collected?*	The procedure to establish the information on responsible persons and company connections is in place on a task-by-task-basis.	The procedure to establish the information on responsible persons and company connections is in place on a task-by-task-basis.	The procedure to establish the information on responsible persons and company connections is in place on a task-by-task-basis.	The procedure to establish the information on responsible persons and company connections is in place on a task-by-task-basis.	Personal Data Act, section 8, paragraph 1 sub-paragraph 8.	**From the person in question and from available registers.**
P 404.0 **Is a concise security clearance sought of the person, if possible?**	A concise security clearance is sought, as necessary, to protect the premises, location or operations.	A concise security clearance is sought, as necessary, to protect the premises, location or operations.	A concise security clearance is sought, as necessary, to protect the premises, location or operations.	A concise security clearance is sought, as necessary, to protect the premises, location or operations.	Act on Background Checks, section 19.	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
P 405.0 **Is it possible to seek a basic security clearance for this project or task?**	No requirements.	A basic security clearance is sought to protect information as necessary.	A basic security clearance is sought to protect information as necessary.	No requirements.		Also when selecting for a new project. The seeker is either the recruiter or the owner of the asset in accordance with the security contract.
P 406.0 **Is credit information collected on the persons selected for the project or task?**	No requirements.	No requirements.	No requirements.	Credit references on the persons may be collected respecting the legal constraints.	Act on the Protection of Privacy, section 5 a.	
P 407.0 **Are non-disclosure or secrecy clauses drafted and introduced in such a way that they reflect the information protection needs of the organisation?**	All personnel, suppliers, partners, sub-contractors and external users sign a non-disclosure or secrecy clause before they are granted access to classified information.	All personnel, suppliers, partners, sub-contractors and external users sign a non-disclosure or secrecy clause before they are granted access to classified information.	All personnel, suppliers, partners, sub-contractors and external users sign a non-disclosure or secrecy clause before they are granted access to classified information.	Non-disclosure or secrecy clauses reflect the information protection needs of the organisation.	ISO/IEC 27002 6.1.5, ISO/IEC 27002 8.1.3 The entire secrecy chain must be supported by secrecy clauses so that when the organisation makes a contract with a sub-contractor or partner company and, in turn, the sub-contractor or partner company makes a contract with their employee, the goal is to establish personal responsibility (employee) and liability (sub-contractor or partner).	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
P 408.0 **Main question: Are the key personnel identified and the dependency of the organisation on them recognised?** *Additional question: Are there plans for personnel or procedures to back them up?*	1. The key personnel of the organisation are recognized and a back-up system is established by for example adequate documention and reserve personnel procedure. 2. The reserve personnel have been trained to their exceptional tasks.	1. The key personnel of the organisation are recognized and a back-up system is established by for example adequate documention and reserve personnel procedure. 2. The reserve personnel have been trained to their exceptional tasks.	1. The key personnel of the organisation are recognized and a back-up system is established by for example adequate documention and reserve personnel procedure. 2. The reserve personnel have been trained to their exceptional tasks.	The key personnel of the organisation are recognized and a back-up system is established following the results of the risk assessment.	VAHTI 8/2006, COBIT 4.1 PO4.13, COBIT 4.1 PO7	

Measures for concluding the contract of employment, subdivision P500

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
P 501.0 **How is it ensured that the candidate and the employer agree on the tasks, responsibilities, rights and duties of the employee in particular as far as information protection is concerned?**	The tasks, responsibilities, rights and duties are defined as clearly as possible for example in the job description.	The tasks, responsibilities, rights and duties are defined as clearly as possible for example in the job description.	The tasks, responsibilities, rights and duties are defined as clearly as possible for example in the job description.	The tasks, responsibilities, rights and duties are defined as clearly as possible for example in the job description.		Also when selecting for a new project.
P 502.0 **How a new employee is introduced to the security regulations of the company?** *Justification: Face-to-face discussion with the security manager (equivalent) about the company's security regulations and their significance considerably improves compliance with regulations.*	Introduction to security.	Introduction to security.	Introduction to security.	Introduction to security.		Also when selecting for a new project.
P 503.0 **How a new employee is introduced to his/her tasks and the operations of the company?**	Introduction to operations and tasks.	Introduction to operations and tasks.	Introduction to operations and tasks.	Introduction to operations and tasks.		Also when selecting for a new project.

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
P 504.0 **How is information security training organised in the company?** *Additional question: how often and how are competences updated?*	Training in information security matters, updates on a regular basis.	Training in information security matters, updates on a regular basis.	Training in information security matters, updates on a regular basis.	Training in information security matters, updates on a regular basis.		Also when selecting for a new project.
P 505.0 **How are process descriptions implemented about authorisation and granting access rights to information and the premises?**	Authorisation and granting access rights to information and the premises.	Authorisation and granting access rights to information and the premises.	Authorisation and granting access rights to information and the premises.	Authorisation and granting access rights to information and the premises.	VAHTI 2/2008	Also when selecting for a new project.

Measures during employment, subdivision P600

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
P 601.0 **How are the guidelines regarding substitutes and key personnel (exemptions from military service for special assignments)?**	The guidelines exist.	The guidelines exist and are maintained.	The guidelines exist and are maintained.	The guidelines exist.		A request is made to see the guidelines.
P 602.0 **How are job satisfaction and job motivation taken care of in the company?** *Additional question: Are personnel encouraged to take part in supplementary education and improve competences?*	Job satisfaction and job motivation are taken care of.	The maintenance of job satisfaction and job motivation can be verified in documents.	It can be verified in documents that job satisfaction and job motivation are taken care of.	Job satisfaction and job motivation are taken care of.		Justification: Low job satisfaction and job motivation levels significantly reduce efficiency and they pose a security risk.
P 603.0 **How is the follow-up on wellbeing at work and working capacity arranged?**	Follow-up on wellbeing at work and working capacity is arranged.	Follow-up on wellbeing at work and working capacity is arranged.	Follow-up on wellbeing at work and working capacity is arranged.	Follow-up on wellbeing at work and working capacity is arranged.	E.g. Occupational Health Care Act, section 13.	Justification: The follow-up on working capacity is an important security issue also in tasks that require reliability.
P 604.0 **What measures are taken when the employee starts to act in a worrying manner without a clear reason? Who is responsible for taking action?**	Significant changes in the behavior or the way to act; instructions needed when professional misconduct is suspected or there is a need for referring the person to medical treatment.	Significant changes in the behavior or the way to act; instructions needed when professional misconduct is suspected or there is a need for referring the person to medical treatment.	Significant changes in the behavior or the way to act; instructions needed when professional misconduct is suspected or there is a need for referring the person to medical treatment.	Significant changes in the behavior or the way to act; instructions needed when professional misconduct is suspected or there is a need for referring the person to medical treatment.		Justification: Decreased working capacity which is caused e.g. by alcoholism or professional misconduct often result in irregular behaviour.

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
P 605.0 **Is there a procedure for terminating a contract of employment?**	There is a procedure in place in the organisation for terminating a contract of employment.	There is a procedure in place for terminating a contract of employment in the organisation.	There is a procedure in place for terminating a contract of employment in the organisation.	There is a procedure in place for terminating a contract of employment in the organisation.		Justification: Following the correct procedure when terminating a contract of employment is an important security issue.
P 606.0 **How are visits arranged?**	There is a procedure in place in the organisation for managing the visitors in the different parts of the premises.	There is a procedure in place in the organisation for managing the visitors in the different parts of the premises.	There is a procedure in place in the organisation for managing the visitors in the different parts of the premises.	There is a procedure in place in the organisation for managing the visitors in the different parts of the premises.		A request is made to see the instructions for visits.

F Physical Security

Contents

Introduction

The auditing criteria for physical security focus on the premises security but other elements of physical security are also taken into account where necessary. The cornerstone of the criteria is the protection of sensitive or classified information, based on defence in depth so that access to such information is prevented as early as possible. Protection requirements become stricter the closer physically one gets to the information (the so-called security zone model). Often the most important assets are the computer rooms where the critical parts of the information systems are located. A number of specific requirements for these are set in the subdivision Information Assurance of these criteria.

Security of Area, subvision F100

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
F 101.0 **As for parking, is it necessary to consider protection from electronic intelligence from a nearby area?**	No requirements for the roads and the parking area.	No requirements for the roads and the parking area.	The parking area shall be located at an appropriate distance or it is protected in such a way that intelligence based on electromagnetic radiation cannot be collected from there. The parking area shall be monitored so that it is not possible to take electronic intelligence devices there. It can also be in a dead spot to make direct electronic intelligence impossible.	No requirements for the roads and the parking area.		If the premises or equipment are not protected, it must be ensured that it is not possible to collect intelligence from the parking area.
F 102.0 **As for the loading and unloading areas, is it necessary to consider protection from electronic intelligence from a nearby area?**	No requirements for the loading and unloading areas.	No requirements for the loading and unloading areas.	The loading and unloading areas shall be located at an appropriate distance or it is protected in such a way that intelligence based on electromagnetic radiation cannot be collected from there. The loading and unloading areas shall be monitored so that it is not possible to take electronic intelligence devices there. It can also be in a dead spot to make direct electronic intelligence impossible.	No requirements for the loading and unloading areas.		If the premises or equipment are not protected, it must be ensured that it is not possible to collect intelligence from the loading and unloading areas.

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
F 103.0 **Is it necessary to control movement on the site and premises with fences, gates and traffic barriers?**	There are no structural requirements for fences, gates and traffic barriers. If a fence is used to strengthen large but weak vehicular doors the fence shall meet the following minimum requirements: -new fence: a wire mesh fence made of zinc-coated steel wire, h= min 2.25m mesh max 40*40 mm, wire thickness min 3.0 mm, distance from the ground max 0.05m, a minimum of two barbed wire on top of each other to be fixed onto the top of the fence (zinc-coated steel min 2*1.6mm), one barbed wire between the bottom side of the wire mesh and the ground (zinc-coated steel min 2*1.6mm), the height of the entire fence structure min 2.40m, the fence posts 70mm in diameter, made of aluminium profile (or equivalent), the distance between posts max 3.00m, the fastening screws (or equivalent) of the wire mesh shall be on the inside of the fenced area. The gates shall be fitted with access control.	There are no structural requirements for fences, gates and traffic barriers. If a fence is used to strengthen large but weak vehicular doors the fence shall meet the following minimum requirements: -new fence: a wire mesh fence made of zinc-coated steel wire, h= min 2.25m mesh max 40*40 mm, wire thickness min 3.0 mm, distance from the ground max 0.05m, a minimum of two barbed wire on top of each other to be fixed onto the top of the fence (zinc-coated steel min 2*1.6mm), one barbed wire between the bottom side of the wire mesh and the ground (zinc-coated steel min 2*1.6mm), the height of the entire fence structure min 2.40m, the fence posts 70mm in diameter, made of aluminium profile (or equivalent), the distance between posts max 3.00m, the fastening screws (or equivalent) of the wire mesh shall be on the inside of the fenced area. The gates shall be fitted with access control.	There are no structural requirements for fences, gates and traffic barriers. If a fence is used to strengthen large but weak vehicular doors the fence shall meet the following minimum requirements: -new fence: a wire mesh fence made of zinc-coated steel wire, h= min 2.25m mesh max 40*40 mm, wire thickness min 3.0 mm, distance from the ground max 0.05m, a minimum of two barbed wire on top of each other to be fixed onto the top of the fence (zinc-coated steel min 2*1.6mm), one barbed wire between the bottom side of the wire mesh and the ground (zinc-coated steel min 2*1.6mm), the height of the entire fence structure min 2.40m, the fence posts 70mm in diameter, made of aluminium profile (or equivalent), the distance between posts max 3.00m, the fastening screws (or equivalent) of the wire mesh shall be on the inside of the fenced area. The gates shall be fitted with access control.	There are no structural requirements for fences, gates and traffic barriers. If a fence is used to strengthen large but weak vehicular doors the fence shall meet the following minimum requirements: -new fence: a wire mesh fence made of zinc-coated steel wire, h= min 2.25m mesh max 40*40 mm, wire thickness min 3.0 mm, distance from the ground max 0.05m, a minimum of two barbed wire on top of each other to be fixed onto the top of the fence (zinc-coated steel min 2*1.6mm), one barbed wire between the bottom side of the wire mesh and the ground (zinc-coated steel min 2*1.6mm), the height of the entire fence structure min 2.40m, the fence posts 70mm in diameter, made of aluminium profile (or equivalent), the distance between posts max 3.00m, the fastening screws (or equivalent) of the wire mesh shall be on the inside of the fenced area. The gates shall be fitted with access control.		All persons and vehicles entering the site of the premises have been checked.
F 104.0 **Is it possible to monitor the movement within the area through a CCTV?**	Sufficient lighting required for the CCTV also in the dark must be taken into account. No other specific requirements.	Sufficient lighting required for the CCTV also in the dark must be taken into account. No other specific requirements.	Sufficient lighting required for the CCTV also in the dark must be taken into account. No other specific requirements.	Sufficient lighting required for the CCTV also in the dark must be taken into account. No other specific requirements.		It must be possible to identify accurately enough the vehicles and people with the CCTV.

Structural security, subdivision F200

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
F 201.0 **What material are the walls, ceiling and floor of the room?**	The walls, ceiling and floor are of regular office structure.	The walls, ceiling and floor of the room shall be made of concrete, steel, tiles or strong wood. Faulty structures must be strengthened. It shall be made impossible to remove whole wall elements from the outside.	The walls, ceiling and floor of the room shall be made of concrete, steel or strong wood. Faulty structures must be strengthened. It shall be made impossible to remove whole wall elements from the outside.	The walls, ceiling and floor are of regular office structure.		

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
F 202.0 **Are there windows below four meters in the room(s)?** *High-level (II) question:* *Are there windows above four meters in the room(s)?*	The windows on the ground level (below 4 m) shall be covered or direct visibility is otherwise prevented from outside the secure area.	The windows on the ground level (below 4 m) shall be provided with the protective glass (SFS-EN 356 / P6B) or a more secure arrangement. In addition, the fastening of the frame to the surrounding wall must be taken into account as well as the structure of the hinges and the locking system.	The rooms on the ground level (below 4m) must not have windows. The windows above the ground level (above 4 m) shall be provided with the protective glass (SFS-EN 356 / P6B) or a more secure arrangement which is safe against breaking and entering and does not carry sound vibrations to the outermost glass. In addition, the fastening of the frame to the surrounding wall must be taken into account as well as the structure of the hinges and the locking system. When IT devices have no Tempest protection, a required attenuation can be achieved by building a Faraday´s cage to the room (if the area has no access control at the minimum distance of 300 m from the asset, the windows and the room must be provided with EMR countermeasures.	The windows shall be protected in such a way that they cannot be opened from the outside without breaking them.		It is easier to enter through weak window openings than through a door.
F 203.0 **Have the room(s) skylights?**	Skylights/trap doors must be locked.	Skylights (or the windows on the level of the roof terraces) must be fitted with a protective glass (SFS-EN 356 / P6B) or a more secure arrangement. In addition, the fastening of the frame to the surrounding wall must be taken into account as well as the structure of the hinges and the locking system.	There must not be skylights or terrace roofs on the level II premises.	Skylights/trap doors must be locked and they are recommended to be fitted with a protective film P1A (SFS-EN 356) or a more secure arrangement.		It is easier to enter through weak window openings than through a door.

