MINISTRY OF FINANCE
Finland

Requirements for ICT Contingency Planning

The Government Information Security Management Board

2b/2012

VAHTI

MINISTRY OF FINANCE

Requirements for ICT Contingency Planning

Government Information Security Management Board

2b/2012

VAHTI

NORDIC ECOLABEL
441 729
Print product

MINISTRY OF FINANCE
PO Box 28 (Snellmaninkatu 1 A) FI-00023 GOVERNMENT
FINLAND
Tel. +358 295 16001
Internet: www.financeministry.fi
Layout: Pirkko Ala-Marttila

Juvenes Print – Finland University Print Ltd.

MINISTRY OF FINANCE

Instruction VM/1619/00.00.00/2012

25 September 2012

To Government Ministries and Agencies

INSTRUCTIONS ON REQUIREMENTS FOR ICT CONTINGENCY PLANNING

The objective of the Ministry of Finance's Instructions on Requirements for ICT Contingency Planning is to enhance and harmonise ICT contingency planning within the ministries and organisations in their administrative branches. According to the Government Resolution on Enhancing Information Security in Central Government (26 November 2009), one of the development priorities is preventive measures and contingency planning. According to the Decree on Information Security in Central Government (681/2010), which came into force on 1 October 2010, every central government organisation must achieve the base level of information security by 30 September 2013. The base level of information security includes procedures in exceptional situations.

These instructions are directed at public sector actors as well as companies in a service agreement relationship with the public sector. The purpose of the requirements is to harmonise key functions with respect to the contingency planning of both the public sector and the private sector. This improves the capacity of services provided and accessed via electronic networks to withstand disruptions and promotes the continuity and recovery of services in exceptional situations. These instructions enhance organisations' contingency planning for information security and cyber threats.

Central government organisations must take into account the ICT contingency planning requirements outlined in these instructions. The requirements should be extended to the central government's internal and external service providers. In procurement preparations and calls for tender concerning individual systems, it is essential to take into account contingency planning requirements.

Guided by the ministries, the administrative branches and agencies should specify for each organisation, service and system the level of contingency they require. Organisations should establish a timetable for the implementation of services in accordance with the contingency levels as well as the adequate resourcing of implementation as part of normal operational and financial planning.

Minister of Public Administration
and Local Government

Henna Virkkunen

Government IT Director

Mikael Kiviniemi
VAHTI Chairman

Enclosed: Instructions on Requirements for ICT Contingency Planning (VAHTI 2/2012)
FOR INFORMATION: Municipalities

VAHTI in brief

The Ministry of Finance is responsible for steering and reconciling the development of public sector, and particularly central government, information security in Finland. The Government Information Security Management Board (VAHTI), which has been established by the Ministry of Finance, is responsible for steering, developing and coordinating central government information security. VAHTI handles all significant central government information security policy and information security guidance matters. In its work, VAHTI supports the Government and the Ministry of Finance in decision-making and also in the preparation of decisions relating to central government information security.

VAHTI's objective is, by developing information security, to improve the reliability, continuity, quality, risk management and contingency planning of central government functions and to promote information security so that it becomes an integral part of central government activity, steering and performance guidance.

VAHTI promotes the implementation of the Government Programme, the Decree on Information Security in Central Government (681/2010), the Security Strategy for Society, the Government IT Strategy, the Government Resolution on Security of Supply, the National Information Security Strategy, the Government Resolution on Enhancing Information Security in Central Government and other key policy outlines of the Government.

On 26 November 2009, the Government made a Resolution on Enhancing Information Security in Central Government. The resolution emphasises VAHTI's position and tasks as the key body responsible for the steering, development and coordination of central government information security. In accordance with the resolution, the administrative branches allocate resources for the development of information security and for cooperation coordinated within VAHTI.

VAHTI acts as the cooperation, preparation and coordination body of central government organisations responsible for the central government's development and steering of information security and data protection, and promotes the development of networked operating practices in public sector information security work.

VAHTI's work has improved central government information security, and the effectiveness of its work is evident not only in central government but also in the business sector and internationally. The result is a very comprehensive set of general information security instructions (www.vm.fi/vahti and www.vahtiohje.fi). Led by the Ministry of Finance and VAHTI, a number of joint information security projects have been implemented with ministries and agencies as well as an extensive central government information security development programme.

For three years in succession, VAHTI has been recognised with an award for its exemplary work in improving Finland's information security.

Contents

1 Introduction

Contingency planning means all of the administrative, operational and technical measures and solutions by which the availability of information and the undisturbed provision of services is ensured. It also covers recovery from disruptions in accordance with service agreements and as specified by service levels

ICT contingency planning ensures continuity of ICT activity and safeguards information through risk management during exceptional situations in normal circumstances as well as in emergencies.