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
F 204.0 **Are there any other openings in the walls, ceiling and floor of the room that could be used for intrusion?**	No requirements.	The walls, ceiling and floor of the room shall not have any other openings than doors, windows, smoke outlets or air inlets secured with intrusion detection systems. The openings can be closed with bars or strong steels grilles.	The walls, ceiling and floor of the room shall not have any other openings than doors, windows, smoke outlets or air inlets secured with intrusion detection systems. The openings can be closed with bars or strong steels grilles.	No recommendations.	The walls, ceiling and floor of the room shall only have locked openings.	Ventilation ducts, cable ducts, smoke outlets and air inlets can be used for intrusion.
F 205.0 **What kind of doors lead to the room?**	No requirements.	The doors must meet the requirements of the burglary resistant SFS EN 1627 class 3. As for door structures, attention must also be paid to the frame structure, the gap between the door and the door frame and fitting the frames to the wall structure. The frame structure must prevent the sawing of fastening screws from the outside. The gap between the door and the door frame must not exceed 2 mm. Seeing through the door to the area to be protected shall be prevented.	The doors must meet the requirements of the burglary resistant SFS EN 1627 class 3. As for door structures, attention must also be paid to the frame structure, the gap between the door and the door frame and fitting the frames to the wall structure. The frame structure must prevent the sawing of fastening screws from the outside. The gap between the door and the door frame must not exceed 2 mm. Seeing through the door to the area to be protected shall be prevented.	No recommendations.		Fastening the skeletal structure of doors, frame structures and frames to the walls shall be strong on higher security levels.

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
F 206.0 **Are there very large doors, e.g. garage doors?**	When such doors cannot be built on the basis of the principles presented above e.g. because of their large size, special attention shall be paid to technically protecting the opening.	When such doors cannot be built on the basis of the principles presented above e.g. because of their large size, special attention shall be paid to technically protecting the opening. Steel barriers shall be in place to stop vehicles from passing through. Approved roller bars function as breaking and entering prevention.	When such doors cannot be built on the basis of the principles presented above e.g. because of their large size, special attention shall be paid to technically protecting the opening. Steel barriers shall be in place to stop vehicles from passing through. Approved roller bars function as breaking and entering prevention.	No recommendations.		Overhead garage doors are often the weak points when looking at breaking and entering prevention.
F 207.0 **How well do sounds carry to adjacent rooms?**	Sound insulation shall be good enough to guarantee that no sounds are directly carried to surrounding rooms.	Sound insulation shall be good enough to guarantee that no sounds are directly carried to surrounding rooms.	Sound insulation shall be good enough to guarantee that no sounds are directly carried to surrounding rooms via cable troughs or air-conditioning casings, for example. Sound insulation material to be added to the cable troughs, sound traps to the AC ducts.	No recommendations.		No voices shall be carried to unprotected adjacent rooms from the room that is protected.
F 208.0 **Is there a safe or a vault in the room for storing the data?**	There is a safe in the room or if classified data is stored in a locked closet the room shall be fitted with intrusion detection systems (the level of the intruder detection centre shall be at least FK class 2). Doors and rooms shall be controlled.	There is a safe installed to the room (minimum requirement Euro II SFS-EN 1143-1) or a vault (minimum requirement Euro IV).	There is a safe installed to the room (minimum requirement Euro II SFS-EN 1143-1) or a vault (minimum requirement Euro IV).	There is a safe (minimum requirement Euro I SFS-EN 1143-1) in the room or if classified data is stored in a locked safe the room shall be fitted with intrusion detection systems (the level of the intruder detection centre shall be at least FK class 2).	Doors and rooms shall be controlled.	Information shall be stored in a locked safe or vault to allow for a longer response time.
F 209.0 **How are access rights managed?**	Access rights to the room(s) in question shall be granted by the designated person responsible for this in the company.	Access rights to the room(s) in question shall be granted by the designated person responsible for this in the company.	Access rights to the room(s) in question shall be granted by the designated person responsible for this in the company.	Access rights to the room(s) in question shall be granted by the designated person responsible for this in the company.		The responsibility for access rights to the rooms shall be unambiguously designated in the process.

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
F 209.1 **Are the access and user rights of all users controlled in accordance with good information management practice?** *Additional question: What kind of procedures are in place to ensure that users get access only to the information they are entitled to?* *Further details in annex 1.*	1) Person responsible for handling access rights has been named. 2) There is a list of the users of the system. 3) Users have only those rights they need to fulfill their tasks. 4) When user rights are granted, it is checked that the user is a member of the personnel or an otherwise authorised user. 5) Handling and granting of user rights has been instructed. 6) There are instructions for immediately informing relevant persons of any changes in the personnel as well as instructions of the action to be taken. 7) The changes in user rights and access rights are communicated both to physical access control and logical access and usage. 8) User rights and access rights are reviewed on a regular basis. 9) There is a separate register on the authorised personnel of co-operation partners or other external actors. 10) Each granted user right yields a document (on paper or electronically).	1) Person responsible for handling access rights has been named. 2) There is a list of the users of the system. 3) Users have only those rights they need to fulfill their tasks. 4) When user rights are granted, it is checked that the user is a member of the personnel or an otherwise authorised user. 5) Handling and granting of user rights has been instructed. 6) There are instructions for immediately informing relevant persons of any changes in the personnel as well as instructions of the action to be taken. 7) The changes in user rights and access rights are communicated both to physical access control and logical access and usage. 8) User rights and access rights are reviewed on a regular basis. 9) There is a separate register on the authorised personnel of co-operation partners or other external actors. 10) Each granted user right yields a document (on paper or electronically).	1) Person responsible for handling access rights has been named. 2) There is a list of the users of the system. 3) Users have only those rights they need to fulfill their tasks. 4) When user rights are granted, it is checked that the user is a member of the personnel or an otherwise authorised user. 5) Handling and granting of user rights has been instructed. 6) There are instructions for immediately informing relevant persons of any changes in the personnel as well as instructions of the action to be taken. 7) The changes in user rights and access rights are communicated both to physical access control and logical access and usage. 8) User rights and access rights are reviewed on a regular basis. 9) There is a separate register on the authorised personnel of co-operation partners or other external actors. 10) Each granted user right yields a document (on paper or electronically).	1) Users have only those rights they need to fulfill their tasks. 2) When user rights are granted, it is checked that the user is a member of the personnel or an otherwise authorised user. 3) Handling and granting of user rights has been instructed. 4) There is a clear and well-functioning way to notify changes and to make necessary changes. 5) The changes in user rights and access rights are communicated both to physical access control and logical access and usage. 6) A person responsible for managing access rights systems is designated.	ISO/IEC 27002 11.1, ISO/IEC 27002 11.1.1, ISO/IEC 27002 11.2.4, ISO/IEC 27002 11.4.1, ISO/IEC 27002 11.6.1, ISO/IEC 27002 8.3.3, COBIT 4.1 PO7, FI NSA guidelines "Handling of international classified information", VAHTI 4/2002, VAHTI 8/2006, EU Council Security Rules 6952/2/11 REV2 /1.4.2011 annex IV, VAHTI 3/2010, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/ guidelines/guidelines_pdf.pdf, http://www.sans.org/critical-security-controls/control.php?id=8, http://www.sans.org/critical-security-controls/control.php?id=11	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
F 209.2 **Main question: What are the procedures to identify external employees and visitors?** *Additional question: Have the personnel been given instructions for hosting visitors?* *Note: Visible identifiers are not necessary when only few persons work in the organisation and they certainly know each other and the duration of each other's employment. Visitors may be left in a public space on their own.*	1) The personnel have been instructed for hosting visitors. 2) Badges with photographs (or equivalent visible identifiers) are used in the organisation. 3) All contractors, external users, maintenance personnel and visitors use a visible identifier (identity card/ visitor badge). 4) Personnel have been instructed to react to anyone who is not wearing a badge (or equivalent visible identifier) on the premises. 5) Visitors shall never be left alone on the premises without the host or his/her representative.	1) The personnel have been instructed for hosting visitors. 2) Badges with photographs (or equivalent visible identifiers) are used in the organisation. 3) All contractors, external users, maintenance personnel and visitors use a visible identifier (identity card/visitor badge). 4) Personnel have been instructed to react to anyone who is not wearing a badge (or equivalent visible identifier) on the premises. 5) Visitors shall never be left alone on the premises without the host or his/her representative.	1) The personnel have been instructed for hosting visitors. 2) Badges with photographs (or equivalent visible identifiers) are used in the organisation. 3) All contractors, external users, maintenance personnel and visitors use a visible identifier (identity card/visitor badge). 4) Personnel have been instructed to react to anyone who is not wearing a badge (or equivalent visible identifier) on the premises. 5) Visitors shall never be left alone on the premises without the host or his/her representative.	The personnel have been instructed for hosting visitors.	ISO/IEC 27002 9.1.2, PCI DSS 9.2, PCI DSS 9.3, VAHTI 8/2006	
F 210.0 **What kind of locking system does the room have?**	The locking system of the protected room shall be in order. The room shall be always locked when it is not manned. An all-purpose lock at the border of a zone is FK safety class 3.	The locking system of the protected room shall be in order. The room shall be always locked. An all-purpose lock at the border of a zone is FK safety class 3. In addition, a safety lock in place at the border of a zone of safety class 4. Within a zone an all-purpose lock, FK safety class 3.	The locking system of the protected room shall be in order. The room shall be always locked. An all-purpose lock at the border of a zone is FK safety class 3. In addition, a safety lock in place at the border of a zone of safety class 4. Within a zone an all-purpose lock, FK safety class 3.	The locking system of the protected room shall be in order. The room shall be always locked when it is not manned. An all-purpose lock at the border of a zone is FK safety class 3.		The locks have been categorised to different levels on the basis of intrusion prevention.

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
F 211.0 **How is the management of (mechanical) keys arranged?**	The management of keys/ access rights shall be in order. This is taken care of a designated person who has a list of the distributed keys, a locking scheme of the premises and a key card.	The management of keys/ access rights shall be in order. This is taken care of a designated person who has a list of the distributed keys, a locking scheme of the premises and a key card.	The management of keys/ access rights shall be in order. This is taken care of a designated person who has a list of the distributed keys, a locking scheme of the premises and a key card.	The management of keys/ access rights shall be in order. This is taken care of a designated person who has a list of the distributed keys, a locking scheme of the premises and a key card.		For the management of the premises, the storage of extra keys and the controlled making of additional keys shall also be checked.
F 212.0 **Who has keys to the protected room?**	Only designated persons shall have keys/access rights to the protected working areas.	Only designated persons shall have keys/access rights to the protected working areas.	Only designated persons shall have keys/access rights to the protected working areas.	Only designated persons shall have keys/access rights to the protected working areas.		For the management of the premises, it shall always be known who has keys to the protected room.
F 213.0 **Which premises does the master key give access to?**	No requirements.	Access to a room of protection level III with a lower level master key shall not be possible. It is forbidden to remove a level III master key (or equivalent) from the premises of the service providers and sub-contractors.	Access to a room of protection level II with a lower level master key shall not be possible. It is forbidden to remove a level II master key (or equivalent) from the premises of the service providers and sub-contractors.	No recommendations.		A master key does not give access to the protected room.
F 214.0 **Have the guards and building maintenance personnel been given keys to the protected room?**	No requirements.	The keys for the guards and building maintenance personnel shall be sealed in view of exceptional situations.	The keys for the guards and building maintenance personnel shall be sealed in view of exceptional situations. In alert situations two people are expected to arrive at a level II room at the same time.	No recommendations.		Guards and building maintenance personnel shall not have uncontrolled access to the protected room.
F 215.0 **What are the guidelines for maintenance measures in the room?**	No requirements.	No requirements.	Maintenance measures in the room shall be carried out under the supervision of a person approved for the project. During maintenance work it is forbidden to handle level III data in the room in question.	No recommendations.		Even if the information is protected external personnel may learn about the protection measures of the room and bring unauthorised equipment into the room.

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
F 216.0 **Are the maintenance, installation and cleaning of the computer room and its equipment done only under supervision?**	The maintenance, installation and cleaning of the computer room and its equipment take place only by person approved for the security level or under the supervision of the personnel.	In addition to the requirements for the base level the following requirements apply: During maintenance work in the room in question it is forbidden to handle information that is classified to the protection level III (CONFIDENTIAL).	In addition to the requirements for the base level the following requirements apply: During maintenance work in the room in question it is forbidden to handle information that is classified to the protection level II (SECRET).	The maintenance, installation and cleaning of the computer room and its equipment comply with risk assessment. Through risk assessment the following may be applied: work approved only when supervised by own personnel; access given by electric recording control (e.g., electric access key and code); and/or protected with agreements.	VAHTI 8/2006, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/ guidelines/ guidelines_pdf.pdf	
F 217.0 **What preparations have been made against eavesdropping, electromagnetic radiation and similar threats?** *Further details in annex 1.*	1) Sound insulation of the premises must be good enough so that normal speaking voice will not be carried outside from a room where classified matters are being discussed. 2) Personnel shall be reminded that they must not discuss classified matters in rest areas (e.g. canteens, smoking areas). 3) The doors and windows must be kept shut when discussing classified matters.	In addition to the base level requirements: 1) Electric devices whose use is specifically forbidden (laptops, mobile phones, etc.) shall not be used in the room. 2) The need to protect the systems from electromagnetic radiation (TEMPEST) shall be assessed case by case. 3) Sound insulation shall be good enough to guarantee that no sounds are directly carried to surrounding rooms via cable troughs or air-conditioning casings, for example.	In addition to the increased level requirements: 1) Electric devices (laptops, mobile phones, etc.) which are not specifically approved must not be taken to the room. 2) The need to have an inspection by an authority against eavesdropping devices (equivalent) shall be assessed case by case. 3) The need to have a TEMPEST or EMP/HMP protection shall be assessed case by case.	The sound insulation of the premises must be good enough so that normal speaking voice will not be carried outside from a room where sensitive matters are being discussed. Personnel shall be reminded that they must not discuss sensitive matters in rest areas (e.g. smoking areas).	FI NSA guidelines "Handling of international classified information", VAHTI 8/2006, EU Council Security Rules 6952/2/11 REV2 /1.4.2011 article 10, VAHTI 2/2010 annex 5 (TTT), VAHTI 3/2010.	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
F 218.0 **Are heating, water, air conditioning and electrical arrangements guaranteed so that they comply with the functional requirements of the organisation?** *Additional question: is the critical equipment of the organisation covered by uninterrupted power supply (UPS)?* *Further details in annex 1.*	1) The arrangements have been verified according to the operational requirements. 2) Critical equipment is identified and necessary measures have been taken.	1) The arrangements have been verified according to the operational requirements. 2) Critical equipment is identified and necessary measures have been taken.	1) The arrangements have been verified according to the operational requirements. 2) Critical equipment is identified and necessary measures have been taken.	1) The arrangements have been verified according to the operational requirements. 2) Critical equipment is identified and necessary measures have been taken.	ISO/IEC 27002 9.1.4, COBIT 4.1 DS12, VAHTI 8/2006, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines_pdf.pdf	
F 219.0 **Have monitors been installed so that classified information is not revealed to passers-by or other unauthorised persons?**	Monitors have been installed in such a way that information is not revealed to unauthorised persons. Laptops have a display privacy filter.	Monitors have been installed in such a way that information is not revealed to unauthorised persons. Laptops have a display privacy filter.	Monitors have been installed in such a way that information is not revealed to unauthorised persons. Laptops have a display privacy filter.	Monitors have been installed in such a way that sensitive information is not revealed to unauthorised persons.	FI NSA guidelines "Handling of international classified information", VAHTI 8/2006. Note: No privacy filters are required for laptops that are used in equally secure conditions as normal monitors.	

Security technical systems, subdivision F300

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
F 301.0 **Is there an intrusion detection system in the room?**	The room is controlled with an intrusion detection system (the level of the intrusion detection centre shall be at least FK class 2). Doors and facilities shall be controlled if protection level IV material is stored in a normal locked drawer or closet.	The room is controlled with an intrusion detection system (at least class 3). Doors, openings, windows and facilities shall be controlled.	The room is controlled with an intrusion detection system (at least class 3). Doors, openings, windows, facilities, walls, ceiling and floor shall be controlled. A strengthened wall structure is fitted with either structure-borne sound detectors or inertia detectors.	The room is controlled with an intrusion detection system (the level of the intrusion detection centre shall be at least FK class 2). Doors and facilities shall be controlled if protection level IV material is stored in a normal locked drawer or closet.		The intrusion detection system gives an indication and starts countermeasures.
F 302.0 **Is there a physical access control system in the room?**	No requirements.	The room shall have physical access control so that only the persons approved for the project have access to the room, and all access can be verified later.	The room shall have physical access control so that only the persons approved for the project have access to the room, and all access can be verified later for each person. When entering, a double authentication shall be used, and when leaving, a physical access control identifier shall be used.	No recommendations.		Access to the protected room can be verified later. Additional comment for level II: double identification prevents the unauthorised use of an identifier.
F 303.0 **Is there a CCTV surveillance system in the room?**	No requirements.	No requirements as regards CCTV. Can be used for peripheral protection to complement weak garage doors.	A level II room shall be fitted with CCTV. Cameras shall be positioned so that level II information is not conveyed via cameras. The CCTV information shall be stored and attached to the intrusion detection system.	No recommendations.		The CCTV surveillance in the server room prevents own personnel from unauthorised action. For level II: when the alarm of the intrusion detection system goes off, the recording device is triggered and images of the intruder are captured.
F 304.0 **Is there a CCTV surveillance system in the server room?**	No requirements.	No requirements.	Computer rooms and server rooms shall be fitted with permanent CCTV.	No recommendations.		The CCTV surveillance in the server room prevents own personnel from unauthorised action.

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
F 305.0 **Is the intrusion detection system functioning properly?**	No requirements.	The intrusion detection system and alarm transmitter are tested once a month. The response time for guard arrival should posses a significant risk of getting caught and the response time shall be tested once a year. The tests shall be documented.	The intrusion detection system and alarm transmitter are tested once a month. The response time for guard arrival should posses a significant risk of getting caught and the response time shall be tested once a year. The tests shall be documented.	No recommendations.		A non-functioning intrusion detection system does not help. Does the response time in guarding and the guard's action correspond to the contract? Too long a response time or the guard's incorrect action diminishes the security achieved with structural protection.
F 306.0 **How is the management of physical access control arranged?**	No requirements.	No requirements.	The management of physical access control may be outsourced if it is well run. Opening the door from a normal employee´s work station to the protected room shall be prevented.	No recommendations.		The administrator of physical access control may create or remove access identifiers of the protected room and monitor doors via remote control.
F 307.0 **How is the management of intrusion detection system arranged?**	No requirements.	No requirements.	The intrusion detection system shall be managed by the company itself.	No recommendations.		The administrator of the intrusion detection system may create or remove control identifiers of the protected room and detectors via remote control.
F 308.0 **How is the management of heating, plumbing and air-conditioning automation arranged?**	No requirements.	No requirements.	If there are servers or other sensitive equipment in class II protected area, the heating, plumbing and air-conditioning shall not be managed via remote control.	No recommendations.		The equipment and information may be damaged if conditions in the room change because of changes in the heating, plumbing and air-conditioning automation via remote control.

I Information Assurance

Content

Introduction

Information Assurance, one of the subdivisions in the National Security Auditing Criteria, provides the minimum requirements for information whose confidentiality, integrity and usability shall be protected. This type of information includes the sensitive information of companies (business secrets regarding product development, for example) and the protected or classified information of the authorities. The information assurance criteria were created as part of the work on Security Auditing Criteria for the Finnish Internal Security Programme in such a way that a number of requirements essential for information assurance criteria were incorporated to the other respective security areas of the Criteria. The physical security issues, for example, dealing with physical protection of ICT, are located in the physical security subdivision of the Criteria. The work on information assurance criteria has paid as close attention as possible to the detailed guidelines of the Government Decree on Information assurance in Central Government and of its complementing instructions. Similarly, one of the aims has been to create material that is commensurate with the guidelines for information assurance prepared for the use of the European Union.

The information assurance criteria have been divided into four subdivisions as presented in the table of contents. Each subdivision has been further divided into four categories. These include requirements for the base level (IV/RESTRICTED); requirements for the increased level (III/CONFIDENTIAL); and requirements for the high level (II/SECRET); and finally, general recommendations for the industry. Recommendations provide a good basis for fulfilling the requirements. The requirements of levels IV-II concern assets only. An asset here refers to the information to be protected and its handling environment. For example, a single information system, part of a network or even a single office room may be an asset. When proceeding to higher levels the requirements accumulate; for example on level II, in addition to fulfilling the specific requirements there, the requirements of levels IV-III shall be met, unless stated otherwise.

When an organisation deals with information that the authorities have classified, it will have to fulfill the requirement levels given by the authorities. Consequently, as for information assurance, the organisation or a part of it has the ICT capabilities to deal with the information on the condition that the requirements set by the other subdivisions of the Auditing Criteria are met. General international requirements were taken into account when the requirement levels of the information assurance criteria were defined; the Finnish legislation, however, provides ultimate guidelines.

This English translation of the Information Assurance Criteria is based on the second version (2011) of the Finnish National Security Auditing Criteria.

Data Communications Security, subdivision I 400

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 401.0 **Is the architecture of the tele-communications network secure?** *Further details in annex 1.*	1) No connection shall be made to non-trustworthy networks without firewalls. The internet connection in particular shall be separated with a firewall from the information networks and information systems of the organisation. 2) Firewall and VPN configurations comply with the information assurance principles of the organisation and they are documented (see I 403.0) 3) The telecommunication network is divided into zones and segments as necessary. The systems of different information assurance level have been placed in separate network areas (e.g. DMZ separation). 4) The zone division criteria are described. 5) The traffic between the zones is controlled and restricted so that only authorised traffic is allowed. 6) The principles of control and restrictions are described. 7) Work stations, laptops and equivalent use a (host-based) firewall solution also within the organisation's network. 8) The physical network is divided into security zones. In practice it is required that the data is encrypted when it goes beyond the controlled physical space (see I 605.0).	1) The information processing environment is a physically separated network with no connections to networks belonging to a lower level. The Security Authority may, case by case, allow the interconnection through a controlled and limited access point to other networks that are accredited for the equal level. 2) It is possible to transfer data to certain level III systems owned by public authorities through a gateway solution that is approved by Security Authorities (e.g. so called data-diode, allowing the data flow only to one direction). 3) If the tasks for certain working position require connection to internet or to systems or networks of other security levels, it is arranged with a separate computer which is not connected to the increased level (III) network. Security Authority may, from case by case basis, accept also particular gateway solutions between systems representing different security levels.	1) The information processing environment is a physically separated network with no connections to networks belonging to a lower level. The Security Authority may, case by case, allow the interconnection through a controlled and limited access point to other networks that are accredited for the equal level. 2) It is possible to transfer data to certain level II systems owned by public authorities through a gateway solution that is approved by Security Authorities (e.g. so called data-diode, allowing the data flow only to one direction). 3) If the tasks for certain working position require connection to internet or to systems or networks of other security levels, it is arranged with a separate computer which is not connected to the increased level (II) network. Security Authority may, from case by case basis, accept also particular gateway solutions between systems representing different security levels.	1) No connection shall be made to non-trustworthy networks without firewalls. The internet connection in particular shall be separated with a firewall from the information networks and information systems of the organisation. 2) Firewall and VPN configurations comply with the information assurance principles of the organisation and they are documented (see I 403.0)	ISO/IEC 27002 11.4.5, ISO/IEC 27002 11.4.6, ISO/IEC 27002 11.6.1, PCI DSS 1.1.5, PCI DSS 1.4, VAHTI 1/2001, VAHTI 2/2003, VAHTI 8/2006, EU Council Security Rules 6952/2/11 REV2 /1.4.2011 annex IV, VAHTI 3/2010, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines_pdf.pdf	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
		4) Certain systems of public authorities contain a large amount of information classified to certain level. The amount may cause an aggregation of the information mass to the next level. In such cases the Security Authority may, from a case by case basis, accept the access to such system from the system accredited to the lower level (i.e. the level of information of separate documents / files.) As a precaution the access has to be limited only to the part of the information the user has a need-to-know. This is to be controlled by logs, where the unauthorized access can be detected and the user identified.	4) Certain systems of public authorities contain a large amount of information classified to certain level. The amount may cause an aggregation of the information mass to the next level. In such cases the Security Authority may, from a case by case basis, accept the access to such system from the system accredited to the lower level (i.e. the level of information of separate documents / files.) As a precaution the access has to be limited only to the part of the information the user has a need-to-know. This is to be controlled by logs, where the unauthorized access can be detected and the user identified.			

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 402.0 **Does the set of rules for the equipment that filter traffic (firewalls or equivalent) comply with good information assurance principles?** *Additional question:* *Have preparations been made for the most common cyber attacks?* *Further details in annex 1.*	1) As a default the set of rules denies all traffic which is not specifically allowed (default-deny). The set of rules allows only the defined traffic that is essential for the operation. 2) Undefined traffic is denied to both directions. 3) Located in the intranet behind the organisation's firewall, the software firewalls of workstations, laptops and equivalent allow only the traffic of specifically defined software/protocols that are essential for operation. 4) The denied packages are written to the log (ref. I 504.0). When it is technically possible, the sending party has to be identified e.g by MAC-address. 5) Web-browsing is filtered according to the operational demand. 6) The following default configurations are in place to prevent common cyber attacks: a) spoofing is denied b) traffic using IP options or source routing is denied by definition in all network devices c) Proxy ARP functionality is denied in all network devices	Same requirements that are set for the base level, concentrating specially for the aspects within the zone and on its borders (see I 401.0). 1) As a default the set of rules denies all traffic which is not specifically allowed (default-deny). The set of rules allows only the defined traffic that is essential for the operation. 2) Undefined traffic is denied to both directions. 3) Located in the intranet behind the organisation's firewall, the software firewalls of workstations, laptops and equivalent allow only the traffic of specifically defined software/protocols that are essential for operation. 4) The denied packages are written to the log (ref. I 504.0). When it is technically possible, the sending party has to be identified e.g by MAC-address. 5) Web-browsing is filtered according to the operational demand. 6) The following default configurations are in place to prevent common cyber attacks: a) spoofing is denied b) traffic using IP options or source routing is denied by definition in all network devices c) Proxy ARP functionality is denied in all network devices	Same requirements that are set for the base level, concentrating specially for the aspects within the zone and on its borders (ref. 401.0). 1) As a default the set of rules denies all traffic which is not specifically allowed (default-deny). The set of rules allows only the defined traffic that is essential for the operation. 2) Undefined traffic is denied to both directions. 3) Located in the intranet behind the organisation's firewall, the software firewalls of workstations, laptops and equivalent allow only the traffic of specifically defined software/protocols that are essential for operation. 4) The denied packages are written to the log (ref. I 504.0). When it is technically possible, the sending party has to be identified e.g by MAC-address. 5) Web-browsing is filtered according to the operational demand. 6) The following default configurations are in place to prevent common cyber attacks: a) spoofing is denied b) traffic using IP options or source routing is denied by definition in all network devices c) Proxy ARP functionality is denied in all network devices	1) As a default the set of rules denies all traffic which is not specifically allowed (default-deny). 2) Undefined traffic is denied to both directions.	Applying VAHTI 2/2003, VAHTI 8/2006, PCI DSS 1.1.5, http://www.cymru.com/Documents/bogon-list.html, RFC 2827, RFC 3704, VAHTI 3/2010, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/ guidelines/guidelines_pdf.pdf, http://www.sans.org/critical-security-controls/control.php?id=5	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
	d) the traffic whose source address or target address is a broadcast address on the LAN is denied e) the traffic with 127.0.0.1 or 0.0.0.0 as a source or target address is denied f) SNMP traffic is allowed only from specifically defined sources g) permitted ICMP traffic is defined. Special attention has to be payed to deny the traffic of ICMP-type 3 (unreachable). h) the traffic which uses reserved addresses (RFC 1918) and either enters from the outside of the network or is directed there is denied i) firewalls are configured to compile fragmented packages before the filtering decision is made j) threat of DoS and DDoS is evaluated and necessary control and prevention measures are implemented.	d) the traffic whose source address or target address is a broadcast address on the LAN is denied e) the traffic with 127.0.0.1 or 0.0.0.0 as a source or target address is denied f) SNMP traffic is allowed only from specifically defined sources g) permitted ICMP traffic is defined. Special attention has to be payed to deny the traffic of ICMP-type 3 (unreachable). h) the traffic which uses reserved addresses (RFC 1918) and either enters from the outside of the network or is directed there is denied i) firewalls are configured to compile fragmented packages before the filtering decision is made j) threat of DoS and DDoS is evaluated and necessary control and prevention measures are implemented.	d) the traffic whose source address or target address is a broadcast address on the LAN is denied e) the traffic with 127.0.0.1 or 0.0.0.0 as a source or target address is denied f) SNMP traffic is allowed only from specifically defined sources g) permitted ICMP traffic is defined. Special attention has to be payed to deny the traffic of ICMP-type 3 (unreachable). h) the traffic which uses reserved addresses (RFC 1918) and either enters from the outside of the network or is directed there is denied i) firewalls are configured to compile fragmented packages before the filtering decision is made j) threat of DoS and DDoS is evaluated and necessary control and prevention measures are implemented.			
I 403.0 **How is it guaranteed that the systems filtering or controlling the traffic function in the desired way?**	1) The responsibilities and organisation for adding, changing or removing rules from/to the set of rules for firewalls and other filtering devices are defined. 2) Filtering rules are documented (see I 401.0). 3) The set of rules for and the desired operation of the systems that filter or control firewalls, IDS systems and other systems are guaranteed with checks.	In addition to the requirements set for the base level: The set of rules for and the desired operation of the systems that filter or control firewalls, IDS systems and other systems are guaranteed with regular checks.	In addition to the requirements set for the base level: The set of rules for and the desired operation of the systems that filter or control firewalls, IDS systems and other systems are guaranteed with regular checks.	1) The responsibilities and organisation for adding, changing or removing rules from/to the set of rules for firewalls and other filtering devices are defined. 2) Filtering rules are documented (see I 401.0).	PCI DSS 1.1.6, VAHTI 2/2010:n liite 5 (TTT)	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 404.0 **Have the management connections been adequately protected?** *Further details in annex 1.*	1) The management traffic of the networks and information systems (incl. servers, workstations, network devices and equivalent) is separated and/or encrypted. 2) Connections to the active devices of the network are allowed only from separately defined sources or by connecting physically to the device.	1) The management traffic of the networks and information systems (incl. servers, workstations, network devices and equivalent) is separated and/or encrypted. 2) Connections to the active devices of the network are allowed only from separately defined sources or by connecting physically to the device.	1) The management traffic of the networks and information systems (incl. servers, workstations, network devices and equivalent) is separated and/or encrypted. 2) Connections to the active devices of the network are allowed only from separately defined sources or by connecting physically to the device.	The management traffic of the networks and information systems (incl. servers, workstations, network devices and equivalent) is separated and/or encrypted.	ISO/IEC 27002 11.1, PCI DSS 2.3, VAHTI 8/2006	
I 405.0 **How have the active devices been configurated with the organisation's own parametres instead of default parameters?** *Further details in annex 1.*	Active network devices are configurated in line with the common procedure of the organisation. At least the following are in practice required: 1) default passwords have been changed 2) only necessary network services are on 3) necessary security updates have been installed in the software of the network devices. 4) the management is not possible without user identification and verification 5) devices have been configured following the advice given by the manufactures and trusted actors 6) workstation ports on switches have been separated and the workstations can not directly communicate with each others. The switches may not echo the traffic (HUB functionality). 7) if VTP domain (VLAN Trunking Protocol domain) is in use, the VTP password has been assigned and activated. 8) switches do not use the default VLAN (typically VLAN 1) for the operational traffic.	In addition to the requirements of the base level the following requirements apply: 1) management operations, including the time and personal identification of the manager can be verified from the logs of network devices. 2) Unused ports in switches are deactivated.	In addition to the requirements of the base level the following requirements apply: 1) management operations, including the time and personal identification of the manager can be verified from the logs of network devices. 2) Unused ports in switches are deactivated.	Active network devices are configurated in line with the common procedure of the organisation. At least the following are in practice recommended: 1) default passwords have been changed 2) only necessary network services are on 3) necessary security updates have been installed in the software of the network devices.	ISO/IEC 27002 11.1, ISO/IEC 11.2.3, PCI DSS 2.1, PCI DSS 2.2, PCI DSS 6.1, PCI DSS 6.2, VAHTI 2/2003, VAHTI 8/2006, ISO/IEC 11.2.3, VAHTI 3/2010, http://www.sans.org/critical-security-controls/control.php?id=4	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 406.0 **How are the wireless networks protected?** *Note: For the levels III and II: it is usually easier to reach the required security level by using physical (cable) networks.*	1) for visitor networks, through which there is no connection to the intranet, encryption and user identification are recommended but not required. 2) The use of the wireless networks that are managed by the organisation is allowed only to identified and authorised users. 3) The traffic is encrypted reliably.	In principal, the wireless networks are forbidden. From the case by case basis such a solution may be approved, where the traffic has been point-to-point (not just the radio frequency path) encrypted with the crypto approved to this level. In this case the wireless network has the similar status as a public network.	Wireless networks are not used. From the case by case basis such a solution may be approved, where the traffic has been point-to-point (not just the radio frequency path) encrypted with the crypto approved to this level. In this case the wireless network has the similar status as a public network.	For visitor networks, through which there is no connection to the intranet, encryption and user identification, are recommended.	ISF-SOGP NW2.4, VAHTI 3/2010, http://www.sans.org/critical-security-controls/control.php?id=14	
I 407.0 **Has the visibility of internal network infrastructure on the internet or on other untrustworthy networks been prevented?** *Additional question:* *Has the unnecessary visibility of the internal network structure and traffic been prevented within the network?*	1) internal network utilises so called private addresses which are not part of the public network 2) unnecessary visibility of the internal network structure and traffic is prevented within the network (see I 402.0 and I 405.0).	1) internal network utilises so called private addresses which are not part of the public network 2) unnecessary visibility of the internal network structure and traffic is prevented within the network (see I 402.0 and I 405.0).	1) internal network utilises so called private addresses which are not part of the public network 2) unnecessary visibility of the internal network structure and traffic is prevented within the network (see I 402.0 and I 405.0).	Internal network utilises so called private addresses which are not part of the public network.	PCI DSS 1.3.8, ISO/IEC 27002 12.5.4	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 408.0 **How are the network, systems and their use monitored?** *Additional question: do the resources meet the operational requirements?* *Note: the requirements for increasing traffic volumes are defined case by case according to the usability requirements.*	1) The baseline of the network traffic is known. At least the normal amount of traffic and the protocols used in different parts of the network shall be known. 2) Resources have been built to meet the requirement for the critical communication systems to function in a secure way also when the volume of the traffic increases from the normal, according to the level set at the risk assessment.	In addition to the base level: A procedure shall be in place to detect, deal with and prevent a cyber attack/attempt to misuse (see A 410.0 and I 504.0). The network traffic is monitored closely enough to detect a) significant deviation in the amount of traffic in the work stations and servers, b) protocols that differ from the baseline, and c) attempts at unauthorised connections (e.g. in the gateway between zones).	In addition to the base level:: A procedure shall be in place to detect, deal with and prevent a cyber attack/attempt to misuse (see A 410.0 and I 504.0). The network traffic is monitored closely enough to detect a) significant deviation in the amount of traffic in the work stations and servers, b) protocols that differ from the baseline, and c) attempts at unauthorised connections (e.g. in the gateway between zones).	Network, systems and their use are monitored according to the operational requirements and the risk assessment. Resources have been built to meet the operational requirements and the requirements set at the risk assessment.	ISO/IEC 27002 10.6.1, ISO/IEC 27002 10.10.2, ISO/IEC 27002 10.3.1, PCI DSS 11.4, COBIT 4.1 DS3, COBIT 4.1 ME1, VAHTI 8/2006, VAHTI 3/2009, VAHTI 3/2010, VAHTI 2/2010 annex 5 (TTT)	
I 409.0 **How are the IPv6 specific security requirements been taken into account in networks and systems?** *Additional question: Have the problematic features for the organisation been noticed and have the necessary countermeasures been taken into use?* *Additional information in annex 1.*	1) IPv6 functionality has been adequately noticed in the general planning of the system/network or it has been deactivated in such systems (workstations, servers, network components etc), where true need to use it cannot be shown. 2) IPv6 Privacy Extensions (RFC 4941) is denied in the network of the organisation, unless a true need can be identified.	1) IPv6 functionality has been adequately noticed in the general planning of the system/network or it has been deactivated in such systems (workstations, servers, network components etc), where true need to use it cannot be shown. 2) IPv6 Privacy Extensions (RFC 4941) is denied in the network of the organisation, unless a true need can be identified.	1) IPv6 functionality has been adequately noticed in the general planning of the system/network or it has been deactivated in such systems (workstations, servers, network components etc), where true need to use it cannot be shown. 2) IPv6 Privacy Extensions (RFC 4941) is denied in the network of the organisation, unless a true need can be identified.	Special features of IPv6 are identified according to the risk assessment.	http://www.nsa.gov/ia/guidance/security_configuration_guides/IPv6.shtml	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 410.0 **How has the security of routing been taken care of?**	1) Routing messages are verified. 2) The verification is in use on the zones towards every neighbour. 3) Necessary and sufficient filters to transfer information are defined in routing.	1) Routing messages are verified. 2) The verification is in use on the zones towards every neighbour. 3) Necessary and sufficient filters to transfer information are defined in routing.	1) Routing messages are verified. 2) The verification is in use on the zones towards every neighbour. 3) Necessary and sufficient filters to transfer information are defined in routing.	Security of routing is noticed following the risk assessment.	VAHTI 3/2010	

Security of Information Systems, subdivision I 500

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 501.0 **Are the users identified and authenticated before access is granted to the information network and information systems of the organisation?** *Additional question:* *How has this been done in practice?*	Users are identified and authenticated before access is granted to the information network and information systems of the organization: 1) Individual and personal user IDs are used 2) All users are identified and authenticated 3) Access to the operating system is controlled by means of a secure login 4) Identification and authentication is done by using well known and secure techniques or it is otherwise taken care on a secure manner. 5) Authentication is done at least by using a password. If the password authentication is used, a) users are introduced to good practices in choosing and using the password b) software observing the use sets certain minimum standards for the password as well as forces the user to change the password regularly 6) When identification for fails after too many attempts in a row the identification process is interlocked. 7) The maintenance identifiers of systems and software are personal. If this is not technically possible in all systems/software, agreed and documented password management procedures are required for identifiers in joint use.	In addition to the base level requirements 1-4, 6, 7: If the same information system is used to manage more than one project of a specific security level a strong user authentication is used to identify the user.	In addition to the base level requirements 1-4, 6 and 7 a strong user authentication is always used to identify the user. See the targeted requirements in annex 1 (I 502.0 / IV & III)	Users are identified and authenticated before access is granted to the information network and information systems of the organisation.	ISO/IEC 27002 11.3.1, ISO/IEC 27002 11.4, ISO/IEC 27002 11.5.1, ISO/IEC 27002 11.5.2, PCI DSS 8.1, PCI DSS 8.5, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines_pdf.pdf, VAHTI 8/2006, VAHTI 2/2010 annex 5 (TTT), VAHTI 3/2010	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 502.0 **Is there a procedure in place in the organisation to systematically install new systems (workstations, portable computers, servers, peripherals, network printers and equivalent) so that the end result is a configuration with the own parameters of the organisation?** *Further details in annex 1.*	There is a procedure in place to install new systems (workstations, laptops, servers, network devices etc.) so that the end result is a configuration with the own parameters of the organisation? See annex 1 (I 502.0 / IV).	There is a procedure in place to install new systems (workstations, laptops, servers, network devices etc.) so that the end result is a configuration with the own parameters of the organisation? See annex 1 (I 502.0 / III).	In addition to the requirements for the increased level: There is a mechanism, method or procedure in place to save all changes made for the system in a format which allows tracing them. See I 504.0. See also annex 1 (I 502.0 / II).	There is a procedure in place to install new systems (workstations, laptops, servers, network devices etc.) so that the end result is a configuration with the own parameters of the organisation?	PCI DSS 2.1, PCI DSS 2.2, ISO/IEC 11.2.3, VAHTI 8/2006, VAHTI 2/2010 annex 5 (TTT), VAHTI 3/2010 Sources for secure configuration of systems/devices: http://www.nsa.gov/ia/guidance/security_configuration_guides/, http://nvd.nist.gov/fdcc/index.cfm, http://web.nvd.nist.gov/view/ncp/repository, http://usgcb.nist.gov/, http://www.ia.nato.int/ > IA Guidance > Best Practices > Security Checklist, http://iase.disa.mil/stigs/stig/index.html, http://iase.disa.mil/stigs/checklist/index.html, http://technet.microsoft.com/en-us/library/cc163140.aspx, http://technet.microsoft.com/en-us/library/cc757698.aspx, http://httpd.apache.org/docs/1.3/misc/security_tips.html, http://csrc.nist.gov/publications/PubsSPs.html, http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml, http://www.hp.com/rnd/pdfs/Hardening_ProCurve_Switches_White_Paper.pdf, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines_pdf.pdf http://kb2.adobe.com/cps/837/cpsid_83709/attachments/ Acrobat_Enterprise_Administration.pdf, http://www.sans.org/critical-security-controls/control.php?id=3, http://www.sans.org/critical-security-controls/control.php?id=4	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 503.0 **What is done to reduce the risks caused by malware?** *Further details in annex 1.*	1) Malware prevention software (anti-malware) has been installed to all such systems that are generally vulnerable to malware infections (especially workstations, laptops and servers). 2) Anti-malware is running and able to act. 3) Anti-malware produces logs of its functions. 4) Malware fingerprints 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. (see A 806.0). 6) Malware detection is monitored. (see A 408.0).	In addition to the base level requirements: On a case by case basis an evaluation is done to define whether the USB-ports or other interfaces are needed. If no true reason can be found, the interfaces are removed from use. In case the need exists, a case by case estimation is done to define the prerequisite and conditions for what kind of devices (like USB-sticks) can be connected to the system.	In addition to the base level requirements: On a case by case basis an evaluation is done to define whether the USB-ports or other interfaces are needed. If no true reason can be found, the interfaces are removed from use. In case the need exists, a case by case estimation is done to define the prerequisite and conditions for what kind of devices (like USB-sticks) can be connected to the system.	Malware detection, prevention and recovery procedures are in place, as well as instructions that keep users adequately in an alert mode.	ISO/IEC 27002 10.4.1, PCI DSS 5.1, PCI DSS 5.2, http://www.sans.org/critical-security-controls/control.php?id=12, VAHTI 2/2010 annex 5 (TTT), VAHTI 3/2010, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines_pdf.pdf	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 504.0 **Are the log procedures of technical devices and services of the organisation implemented?** *Additional question:* *Is the key log data compiled from the networks, equipment and systems and is it appropriately dealt with?* *Further details in annex 1.*	1) Logs cover the detection of security breaches or attempts to such. 2) Crucial recordings are stored 6 months or as long as the separate contract defines. 3) Log files containing classified information are protected accordingly (access control, handling, deleting).	In addition to the base level requirements 1 and 3: 1) Crucial recordings are stored 24 months or as long as the separate contract defines 2) Procedure to detect, handle and prevent attacks or misuse is in place. The procedure includes a log monitoring program to be ran at least once a week in order to detect abnormal activities. Especially the unauthorised use of an information system has to be detected (see I 408.0 and A 410.0). 3) Information systems of the same organisation or same zone bear the same time, synchronised with a trusted time source. 4) Log files and their registering services have been protected against fraud and unauthorised access. There is a procedure in place to ensure the integrity of the logs. 5) Backups of crucial log information are made regularly. 6) Handling and usage of the log files are registered. 7) Critical maintenance operations are recorded (audit trail).	In addition to the increased level requirements 1) The integrity of the information system is confirmed at least once a week (see I 502.0). 2) log files of the handling of level II information are stored (see I 607.0).	1) Logs cover the detection of security breaches or attempts to such. 2) Crucial recordings are stored as long as the risk assessment defines.	ISO/IEC 27002 10.6.1, ISO/IEC 27002 10.10.1, ISO/IEC 27002 10.10.2, ISO/IEC 27002 10.10.3, ISO/IEC 27002 10.10.6, PCI DSS 10.1, PCI DSS 10.2, PCI DSS 10.3, PCI DSS 10.4, PCI DSS 10.5, VAHTI 8/2006, VAHTI 3/2009, VAd.HTI 2/2010 annex 5 (TTT), VAHTI 3/2010 http://www.sans.org/critical-security-controls/control.php?id=6, http://technet.microsoft.com/en-us/library/bb742610.aspx, http://technet.microsoft.com/en-us/library/dd408940%28WS.10%29.aspx, http://www.team-cymru.org/ReadingRoom/Templates/secure-ntp-template.html	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 505.0 **How is classified information stored in information systems?** *Further details in annex 1.*	1) In information systems the classified information is separated through user right definitions and handling requirements for the system, or through some other, equivalent manner. 2) Temporary files are deleted regularly (see I 603.0). 3) hard disks of the computers handling level IV information are protected in a sufficient way (see I 506).	In addition to the base level requirements 1 and 2: 1) In servers, workstations, laptops and in other devices with memory functions the information belonging to level III is always stored in a reliably encrypted form (see I 509.0). 2)In case the server acts as a storage device for projects of multiple security levels, the information stored to server are in encrypted form and placed in folders/area with controlled access. 3) Level III information is kept separate from public information or from information belonging to other security levels.	1) In servers, workstations, laptops and in other memory units the information belonging to level II are always stored in an reliably encrypted form (see I 509.0). 3) Level II information is kept separate from public information or from information belonging to other security levels.	In information systems the classified information is separated through user right definitions and handling requirements for the system, or through some other, equivalent manner.	VAHTI 8/2006, VAHTI 2/2010, VAHTI 3/2010 http://www.nsa.gov/ia/guidance/security_configuration_guides/ database_servers.shtml, http://www.oracle.com/technetwork/articles/idm/tde-089026.html, http://www.oracle.com/technetwork/database/security/twp-transparent-data-encryption-bes-130696.pdf, http://www.ibm.com/developerworks/data/library/techarticle/dm-0907encryptionexpert/, http://publib.boulder.ibm.com/epubs/pdf/eetuga13.pdf, http://technet.microsoft.com/en-us/library/cc278098%28SQL.100%29.aspx, http://technet.microsoft.com/en-us/library/cc875821.aspx, http://support.microsoft.com/kb/223316, http://publib.boulder.ibm.com/infocenter/lnxinfo/v3r0m0/topic/liaai/secure/ liaaisecuresles.htm, http://www.linuxtopia.org/online_books/suse_linux_guides/SLES10/ suse_enterprise_linux_server_installation_admin/cha_cryptofs.html, http://www.postgresql.org/docs/manuals/, http://www.sans.org/critical-security-controls/control.php?id=15	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 506.0 **How is it ensured that movable hard disks, memories, media, smart phones, mobile terminals and equivalent devices that contain classified information are always protected against unauthorised access?** *Further details in annex 1.*	1) Laptops and their hard disks, USB-sticks and other mass storage media containing classified information are protected in a trustworthy way. 2) Smartphones containing classified information: a) access to the information stored to the phone or to the memory card is protected with password b) automatic locking of the phone or the SIM-card is in use c) remote erasing possibility is in use d) data in the phone and in the memory card is protected e) network and malware threats are notified according to the risk assessment f) Bluetooth-and WLAN-connections are by definition switched off and are activated only for the time they are in use. In Bluetooth-settings the phone visibility is set to ”hide/non-visible” by definition.	In addition to the base level requirement 1: Information classified to level III (CONFIDENTIAL) is not handled with smartphones by definition. Security Authorities can, however, approve certain solutions, where the smartphone and all the traffic through it is protected in a trustworthy way.	In addition to the base level requirement 1: Information classified to level II (SECRET) is not handled with smartphones by definition. Security Authorities can, however, approve certain solutions, where the smartphone and all the traffic through it is protected in a trustworthy way.	Laptops and their hard disks, USB-sticks and other mass storage media containing classified information are sufficiently protected. Smartphones containing classified information are protected according to the risk assessment (locking, encryption, remote controls, etc.).	ISO/IEC 27002 10.8.3, ISO/IEC 27002 9.2.5, VAHTI 8/2006, VAHTI 2/2010, VAHTI 3/2010, EU Council Security Rules 6952/2/11 REV2 /1.4.2011 article 9, http://www.sans.org/score/handheldschecklist.php	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 507.0 **How is it ensured that third parties do not access classified information in connection with maintenance measures or deactivation?** *Further details in annex 1.*	1) All parts of devices containing classified information (hard disks, mass storage media, memory cards etc.) are erased in a trustworthy way when the device is removed from service or sent away for reparation (see I 603.0). If the trustworthy erasure is not possible, the part containing classified information is destroyed mechanically. 2) Service functions carried out by third parties are monitored in cases where the memory of the device cannot be reliably erased for the service (e.g. multifunction copy machines).	1) All parts of devices containing classified information (hard disks, mass storage media, memory cards etc.) are erased in a trustworthy way when the device is removed from service or sent away for reparation (see I 603.0). If the trustworthy erasure is not possible, the part containing classified information is destroyed mechanically. 2) Service functions carried out by third parties are monitored in cases where the memory of the device cannot be reliably erased for the service (e.g. multifunction copy machines).	1) All parts of devices containing classified information (hard disks, mass storage media, memory cards etc.) are erased in a trustworthy way when the device is removed from service or sent away for reparation (see I 603.0).. If the trustworthy erasure is not possible, the part containing classified information is destroyed mechanically. 2) Service functions carried out by third parties are monitored in cases where the memory of the device cannot be reliably erased for the service (e.g. multifunction copy machines).	1) All parts of devices containing classified information (hard disks, mass storage media, memory cards etc.) are erased in a trustworthy way when the device is removed from service or sent away for reparation (see I 603.0). If the trustworthy erasure is not possible, the part containing classified information is destroyed mechanically. 2) Service functions carried out by third parties are monitored in cases where the memory of the device cannot be reliably erased for the service (e.g. multifunction copy machines).	ISO/IEC 27002 9.2, ISO/IEC 27002 9.2.6, VAHTI 8/2006, VAHTI 2/2010	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 508.0 **How is it ensured that there are no unauthorised devices or systems in the organisation's network?** *Additional questions:* *How is it known what (IT system related) equipment is used in the organisation? How is the information managed on the software used and their versions and licenses? Will it be detected if a piece of equipment is removed, unauthorized, from the premises of the organisation? Will it be detected if unauthorized software is installed in the systems?* *Are all the premises checked, on a permanent basis, from which it is possible to access the network of the organisation, to detect unauthorised equipment and software?*	1) Devices are listed on a register, including the ones taken out of service or destroyed. 2) Software is listed on a register with details of programmes in use and their licenses. 3) Server rooms, switching closets and similar spaces are regularly checked, based on a verifiable plan in order to locate unauthorised devices (packet capturers, key-loggers, wireless base stations etc.).	In addition to the base level requirements: 1) All spaces, where access to closed network is possible are checked based on a verifiable plan in order to locate unauthorised devices. 2) Network plugs or other similar connectors, which are not in use, are physically disconnected. 3) Connections of unknown devices are prevented using the techniques provided by the network technology.	In addition to the increased level requirements: 1) Cabling of the electric current and the IT network cabling that transfers data or supports IT services are protected against eavesdropping and damages. 2) Devices are protected against connecting unauthorised components (key-loggers etc.). If sealing is used, the seals are always checked before taking the device into use.	1) Devices are listed on a register, including the ones taken out of service or destroyed. 2) Software is listed on a register with details of programmes in use and their licenses.	ISO/IEC 27002 9.2.1, ISO/IEC 27002 9.2.3, ISO/IEC 27002 11.4.1, ISO/IEC 27002 15.1.2, VAHTI 8/2006, VAHTI 2/2010 annex 5 (TTT), VAHTI 3/2010, http://www.sans.org/critical-security-controls/control.php?id=1, http://www.sans.org/critical-security-controls/control.php?id=2, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines_pdf.pdf	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 509.0 **How is it guaranteed that encryption solutions are secure enough?** *Further details in annex 1.*	Crypto solutions and products are approved to fulfil the requirements set for the classification level by a) international Security Authority, b) National Security Authority (e.g. NCSA), or c) a separate auditing carried out for the solution.	Crypto solutions and products are approved to fulfil the requirements set for the classification level by a) international Security Authority, b) National Security Authority (e.g. NCSA), or c) a separate auditing carried out for the solution.	Crypto solutions and products are approved to fulfil the requirements set for the classification level by a) international Security Authority, b) National Security Authority (e.g. NCSA), or c) a separate auditing carried out for the solution.	Well known and generally trustworthy crypto solutions are used or the level of the solution in use is verified by some other means.	EU Council Security Rules 6952/2/11 REV2 /1.4.2011 article 10, http://www.consilium.europa.eu/information-assurance, http://www.ia.nato.int/niapc, List of approved crypto products maintained by the national Crypto Approval Authority, FI NSA guidelines "Handling of international classified information".	
I 510.0 **Management of encryption keys** **Are the secret keys only used by authorised users and processes?** *Additional question:* *Are the processes and procedures of the encryption key management documented and appropriately implemented?* *Further details in annex 1.*	1) Secret keys are only in use for authorised users and processes. 2) Processes and procedures for key management are documented and appropriately implemented. Processes require a) cryptographically strong keys, b) secure key delivery system, c) secure key storage, d) regular key changes, e) change of old or exposed keys, f) prevention of unauthorised key changes.	1) Secret keys are only in use for authorised users and processes. 2) Processes and procedures for key management are documented and appropriately implemented. Processes require a) cryptographically strong keys, b) secure key delivery system, c) secure key storage, d) regular key changes, e) change of old or exposed keys, f) prevention of unauthorised key changes.	1) Secret keys are only in use for authorised users and processes. 2) Processes and procedures for key management are documented and appropriately implemented. Processes require a) cryptographically strong keys, b) secure key delivery system, c) secure key storage, d) regular key changes, e) change of old or exposed keys, f) prevention of unauthorised key changes.	Secret keys are only in use for authorised users and processes.	ISO/IEC 27002 12.3.2, PCI DSS 3.6, VAHTI 8/2006, VAHTI 2/2010	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 511.0 **In session management, is a known and trustworthy technique used?**	In session management a known and trustworthy technique is used or the hijacking or cloning of the session has been made difficult through countermeasures. If no known technique is used, at least following aspects are paid attention to: 1) prevention of re-activation of closed sessions, 2) separation of session keys from the keys used to transfer them, 3) termination of the session if no user activities detected for certain period, 4) time limits for sessions.	In session management a known and trustworthy technique is used or the hijacking or cloning of the session has been made difficult through countermeasures. If no known technique is used, at least following aspects are paid attention to: 1) prevention of re-activation of closed sessions, 2) separation of session keys from the keys used to transfer them, 3) termination of the session if no user activities detected for certain period, 4) time limits for sessions.	In session management a known and trustworthy technique is used or the hijacking or cloning of the session has been made difficult through countermeasures. If no known technique is used, at least following aspects are paid attention to: 1) prevention of re-activation of closed sessions, 2) separation of session keys from the keys used to transfer them, 3) termination of the session if no user activities detected for certain period, 4) time limits for sessions.	In session management a known and trustworthy technique is used or the hijacking or cloning of the session has been made difficult through countermeasures. If no known technique is used, at least following aspects are paid attention to: 1) prevention of re-activation of closed sessions, 2) separation of session keys from the keys used to transfer them, 3) termination of the session if no user activities detected for certain period, 4) time limits for sessions.	ISO/IEC 27002 11.5, VAHTI 3/2001	
I 512.0 **Has it been ensured that authentication data is not stored in the information systems as clear text?**	Authentication data (like passwords, fingerprints etc.) is not stored in the information systems in clear text format. In information systems only hash data, derived from the authentication data by one-way hash function or by similar trustworthy method, may be stored.	Authentication data (like passwords, fingerprints etc.) is not stored in the information systems in clear text format. In information systems only hash data, derived from the authentication data by one-way hash function or by similar trustworthy method, may be stored.	Authentication data (like passwords, fingerprints etc.) is not stored in the information systems in clear text format. In information systems only hash data, derived from the authentication data by one-way hash function or by similar trustworthy method, may be stored.	Authentication data (like passwords, fingerprints etc.) is not stored in the information systems in clear text format. In information systems only hash data, derived from the authentication data by one-way hash function or by similar trustworthy method, may be stored.	PCI DSS 3.2, PCI DSS 8.4, ISO/IEC 27002 11.5.3	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 513.0 **How is the security of the runnable code ensured?**	Software is purchased and installed only from trusted and authorised sources.	In addition to the base level requirements: 1) Integrity of the software or updates to be installed is verified (checksums, anti-malware) 2) Applications that are purchased or implemented fulfil the principles of secure programming, e.g. Open Web Application Security Project Guide. Suppliers are asked to verify how information assurance as such has been taken into account in product development.	In addition to the base level requirements: Two possibilities: 1) Only systems and software approved by Security Authorities to the actual system environment are used. 2) Applications that are purchased or implemented fulfil the principles of secure programming, e.g. Open Web Application Security Project Guide. Suppliers are asked to verify how information assurance as such has been taken into account in product development. In addition all code that has elementary effect to the security of the system can be openly checked (e.g. back doors, insecure implementations etc.) or the contract includes the right to verify the source code. In alternative 2) a proof has to be given of the security verification of the code (e.g. description of suppliers' processes and an audit report given by a neutral party).	Software is purchased and installed only from trusted and authorised sources.	ISO/IEC 27002 12.2.1, ISO/IEC 27002 12.4.1, ISO/IEC 27002 15.1.2, PCI DSS 6.5, VAHTI 8/2006, http://www.bsi-mm.com/, http://www.opensamm.org/, http://www.owasp.org/index.php/Category:OWASP_Guide_Project, http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project, http://www.cpni.gov.uk/Docs/Vendor_security_questions.pdf, http://www.sans.org/critical-security-controls/control.php?id=7	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 514.0 **How is it ensured that the hardware purchased for the organisation follow the information assurance principles and can be seen secure enough for the purpose?**	Information assurance principles are taken into account when purchasing hardware. At least the following is to be taken into account: 1) does the device allow a secure enough access control (e.g. phone, printer, network device, laptop) 2) are the documents stored in the memory of the device (e.g. printers, copy machines) 3) can the memory component of the device be encrypted (e.g. printer, laptop, phone), 4) how good is the assistance offered by the manufacturer (security updates, licence and guarantee terms, etc.) 5) are there additional security features in the device 6) can the device be self-modified to make it more secure	Information assurance principles are taken into account when purchasing hardware. At least the following is to be taken into account: 1) does the device allow a secure enough access control (e.g. phone, printer, network device, laptop) 2) are the documents stored in the memory of the device (e.g. printers, copy machines) 3) can the memory component of the device be encrypted (e.g. printer, laptop, phone), 4) how good is the assistance offered by the manufacturer (security updates, licence and guarantee terms, etc.) 5) are there additional security features in the device 6) can the device be self-modified to make it more secure	Information assurance principles are taken into account when purchasing hardware. At least the following is to be taken into account: 1) does the device allow a secure enough access control (e.g. phone, printer, network device, laptop) 2) are the documents stored in the memory of the device (e.g. printers, copy machines) 3) can the memory component of the device be encrypted (e.g. printer, laptop, phone), 4) how good is the assistance offered by the manufacturer (security updates, licence and guarantee terms, etc.) 5) are there additional security features in the device 6) can the device be self-modified to make it more secure	Information assurance principles are taken into account when purchasing hardware. At least the following is to be taken into account: 1) does the device allow a secure enough access control (e.g. phone, printer, network device, laptop) 2) are the documents stored in the memory of the device (e.g. printers, copy machines) 3) can the memory component of the device be encrypted (e.g. printer, laptop, phone), 4) how good is the assistance offered by the manufacturer (security updates, licence and guarantee terms, etc.) 5) are there additional security features in the device 6) can the device be self-modified to make it more secure	ISO 27002 12.1.1, VAHTI 8/2006, VAHTI 2/2010 annex 5 (TTT)	

Security of Information, subdivision I 600

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 601.0 **What kind of a information classification system does the organisation employ?** *Note: see handling requirements in I 505.0, I 602.0, I 506.0, I 603.0, I 604.0, I 605.0, I 606.0, I 607.0.*	1) Information is classified according to their significance and/or due to the legal requirements. Documents (e.g. drafts) that need safeguarding (e.g. classified) are marked with a marking which describes the level of safeguarding. 2) Documents are marked with the marking equivalent to the highest part of the document (incl. annexes). 3) In case the main text and the annexes are classified to a different level, this is stated in the document.	1) Information is classified according to their significance and/ or due to the legal requirements. Documents (e.g. drafts) that need safeguarding (e.g. classified) are marked with a marking which describes the level of safeguarding. 2) Documents are marked with the marking equivalent to the highest part of the document (incl. annexes). 3) In case the main text and the annexes are classified to a different level, this is stated in the document.	1) Information is classified according to their significance and/ or due to the legal requirements. Documents (e.g. drafts) that need safeguarding (e.g. classified) are marked with a marking which describes the level of safeguarding. 2) Documents are marked with the marking equivalent to the highest part of the document (incl. annexes). 3) In case the main text and the annexes are classified to a different level, this is stated in the document.	1) Information is classified according to their significance and/or due to the legal requirements. Documents (e.g. drafts) that need safeguarding (e.g. classified) are marked with a marking which describes the level of safeguarding. 2) Documents are marked with the marking equivalent to the highest part of the document (incl. annexes). 3) In case the main text and the annexes are classified to a different level, this is stated in the document.	ISO/IEC 27002 7.2.1, VAHTI 2/2010, COBIT 4.1 PO2.3, FI NSA guidelines "Handling of international classified information", EU Council Security Rules 6952/2/11 REV2 /1.4.2011 article 2, http://www.finlex.fi/fi/laki/ajantasa/1999/19990621	
I 602.0 **Has it been ensured that the data and storage media containing classified information are securely stored?** *Further information in annex 1.*	1) Classified information is stored in closets with locks or in safes. 2) When leaving the room the non-encrypted classified material (papers, mass media etc.) are put into a safe, into a closet with a lock or to some other similar storage space. 3) When leaving the room the work space is checked and the room is locked to prevent unauthorised access.	When leaving the room the material (papers, mass media etc.) classified to level III (CONFIDENTIAL) are put into a safe, minimum level of which is EURO class II (EN 1143-1) or to some other secure storage space (e.g. vault with IDS and certified to EURO IV).	When leaving the room the material (papers, mass media etc.) classified to level II (SECRET) are put into a safe, minimum level of which is EURO class II (EN 1143-1) or to some other secure storage space (e.g. vault with IDS and certified to EURO IV).	Sensitive material is stored in closets with locks or in safes.	VAHTI 8/2006, VAHTI 2/2010, EU Council Security Rules 6952/2/11 REV2 /1.4.2011 annex II	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 603.0 **Is the data containing classified information securely destroyed?** *Further information in annex 1.*	1) Classified electronic material is destroyed securely (writing over or destructing physically the storage media). 2) Temporary files resulting from the normal use of the IT-systems are deleted regularly. See I 505.0. 3) Classified material that is not in the electronic format is destroyed securely. Organisation has a paper shredder able to shred the paper to the maximum size of 2mm x 15mm (DIN 32757/ DIN 4) or some other approved method to destroy the material classified to level IV (like burning).	In addition to the base level requirements: new projects (e.g. software development) are always started with a "clean" hardware, without any remain from the previous projects. 2) Separate mass storage media is in use for all clients (e.g. own hard disks for each project. Security Authorities may, on a case by case basis, accept the solution where different projects are handled on separate logical memory partitions (e.g. virtualising). 3) Organisation has a paper shredder able to shred the level III paper to the maximum size of 2mm x 15mm (DIN 32757/ DIN 4).	In addition to the increased level requirements 1) The material classified to level II is destructed under the surveillance of another person. The destruction is done with the method approved by authorities, e.g. with paper shredder able to shred the level II paper to the maximum size of 2mm x 15mm (DIN 32757/ DIN 4). 2) Destruction of the material is documented.	1) Classified electronic material is destroyed securely (writing over or destructing physically the storage media). 2) Classified material that is not in the electronic format is destroyed securely.	COBIT 4.1 DS11, VAHTI 8/2006, VAHTI 2/2010, EU Council Security Rules 6952/2/11 REV2 /1.4.2011 annex III	
I 604.0 **Is it secure to copy and print classified data?** *Further information in annex 1.*	1) Copies are handled in a similar way as the original document. 2) Copies can be further released to people who have a right to access and need-to-know to the information 3) Original classification markings are maintained in copying and in printing (or equivalent markings are added right after copying/printing).	In addition to the base level requirements : 1) A copy or a print-out is allowed to be made only with the device approved to the classification level. 2) Copy machines and printers are to be used in an approved space with no data or maintenance connections outside of the space, unless separately approved by authorities. 3) Mass storage media of printers, copy machines or similar devices are to be managed by the security officer of the organisation. 4) Requirements set for the electromagnetic radiation have to be fulfilled (see F 217.0)	In addition to the increased level requirements: 1) Information of copies is marked to the first page of the original and to the copies (and registers) in order to be able to track down each copy when ever needed. 2) Copy or printout is allowed to be produced only with a device deliberately approved for the project or for the working environment. 3) It is considered from a case by case basis whether every copy has to be written to a log with name of the person who took the copy/ printout. Note: also electronic copies are covered by the rule.	Sensitive material is copied and printed out according to the guidance derived from the risk assessment.	FI NSA guidelines "Handling of international classified information", VAHTI 2/2010	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 605.0 **Is the electronic transfer of classified data securely organised?** *Additional question:* *Have telecommunications (incl. electronic communication) been protected with sufficient mechanisms in view of the risks?* *Further information in annex 1.*	1) Organisation is able to detect information that needs safeguarding and willing to take appropriate measures to transfer them in a secure manner. 2) Connection between the email server and the client software is protected. 3) In case classified information is handled in emails, fax-messages, flash messages, IRC-conversations, VoIP calls, etc., the information is protected in a way which prevents the classified information to get compromised. 4) Every time when the traffic utilises public networks (internet, telecom network, mobile phone network or other network that does not meet safeguarding requirements for the classification level), the traffic or the data is encrypted in a trustworthy way when level IV (RESTRICTED) information is transferred. 5) The connection is point-to-point encrypted in a reliable way. On a case by case basis such a realisation can be accepted where a) data is transferred in a clear mode within the trusted intranet or in part of it b) traffic is encrypted from server to server or between organisations from border to border	1) Fax transfers are used only if the fax machine(s) is a) equipped with encryption device approved by Security Authority b) there is no unauthorised entry to the fax machine at the receiving end 2) Telephone connections can be used to deliver information concerning the classification level III (CONFIDENTIAL) only, if the phone has been equipped with a point-to-point crypto device/ component approved by Security Authority (see I 506.0).	1) Information classified to level II (SECRET) is not by definition transferred over public networks. Security Authority may, however, approve on a case by case basis a system where level II classified information may be exchanged between the points that have been defined beforehand. 2) Information classified to level II is not recorded and is not transferred in any form in such a network or device which has not been approved for this specific use by Security Authority in advance. Information is recorded only through defined devices. 3) Through the telephone information classified to level II can be discussed only if the Security Authority has approved the entire environment and the procedure for this particular use (see I 506.0).	Organisation is able to detect information that needs safeguarding and willing to take appropriate measures to transfer them in a secure manner.	ISO/IEC 27002 10.8, applying PCI DSS 4.1, FI NSA guidelines "Handling of international classified information", VAHTI 2/2010, EU Council Security Rules 6952/2/11 REV2 /1.4.2011 annex IV	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
	6) When sending email or fax the receiving address/number is first confirmed. 7) When classified information is transferred from a system to another, it is protected during the transfer and in the receiving system following the original safeguarding level.. 8) Case by case the need to confirm the integrity of the (email)message is evaluated. In addition it may be considered if there is a need to know that the message has been received/ read.					

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 606.0 **Is classified information securely forwarded by post and/ or via courier service?**	1) Letters/packages are addressed with names. 2) Packages may not reveal from outside that it contains classified information. Note: envelopes (or equivalents) which are used for this purpose must be non-transparent. 3) Internal post handling chain within the organisation consists only of approved personnel.	In addition to the base level requirement 1: 1) Classified information or material is carried as registered post in a non-transparent double envelope. The outmost envelope may not contain any sign of a classification. 2) Internal post handling chain within the organisation consists only of approved personnel, who have a approved and registered right to access information of classification level III. Person(s) have to have the need-to-know, defined by his/her superior to familiarise with the information. 3) When using courier services the letter or package clearly has to indicate that the package is to be carried only by courier. The courier has to be trained and equipped both with a courier certificate as well as with courier post list, to which the receiver confirms the delivery with a signature.	In addition to the increased level requirements: 1) Information or material classified to level II (SECRET) is not carried by post. This material is carried only personally or by using courier services certified to this particular level by the Security Authority. 2) When using courier services the content of the delivery has to be carried inside of a double envelope, inner of which is sealed. The receiving party confirms that the seal is not broken and informs the sending party immediately if there is any sign of tampering or of an attempt. 3) Internal post handling chain within the organisation consists only of such approved personnel, who have been approved by the owner of the information and who have a registered right to access information of classification level II. Person(s) have to have the need-to-know, defined by his/her superior to familiarise with the information. Every person who familiarises himself/ herself with the document writes his/ her full name and the date to the cover page of the document or to a separate signature book.	The carriage is done in a way which is considered to be secure enough, following the risk assessment.	ISO/IEC 27002 10.8.3, FI NSA guidelines "Handling of international classified information", VAHTI 2/2010	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 607.0 **Is it possible to track where and where from classified information has been forwarded?** *Additional question:* *Is classified information registered?*	No requirements.	Delivery is registered. No requirements to track the delivery. Note! EU Classified Information is registered.	1) Information classified to level II, regardless of its form, is registered before the delivery process begins and at the end of the process. If a communications and information system is in case, the registering may be carried out through processes within the system. 2) Information classified to level II is registered to a specific level II registry only. 3) The register is handled and stored in a similar manner as the document classified to level II. 4) The register has to indicate who has the access to the document at each moment. This goes on until the end of the life cycle of the information or document. 5) Log files of the handling of information classified to level II are recorded (see I 504.0).	No special recommendations.		

Security of Information Handling, subdivision I 700

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 701.0 **Has it been ensured that the organisation has, in view of its operations, adequate business continuity plans?** *Additional questions:* *Is recovery readiness tested on a regular basis?* *Is classified information protected also in emergency situations?* *Further information in annex 1.*	1) Usability requirements of systems have been defined. 2) Organisation has made it sure that if critical networks (incl. internet connection), network devices, information systems servers or equivalent fail, the recovery will be completed within the time set in the operational requirements. 3) Plans cover the safeguarding of classified information in emergency situations. Safeguarding has to cover the confidentiality, integrity and usability of the information. 4) Plans include proactive and reactive measures.	1) Usability requirements of systems have been defined. 2) Organisation has made it sure that if critical networks (incl. internet connection), network devices, information systems servers or equivalent fail, the recovery will be completed within the time set in the operational requirements. 3) Plans cover the safeguarding of classified information in emergency situations. Safeguarding has to cover the confidentiality, integrity and usability of the information. 4) Plans include proactive and reactive measures.	1) Usability requirements of systems have been defined. 2) Organisation has made it sure that if critical networks (incl. internet connection), network devices, information systems servers or equivalent fail, the recovery will be completed within the time set in the operational requirements. 3) Plans cover the safeguarding of classified information in emergency situations. Safeguarding has to cover the confidentiality, integrity and usability of the information. 4) Plans include proactive and reactive measures.	1) Usability requirements of systems have been defined. 2) Organisation has made it sure that if critical networks (incl. internet connection), network devices, information systems servers or equivalent fail, the recovery will be completed within the time set in the operational requirements.	ISO/IEC 27002 14.1, ISO/IEC 24762, ISO/IEC 27031, COBIT 4.1 DS4, VAHTI 8/2006, EU Council Security Rules 6952/2/11 REV2 /1.4.2011 article 5, VAHTI 2/2010 annex 5 (TTT), VAHTI 3/2010	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 702.0 **Does the documentation available in the organisation allow recovery from malfunctions, disturbances, attacks, and so on?** *Additional questions: Is recovery possible if the person responsible for the system or network is not available? How fast will recovery happen? Is it monitored on a regular basis that the documentation of the environment handling protected information is up-to-date? What action is taken if the information is insufficient?* *Further information in annex 1.*	1) Networks, systems and their settings have been documented in a way that malfunctions and other operational disturbances can be fixed according to the operational requirements. 2) Documentation dealing with the environment where classified information is handled is equal to the realisation. 3) Differences are handled as information assurance deviations.	1) Networks, systems and their settings have been documented in a way that malfunctions and other operational disturbances can be fixed according to the operational requirements. 2) Documentation dealing with the environment where classified information is handled is equal to the realisation. 3) Differences are handled as information assurance deviations.	1) Networks, systems and their settings have been documented in a way that malfunctions and other operational disturbances can be fixed according to the operational requirements. 2) Documentation dealing with the environment where classified information is handled is equal to the realisation. 3) Differences are handled as information assurance deviations.	Networks, systems and their settings have been documented in a way that malfunctions and other operational disturbances can be fixed according to the operational requirements.	ISO/IEC 27002 14.1, ISO/IEC 27002 10.1, VAHTI 2/2001, VAHTI 5/2004, VAHTI 8/2006, VAHTI 2/2010 annex 5 (TTT), VAHTI 3/2010, http://www.interpol.int/public/technologycrime/crimeprev/companychecklist.asp, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/ guidelines/guidelines_pdf.pdf	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 703.0 **Does the organisation apply clear principles and procedures regarding who have the right to install software, network connections and peripherals?** *Additional questions:* *Are only the networks and systems used that have passed the approval process? Are only premises, networks and systems approved by the authorities used for handling classified information? How is the integrity of information systems guaranteed?* *Further information in annex 1.*	1) Organisation applies clear principles and procedures regarding who have the right to install software, network connections and peripherals. 2) Implementation of principles is supervised and ensured by technical means (e.g. by limiting the installation and modification rights to the maintenance personnel). 3) Modifications to security settings and applications are denied from end-users. 4) Organisation has the criteria to accept new systems, system updates and other relevant changes. Only the networks and systems which have passed the approval process are used (see configuration management in A 608.0). 5) Only networks and systems approved by competent authorities are used to handle classified information.	In addition to the base level requirements: Handling of classified information is done only on premises approved by competent authorities.	In addition to the base level requirements: Handling of classified information is done only on premises approved by competent authorities.	1) Organisation applies clear principles and procedures regarding who have the right to install software, network connections and peripherals. 2) Implementation of principles is supervised and ensured by technical means (e.g. by limiting the installation and modification rights to the maintenance personnel). 3) Modifications to security settings and applications are denied from end-users.	ISO/IEC 27002 10.3.2, ISO/IEC 27002 12.1.1, ISO/IEC 27002 12.4.1, FI NSA guidelines "Handling of international classified information", VAHTI 8/2006, EU Council Security Rules 6952/2/11 REV2 /1.4.2011 articles 9 and 10, VAHTI 2/2010 annex 5 (TTT), VAHTI 3/2010	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 704.0 **Has the organisation adopted principles and security mechanisms against the risks of remote working?** *Further information in annex 1.*	1) Organisation has adopted principles and security mechanisms against the risks of remote working 2) The personnel have been informed about the principles and the required mechanisms. 3) Personnel have access to a guideline documentation concerning security of remote working and business trips. 4) Devices, information or applications are not removed from the office environment without authorisation. 5) In remote controlling of systems strong authentication methods are used. 6) Devices containing classified information have been safeguarded against unauthorised access, misuse or corruption during their stay outside the premises of the organisation. 7) Devices and storage media are not left without surveillance in public places. Laptops are carried as hand package. 8) Only such remote connections are used which are reliable and have been approved to the particular working environment (e.g. company laptop).	Remote management or controlling of level III systems is denied by definition. Remote controlling may only be allowed through procedures specially approved by a competent authority.	Remote management or controlling of level II systems is denied. In the communication systems of public authorities a limited remote controlling may be accepted after a separate accreditation procedure.	1) Organisation has adopted principles and security mechanisms against the risks of remote working 2) Organisation has adopted principles and security mechanisms against the risks of remote working	ISO/IEC 27002 10.8.3, ISO/IEC 27002 11.4.2, ISO/IEC 27002 11.7.1, ISO/IEC 27002 11.7.2, ISO/IEC 27002 9.2, ISO/IEC 27002 9.2.5, ISO/IEC 27002 9.2.7, VAHTI 1/2001, VAHTI 2/2003, VAHTI 8/2006	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 705.0 **Are the development/ testing and production systems separate?** *Further information in annex 1.*	1) Development / testing and production systems are separate. 2) Before taking a new system into use, test data, default and test user accounts (or similar) are erased. 3) Classified information is not copied to test or development environment if their classification level is lower than the one of the production environment.	1) Development / testing and production systems are separate. 2) Before taking a new system into use, test data, default and test user accounts (or similar) are erased. 3) Classified information is not copied to test or development environment if their classification level is lower than the one of the production environment.	1) Development / testing and production systems are separate. 2) Before taking a new system into use, test data, default and test user accounts (or similar) are erased. 3) Classified information is not copied to test or development environment if their classification level is lower than the one of the production environment.	1) Development/ testing and production systems are separate. 2) Before taking a new system into use, test data, default and test user accounts (or similar) are erased.	ISO/IEC 27002 10.1.4, PCI DSS 6.3.2, PCI DSS 6.3.4, PCI DSS 6.3.5, PCI DSS 6.3.6	
I 706.0 **How is it guaranteed that the network and its services do not have known vulnerabilities?** *Additional questions:* *Is there a designated person to do follow-up on information assurance bulletins? Are there established procedures for installing information assurance updates? Is the implementation monitored?* *Further information in annex 1.*	1) Information given by public authorities (like CERT-organisations), manufacturers and other relevant actors are followed and necessary security updates are installed in a controlled manner. 2) The network, the services, workstations connected to the network and laptops are scanned yearly to locate possible vulnerabilities.	In addition to the base level requirement 1: Scanning is done at least twice a year and always after significant changes in the configuration.	In addition to the base level requirement 1: Scanning is done at least twice a year and always after significant changes in the configuration.	Information given by public authorities (like CERT-organisations), manufacturers and other relevant actors are followed and necessary security updates are installed in a controlled manner.	ISO/IEC 27002 12.6.1, ISF-SOGP CI3.6, PCI DSS 6.1, PCI DSS 6.2, PCI DSS 11.2, VAHTI 8/2006, VAHTI 2/2010 annex 5 (TTT), VAHTI 3/2010, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines_pdf.pdf, http://www.sans.org/critical-security-controls/control.php?id=10 Information assurance bulletins: http://cert.fi/palvelut/postituslistat.html, http://www.securityfocus.com/archive/1	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 707.0 **How is it ensured that during pauses or after work the equipment are not left without proper protection?** *Note: See the automatic locking of workstations:* *I 502.0*	1) Users are entitled to the following: a) Workstation, terminal, laptop (or similar) is locked always when the user leaves the device (password protected screen saver etc.). b) Active sessions are terminated after the work has been completed and on longer breaks (e.g. remote connections and server sessions are disconnected). c) After the work has been completed the user logs out from the system. 2) In case a device containing classified information is left to a space where unauthorised people have access to, the password protection is activated when leaving the device (e.g. by switching off the laptop causing the encryption to activate).	In addition to the base level requirement 1: By definition devices containing information classified to level III are not left to a space where unauthorised people have access to.	In addition to the base level requirement 1: By definition devices containing information classified to level II are not left to a space where unauthorised people have access to.	Users are guided to the following: a) Workstation, terminal, laptop (or similar) is locked always when the user leaves the device (password protected screen saver etc.). b) Active sessions are terminated after the work has been completed and on longer breaks (e.g. remote connections and server sessions are disconnected). c) After the work has been completed the user logs out from the system.	ISO/IEC 27002 11.3.2	
I 708.0 **Is the so called clear desk policy applied? Does this also apply to display screens?**	1) Clear desk policy concerning papers and removable storage media as well as the clear display policy concerning IT-services is in use. 2) Employees look after that no classified material or notes are left to meeting rooms after meetings.	1) Clear desk policy concerning papers and removable storage media as well as the clear display policy concerning IT-services is in use. 2) Employees look after that no classified material or notes are left to meeting rooms after meetings.	1) Clear desk policy concerning papers and removable storage media as well as the clear display policy concerning IT-services is in use. 2) Employees look after that no classified material or notes are left to meeting rooms after meetings.	1) Clear desk policy concerning papers and removable storage media as well as the clear display policy concerning IT-services is in use. 2) Employees look after that no classified material or notes are left to meeting rooms after meetings.	ISO/IEC 27002 11.3.3, VAHTI 8/2006	

Question	Requirements for the base level (IV)	Requirements for the increased level (III)	Requirements for the high level (II)	Recommendations for the industry	Source/ additional information	Note
I 709.0 **Have tasks been sufficiently separated to ensure that the so-called dangerous combination of duties does not occur?** *Additional question: Has it been ensured that critical maintenance measures require approval from two or more people?*	No requirements.	1) Tasks and areas of responsibility have been separated from each other's when possible to decrease the risks for unauthorised or unintentional modification or misuse of classified information. 2) It is advisable to avoid dangerous combinations of duties. However, if they occur, a monitoring method has to be in use. 3) Critical functions to which monitoring and surveillance is targeted have to be defined system by system.	1) Tasks and areas of responsibility have been separated from each other's when possible to decrease the risks for unauthorised or unintentional modification or misuse of classified information. 2) It is advisable to avoid dangerous combinations of duties. However, if they occur, a monitoring method has to be in use. 3) Critical functions to which monitoring and surveillance is targeted have to be defined system by system.	Tasks and areas of responsibility have been separated from each other's when possible to decrease the risks for unauthorised or unintentional modification or misuse of classified information.	ISO/IEC 27002 10.1.3, VAHTI 8/2006, COBIT 4.1 PO4.10	
I 710.0 **Is there a sufficient back-up procedure in place?** *Further information in annex 1.*	1) Back-up procedures meet the operational requirements. 2) Back-up copies are stored in a different physical space than where the system itself is located. 3) Access to back-up copies is prohibited from unauthorised personnel. 4) Back-up copies containing classified information are stored in a place that meets the requirements set by the classification level of the information. Back-up copies may be encrypted, when needed.	In addition to the base level requirements: Lists of back-up media exist.	In addition to the base level requirements: Lists of back-up media exist.	1) Back-up procedures meet the operational requirements. 2) Back-up copies are stored in a different physical space than where the system itself is located. 3) Access to back-up copies is prohibited from unauthorised personnel.	ISO/IEC 27002 10.5.1, PCI DSS 9.5, COBIT 4.1 DS4, COBIT 4.1 DS11, VAHTI 2/2010 annex 5 (TTT), VAHTI 3/2010, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/ guidelines/guidelines_pdf.pdf	

ANNEX 1: FURTHER NOTES FOR AUDITING QUESTIONS

A 401.1

1) Detection of objects/targets to be safeguarded may be done e.g. by listing the objects or targets to be safeguarded together with the requested safeguarding measures, according to the requirements set by the integrity, confidentiality and usability.
2) Following the previous, the threats can be detected by asking the list of the risks detected for the object/target to be safeguarded.
3) Can be detected by asking for the list of the objects to be safeguarded and for the personnel responsible for it.
4) It is essential to ensure that the protections of the critical systems for the organisation are on adequate level.

A 408.0

Note, on level III:

1) This can be verified by requesting examples of how information assurance has been assessed and developed and by requesting for a description of the used systematic method and to show the results it produced.
Furthermore, this can be verified by requesting to see the report produced by an external auditor.

A 608.0

The requirement may be fulfilled by incorporating into the process of the most significant changes the following: identifying and recording changes; planning and testing changes; assessing the possible impact of changes including effects on security and the formal approval process of changes. For verification, information assurance principles, information assurance policies and information assurance guidelines are compared to actual implementation in the organisation.

F 201.0

Recommendation for the floor structure in levels III and II: hollow concrete plate element, added with a separate surface level concrete casting.
Recommendation of the wall structure for levels III and II: concrete elements reinforced with steel or a min. 1500 mm thick concrete/steel structure.
It is advisable to notify the structural fire safety requirements for the wall, floor and ceiling structures.

F 205.0

Door structures: it is recommended that doors including the protection against intrusion should be so called combination doors, which incorporate also the requirements concerning the sound insulation and fire safety.

F 209.1

Can be implemented e.g. by reviewing the user rights and access rights of all personnel, suppliers and external users on a regular basis, for example every six months. In addition, in all changes such as promotions, demotions, job rotation and, in particular, when employment ends there should be a clear and well-functioning procedure for changing or revoking rights. For example, the superior informs the responsible persons in advance of the changes and, as a result, all rights are kept updated. In practice, this may mean that user rights and access rights are revoked or changed in the central administration system or separately in individual systems.

F 217.0

In some situations it may be permitted to take electric devices into a room if batteries are removed, for example.
When handling international classified information (like EU Classified Information) the countermeasures against electromagnetic radiation/propagation (TEMPEST) are normally set as a requirement from the level III (CONFIDENTIAL) upwards. When handling classified information originating from some other country or from national basis, the above mentioned protection is normally required either from the level III (CONFIDENTIAL) or from the level II (SECRET). Protection against electromagnetic radiation is achieved by choosing an appropriate location; by lining; or by using protected equipment and cablings (TEMPEST). See the requirements for physical security.

F 218.0

With a definition "according to the operational requirements" is referred to the usability requirements of the system. If these are considered essential, the requirement for back-ups is set as a requirement. Back-ups can be understood e.g. as the protection of important systems and device rooms against the environment (intrusion, fire, heat, gases, dust, vibration, water). In addition, back-up operations may include the duplication of critical devices and / or using uninterruptable power supplies (UPS).

I 401.0

It is possible to connect level IV systems / information processing environment to the Internet and to other un-trusted networks when other safeguarding requirements are fulfilled. A typical using environment for a level IV system is the office network of the organisation.
Information processing environment of the level III are by definition separated from un-trusted networks and systems. Level III information processing environments are normally disconnected from other networks / systems. The Security Authority may, however, in some cases approve the physical interconnection between level III information processing environment and an accredited network of a lower level. Such separately approved networks or systems can be divided as follows:

A. Data transfer systems

Level III system or network may be a data transfer system between two or more physical points. In this case each of these points has to 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 firewall] – [Internet] – [hardware firewall]- [crypto device approved to the level] – [hardware or software firewall] -[physically separated network/work station]. See I 509.0 for approved crypto applications. The arrangement can be accredited by the Security Authority accordingly to level II.

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.

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 separate data diode , allowing only a one-way traffic. The arrangement can be accredited by the Security Authority accordingly to level II.
C2. The data handling of the lower level environment, executed by the end-user from the level III information processing environment, can be done with a terminated gateway solution (e.g. certain virtual desk top environments). The arrangement can be accredited by the Security Authority accordingly to special government systems from level II to level III.
C3. In level III information processing environment the use of a lower level network can be achieved by a gateway solution which strictly limits the traffic and information contents, and in which the filtering of the contents takes place on protocol and / or application level between the servers.

D. Other information processing environments

Other level III information processing environments are normally research and development networks of the organization and other level III information processing environments. The most common system which the Security Authority may approve to be connected to such an environment is the update server serving solely this environment. Centralised security updates and malware detection delivery may be approved with certain limitations. Updates and detection bases are received from the update server normally though air-gap. On case by case basis a solution can be approved to download the updates and detection bases directly from the Internet. In such cases the update server has to be configured to the strictest; to allow the connections to the Internet on network and application levels only to the updates services of manufacturers; and the connection to level III network has to be limited only to connections necessary for update deliveries. The latest limitation can be achieved by using the so called data diode, which limits the traffic to one way only, or by using some other method that has separately been approved as reliable. It is possible, on case by case basis, to accept an optical disk or USB-stick as a system connected to level III network.

For companies the environments presented in chapter D are normally the only acceptable solutions. A network of several projects may be approved for level III on case by case basis. For level II solutions limited to one project only can be accepted.

On approvals made case by case the approving authority has to be the owner of the information or the authority designated as responsible for the approval. For instance in cases where international classified information is handled, it is up to the Security Accreditation Authority, SAA (in Finland the NCSA-FI, located in the Finnish Communications Regulatory Authority, FICORA) to inspect and approve the environment.

I 402.0

For workstations and laptops, the firewall requirement on the base level (level IV) is easiest to achieve by a software firewall, where permitted software has been defined and the traffic of others actors is denied.

What comes to the requirement 5 on level IV it is to be notified that on certain networks where international information is handled it is acceptable to allow the web-browsing only to addresses approved in beforehand (whitelisting).

The consequences of denials of service (DoS, DDoS) can be decreased e.g. by
1) using an adequate data transfer, network device and server capacity,
2) using reserve connections (connections using a separate routing, connection from different operators, alternative information transfer media, like radio links and satellite connections)
3) placing a contract with the operator of a constant or separate messaging procedure concerning the upcoming data scrubbing performed by the operator. The malicious results of spam messages can be decreased by filtering (in operator network, at the edge of the organisation network, in work stations) and by setting the maximum size for the attachment files.

See the configuration requirements set for network devices in I 405.0.

I 404.0

Here active network devices refer to firewalls, routers, switches, wireless base stations and equivalent devices / systems. If network devices are managed by other means than physically connecting to the device, and if the management connection is not physically separated the management traffic shall be encrypted. Often the requirement is best met when the management of network devices is prevented by using telnet and the SSH connection for management. In the same way other non-encrypted management applications should be avoided (e.g., HTTPS to be used instead of HTTP in systems managed with a web browser.

I 405.0

Here active network devices refer to firewalls, routers, switches, wireless base stations and equivalent devices / systems. See I 502.0, particularly the sources. When the control of the network device is not possible through the individual user ID, the use of common (maintenance) user IDs has to be covered by rules (see I 501.0). When the size of the environment is large (mainly network devices, especially routers), the authentication is recommended to be done by using duplicated AAA-servers (especially TACACS+, RADIUS or Kerberos). It has to be notified that the chance of default passwords covers also the SNMP community passwords (Community Strings).
For the requirement 6 on level IV there are name practices dedicated to manufacturers, like “private VLAN” and/or “protected port”.
When implementing the requirement 1 for level III it is recommended to record all control commands that are used.
Note! See the log requirement in I 504.0, filtering requirement in I 402.0 and in I 508.0.

I 409.0

When IPv6 feature is used in work stations, servers, network devices or in other similar systems, the consequences should be taken into account especially in traffic filtering (firewalls have to cover IPv6 traffic as well) and in routing (see I 410.0). It is also worth noticing that intranet users ought to be identified afterwards e.g. for solving information assurance incidents. IPv6 Privacy Extensions may cause significant difficulties to the identification.

I 410.0

OSPF: To be used MD5 based, stronger RFC 5709 compatible or in IPv6 cases OSPFv3 authentication.
IS-IS: To be used MD5 based or RFC 5310 compatible authentication.
BGP: To be used MD5 based authentication.

I 501.0

At least the following shall be taken care of as part of reliably organising identification and authentication

i) the authentication is protected against man-in-the-middle attacks
ii) at login and before authentication no unnecessary information is revealed
iii) authentication credentials are always encrypted if they are sent via network
iv) authentication method is protected against resent attacks
v) authentication method is protected against brute force attacks. The B and A level requirement for strong user identification can be arranged in some cases so that the information system can be accessed only from a carefully restricted physical space where access is controlled with strong authentication. Then the user can be identified in the information system through a user ID/password.

I 502.0

On base level (IV):
Workstations and laptops:

1) the platform consists only of the software elements necessary for the system
2) necessary security updates are installed to the operating system and to the application software
3) Access rights to user accounts automatically created when installing the system (e.g. "administrator" and "guest") are limited to minimum or removed from use.
4) Default passwords are changed.
5) Work stations lock up automatically, if not used for certain period. Minimum requirement is to use a password protected screen saver, which activates after 10 minutes of idling time.
6) User rights are set according to F 209.1.
7) Logging methods are set (further information: I 504.0).
8) 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).
9) Software applications, especially web-browsers, PDF readers, office software and e-mail applications are configured in a secure manner.

9.1) E-mail applications: a) automatic running of programme code denied, b) Sending of e-mail in HTML-mode is prevented and when receiving such, it is translated to text mode, c) automatic preview of e-mails is prevented, d) attachment files are not automatically opened, e) as attachments to the e-mail message only certain types of files are accepted. Use of other types is technically prevented e.g. by filtering them and notifying the uses with a message, f) e-mail messages considered as spam are filtered or at least equipped with a warning in the title field of the message.

9.2) PDF readers, word processors and similar: automatic running of programme code (especially Java Script and macros) is denied by default.

Servers, in addition to the requirements for workstations:

1) User rights for platform components, processes (e.g. server processes), folders and add-on programmes are set according to the principle of least privilege
2) servers are configured according to the instructions of manufacturers or other trusted parties
3) e-mail servers do not accept a) relaying (open relay), b) verification of the address or the membership of the list (commands "VRFY" and "EXPN"), c) unprotected user connections (TLS/SSL or equivalent required) d) too large attachment files.

Network devices: I 405.0

Network printers, phone systems and similar:

Equal requirements as for the workstations and for the servers taking into account the specific aspects: services (especially network services) are limited to the ones needed, default administration passwords are changed, and the necessary security updates are installed.

On increased level (III)

Workstations, laptops and servers:

1) The services provided (especially network services) are set to minimum and limited only to the necessary ones. Network zoning is never used when the device is connecting to un-trusted network.
2) Operating systems and other programmes are configured to download updates only from the source specified for the purpose and all unnecessary network traffic is not allowed.
3) BIOS-settings are set to meet the security requirements and the changing of the settings is prevented from unauthorised users: a) access to BIOS settings is protected with password, b) boot up is allowed only from primary hard disk, c) unnecessary services and ports are removed from use.

The requirement 2 is targeted to increase the ability to detect unauthorised traffic, e.g. by minimising the software update requests. In practice this means e.g. that unless there is a need or will to let applications to update themselves automatically (or it is not possible from the perspective of user rights), the applications are configured not to send request for updates.
In system configuration on level III FDCC requirements (or equal) are to be fulfilled. In handling of certain part of the international information the FDCC requirement is valid already on level IV (RESTRICTED). The level II requirements may be accomplished by using software detecting the integrity of the system. More information can be found from http://nsrc.org/security/#integrity. See e-mail safeguarding requirements from I 605.0.

I 503.0

It is recommended that the results derived from anti-malware are followed through a centralized administration system.
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). Especially on level II systems the updates are normally loaded in manually. In both cases it is important to be sure of the integrity of updates (source, check sums etc.).
The requirements set for levels III and II are set to reduce especially the risk of malware contamination caused by the use of USB-sticks. On case by case basis the requirement may be set to ensure that only such USB-sticks (or other removable mass storage media) which have been approved for use and are not connected to any other system. On case by case an arrangement may be accepted, where only storage media delivered by the ICT-administration of the organisation may be used and connections of all other storage media is not allowed, or is technically prevented.
On cases where there is a specific need to import information from untrustworthy sources by using a storage media there has to be a procedure in place to decrease the risk. One possibility could be to check the storage media in an isolated check point and to transfer on the information by using a separate storage media. Note: on level III at least the memory area has to be checked. On level II also the controller level tailored risks are to be taken into account.

I 504.0

The requirement of the coverage can be in most cases 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 is to be confirmed afterwards what kind of administrative functions the network device has gone through, when and by who (see I 405.0).
Event logs should be gathered of the use of the system, of user activities, of functions and exceptions dealing with security. One method that can be recommended to protect the logs is to forward all logging information on a centralised manner to a specific, strongly safeguarded logging server, the information content of which is periodically backed up.
What is understood with the term “crucial recordings” depends on the context. What is always counted on is the log data of fundamental network devices and servers. Depending on the using environment and the security level also the log data of e.g. workstations etc. is often covered by the definition.
On workstations and servers the implementation often needs the logging to be switched on and the default values to be changed what comes to storage duration and mode. E.g. in Windows environment 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 addition the duration and storage capacity of the logs should be increased. Recommendation: at first stage reserve at least 500 Mb for logs or make estimation according to the system environment. To define the 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 duration. Note: it is advisable to reserve some buffer capacity, as situations change and because certain cyber attacks increase log activities a lot.
To achieve the level III requirement 2 e.g. automated scripts, through which the changes in log information and in file systems can be viewed. In Windows environment most crucial information can be gathered e.g. with the help of wmic-tool (Windows Management Instrumentation Command-line). Accordingly in most of the Unix/Linux environments the crucial information can typically be gathered and viewed through scripts and tools supported by the system (e.g. last) from the following locations:

- /var/run/utmp
- /var/log/wtmp
- /var/log/btmp
- /var/log/messages
- /var/log/secure

There are several ways to monitor the network traffic, from the scrutiny carried out on the level of crucial network nodes, all the way to the sensors on workstations/servers and to the combination of these both.
On certain networks handling international classified information the monitoring of logs is required already from the level IV (RESTRICTED).
More system based guidance can be found e.g. from sources described on the source field of I 502.0.

I 505.0

The requirements about server level encryption may in some particular server environments be replaced with some other solution approved by the Security Authority. Such a procedure requires always exceptionally reliable implementation of physical and logical access control, as well as administrative measures in handling storage media.
The meaning of the separation of information by the classification level is to guarantee that people who don't have access rights to the upper level information can not have access to it. Information belonging to different classification levels may be stored on same locations, when all personnel having access to the storage location have access right to all of the information stored on the location (example: hard disk of the laptop used by one person only).
Owners of the classified information often reserve the right to audit all networks or systems, where their information is handled. In audits it is normal to request physical and logical access to the target under audit, making therefore possible for the auditor to have access to the actual information. In systems where multiple projects are handled it is essential to guarantee through the structure of the network or system that people who don't have the access right to the information of the other owner cannot access this information. For the information of level IV it is in most cases sufficient that the access is controlled through logical separation (e.g. virtual servers to each project). From level III on a physical separation is typically required and/or encryption of information/information transfer in devices used for several projects.

Recommendation to destroy temporary files: using logon or logoff scripts files are destroyed with overwriting method from the most common folders and of most common document formats, stored in temporary files. In practice e.g. %HOMEPATH%/Local Settings/Temp with sub-folders, of which the following are overwritten: .doc*, .dot*, .xls*, .ppt*, .pdf, .rtf, .txt, acc*, .htm*, .mht, .xml, .jpg, .jpeg, .png, .tif*, .gif, .bmp, .zip, .gz, .tgz, .rar, .part, .tmp.
In servers and in other such environments where the system is not often restarted, it is recommended that the overwriting is programmed to take place on certain periods, like once in 24 hours.

I 506.0

Most of the common operating systems offer the possibility to encrypt the hard disk already when installing the system. Alternatively a separate software solution may be used. There are both software and hardware solutions to encipher USB-sticks and other mass storage media. See I 509.0.

I 507.0

With the erasure in a trustworthy way is meant in this occasion the overwriting of the information. This requirement is valid for all devices to which classified information once has been stored, e.g. laptops, workstations, servers, phones, printers, network devices etc.
See I 603.0. When it is impossible to overwrite the information in a trustworthy way, the device or the part of it has to be destroyed mechanically.

I 508.0

The requirement 3 for the classification level III can be implemented e.g. by using 802.1X procedures.
To fulfil the requirement for the classification level II it may be necessary to
a) place the devices on a security rack (or similar) that is sealed and/or equipped with an alarm system
b) to use devices protected against tampering, or
c) some other similar method (e.g. sealing the devices in use).
Shielding of the electricity and data cablings may be required for part of the international classified information already from the level III (CONFIDENTIAL).
See: Configuration of network devices, I 405.0

I 509.0

Especially when ciphering international classified information only the crypto solutions approved by the owner (e.g. EU) of the information may be used. The national Crypto Approval Authority, CAA (in Finland the NCSA-FI of the Communications Regulatory Authority, FICORA) has certain limited possibilities to approve also other products or solutions to protect the international classified information.
To get approval by several international security authorities certain certificates are required for the product (especially the Common Criteria, sometimes also FIPS 140), in addition to fulfilling certain special requirements (e.g. release and analysis of the source code, TEMPEST shielding).

I 510.0

Includes also the TLS/SSL keys. See I 509.0. The requirement for the key exchange period is determined according to the using environment and purpose.
In situations where the classified information has to be sent over untrustworthy network, and where there is no protected and approved (by authorities) information exchange channel in use, it is recommended to use the following method to form the encryption key:
A common part of the encryption key, consisting of 15 characters is settled between the user points. Settling has to be done face-to-face or by some other reliable method approved by Security Authorities. When sending the information between the terminal points the sender adds to the encryption key a "random" part consisting from 10 till 15 characters and uses this one time key of 25-30 characters to encipher the information. After this the sender can send the latter part of the key to the receiving party with some other communication method, like SMS. Note: the latter part has to be changed after each transmission.
The procedure described and the encryption solution has to be approved in beforehand by the owner of the information or by the actor designated by the owner of the information. In case of exchange of the international classified information this authority is the national Crypto Approval Authority, CAA (in Finland the NCSA-FI of the Communications Regulatory Authority, FICORA).
Solutions based solely on software applications are typically approved to level IV only, but in some cases to level III. For the information classified to SECRET (level II) requirements for the encryption software platform (hardware) are typically set. This is usually the case already in level III.

I 513.0

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 feedings and with large quantity of feedings.
4) Depending on the developing environment there is a policy in use for functions and interfaces that 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 is ensured.

In addition the documentation of the programmes to be purchased has to be available and to give information at least of the network ports used by the programme. It is recommended also to require that
a) applications use a small amount of designated ports
b) applications using dynamic ports use only a small port space, and
c) programmes don't require large user rights to function (i.e. programmes have to run with the rights of a basic user)

I 514.0

The information assurance requirements set for the device to be purchased are highly depending on the using purpose. E.g. for the printer very different requirements may be set depending on the level of the information to be printed. The requirements may consist of access control (just locking vs. user identification and authentication), possibility to gather logs, possibility to encrypt and erase the memory/hard disk, switching (local vs. network printer), encryption of network traffic, security solutions of remote management, Tempest shielding etc.

I 602.0

See the material in information systems: I 505.0, I 506.0, I 507.0, I 514.0. For storage spaces (safes etc.) the detailed requirements given in subdivision F have to be taken into account from regular basis (e.g. the class, attachment method, additional requirements for intrusion detection systems etc.) Backups: storage in a separate sag space (I 701.0).

I 603.0

1) Destruction of classified electronic material is done in a reliable way (overwriting or physical destruction of the recording).
2) Temporary classified files created during the use of information systems are destroyed regularly. See I 505.0.
3) Destruction of classified information which is in non-electronic form is organised in a reliable manner. The organisation has a paper shredder, resulting of which is maximum 2mm x 15mm (DIN 32757/ DIN 4), or some other approve method to destroy the material of level IV (like burning).

I 604.0

For some international classified material the traceability is required already from the level III (CONFIDENTIAL). The need is verified case by case. On the requirement 3 for level III it has to be taken care that the service personnel has no access to the device (printer etc.) without escort. See visitor requirements in F 209.2.

I 605.0

Covers telephone, telefax, e-mail, short messaging and other data transfer methods.
Requirement 2 for level IV: in most cases it is easiest to use encryption protocols instead of using non-ciphering alternatives. E.g. IMAPS protocol instead of IMAP. See I 502.0 and I 511.0.
Requirement 3 for level IV: in most cases the implementation is easiest when using point-to-point encryption on application layer level or by writing the safeguarded information into the attachment file which is encrypted in a reliable manner (sees I 509.0). In some cases the use of company level rapid messages and / or VoIP solutions is recommended. In these cases the server, client software and the traffic between them is kept inside the trusted network component and the traffic is enciphered.
Requirement 4 for level IV: See I 401.0.
Requirement 1 for level II: to transfer the material over the public network requires the written approval given by the Security Authority and concerning the system complex to be used. This system complex consists of e.g. a separately accredited information system with dedicated configurations, of an approved crypto solution (software + hardware platform), as well as of the physical location of the system including the safeguarding measures (e.g. access control, Tempest shielding etc.) See I 401.0.

I 701.0

For the environments of high usability requirements a business continuity / recovery plan is required, as well as regular testing of the plan.
See documentation requirement in I 702.0, risk analysis requirement in A 401.2 and the requirements for the heating, water, air conditioning and electrical arrangements in F 218.0.

I 702.0

In practice this requires in most cases the documentation of the structure of the network, IP addresses, zones, segments, firewall rules, operating system and firmware versions of network devices, software version and settings of servers and production systems etc. in such a detailed level, that the recovery takes place according to the continuity plan, regardless of malfunctioning of whichever of the above mentioned components.
Depending of duties or the sector organisation is working on, it may be possible that the requirement is set for the documentation to make it possible for the external actor to be able to set the malfunctioning networks and systems into normal operating condition. The documentation has to be kept up to date. One recommended method to keep the documentation is to use a wiki system, where all changes in network or system are updated when they occur. There are also several professional applications for this use on the market.

I 703.0

1) Clear principles and procedures are in use of who is allowed to install programmes, data connections and peripherals.
2) Following the principles is monitored and verified by technical means (like by limiting the installation and configuration rights to the maintenance personnel.
3) Unauthorised changes to security settings and applications are prevented from basic users.
4) Acceptance criteria exists for new systems, system updates and similar. Only such systems and networks which have gone through the approval are used. See: A 608.0.
5) Only networks and systems accredited by authorities are used to handle classified information.

I 704.0

The remote management or controlling procedure accepted for level III takes into account e.g. the physical and logical access control of the remote sites, the devices and programmes used, encryption of the remote management traffic, and the reliability of the above mentioned especially what comes to the confidentiality and integrity.
In government level II systems it may be possible on a case by case basis to accept the use of limited remote management. The case by case acceptable use of limited remote management means in this connection almost without exception the centralised delivery of security updates and malware fingerprint bases. The remote management can be accepted in such cases, where, after a thorough and complete risk analysis the result shows that the remote management forms a considerably lower risk than the local management. The prerequisite for accepting this kind of remote management is the incorporation of the update server into the same information system and the separation of it from other systems.

I 705.0

The production system has to be a separate one in order to guarantee that the development and testing functions do not cause interruptions in the production or security risks. The production data may be copied to the development and testing environment after the data has been sanitized in a way which guarantees that the confidentiality is not endangered. See A 608.0 (management of changes).

I 706.0

Examples of the implementation: information updates from CERT-community and from manufacturers are subscribed as e-mail. From these updates such information is picked up, which have impact to the security of the systems of the organisation and these are installed to operating systems, network devices (mainly firmware), server applications etc. The influences of updates should be tested before bringing the updates to the production environment. Testing can be done in an isolated test environment or by a small user group.
To ”significant changes” can be counted e.g. changes in network topology, new systems to be taken into use and / or major updates to old systems, changes on filtering rules of firewalls etc.

I 710.0

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) Intervals for backups are 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.)

National Security Auditing Criteria

ISBN: 978-951-25-2247-7 print
ISBN: 978-951-25-2248-4 pdf

www.defmin.fi