These instructions are directed at public sector actors as well as companies in a service agreement relationship with the public sector. Uniform requirements are established to harmonise functions which are of key importance to the contingency planning of both the public and private sectors. This improves the capacity of services provided and accessed via electronic networks to withstand incidents and promotes the continuity and recovery of services in exceptional situations. They help organisations in contingency planning for information security and cyber threats.

Guided by the ministries, the administrative branches and agencies should

- specify for each organisation, service and system the level of contingency planning they require;
- establish a timetable for implementing services in accordance with the specified contingency planning level;
- arrange resources for implementation as part of normal operational and financial planning.

1.1 Chapter guide

These instructions describe the key principles for the management and implementation of ICT contingency planning. They replace the General Instructions on ICT Contingency Planning (VAHTI 2/2009).

This document is meant for management responsible for operational planning. The most important issues for senior management are presented in text boxes. Chapter 4 presents for each subarea the general requirements that must be fulfilled in an organisation's activities and supporting services. After each requirement, an explanation is given of what the requirement means and what it improves from the perspective of contingency planning.

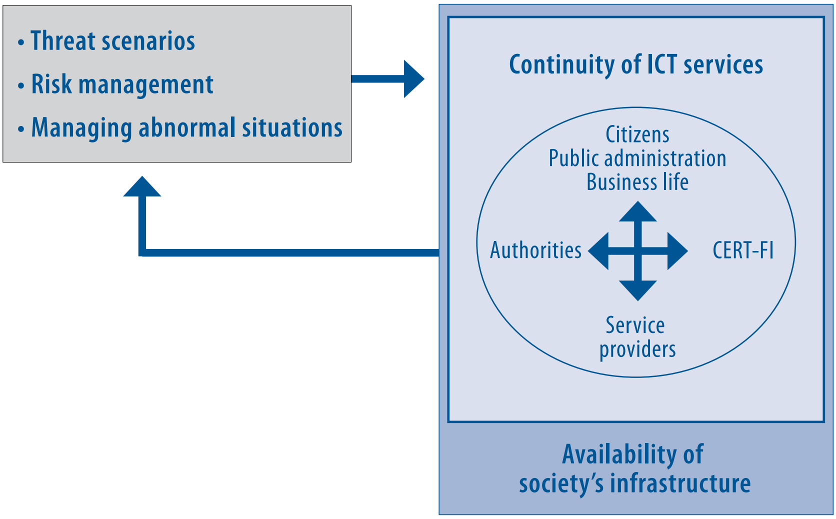
The requirement cards in Appendix 1 are intended for actors responsible for service and system implementation and for ICT contingency planning. They describe in more detail the base-level, increased-level and high-level requirements, specifying each general requirement. The cards also give for these requirements examples of possible implementation of the requirement or explain what is being sought through the implementation of the requirement.

1.2 Justifications

Contingency planning for exceptional situations in normal conditions is part of the good information management practice of every organisation. The normative basis for contingency planning in emergencies consists of the emergency powers act (Valmiuslaki 1552/2011) and Government Decision 539/2008 on objectives for security of supply. The emergency powers act obliges public authorities to undertake contingency planning. In addition, the Government Resolution on Enhancing Information Security in Central Government (2009) as well as the Security Strategy for Society (2010) play a key role in steering contingency planning and in specifying requirements. The strategy prescribes the vital functions of society that must be secured in exceptional situations in normal conditions and in emergencies. Strategic tasks have been specified for administrative branches with respect to the management of vital functions. In addition to these, each agency and organisation may also have other critical services and tasks associated with their own activities.

The vital functions of society and their support services and systems form interdependent networks. Various government actors, citizens, organisations and businesses as well as information and communication technology service providers participate in service networks consisting of service users and maintainers. Services are dependent on the smooth functioning of society's ICT infrastructure. The continuity of ICT services is ensured by the interaction of public authorities, customer organisations and service providers as well as through the application of common operating principles and procedures.

Figure 1: ICT contingency planning means cooperation across the whole society



It is essential to ensure that the entire service network is able to continue to operate in accordance with set requirements in various exceptional situations in normal conditions and in threat scenarios outlined in the Security Strategy for Society.

From all parts of the network, this requires consistent protection of information at agreed levels as well as the ability to continue operations and services in exceptional situations in normal conditions and in emergencies.

Society's vital functions:

- Management of Government affairs
- International activity
- Finland's defence capability
- Internal security
- Functioning of the economy and infrastructure
- The population's income security and capability to function
- Psychological crisis tolerance

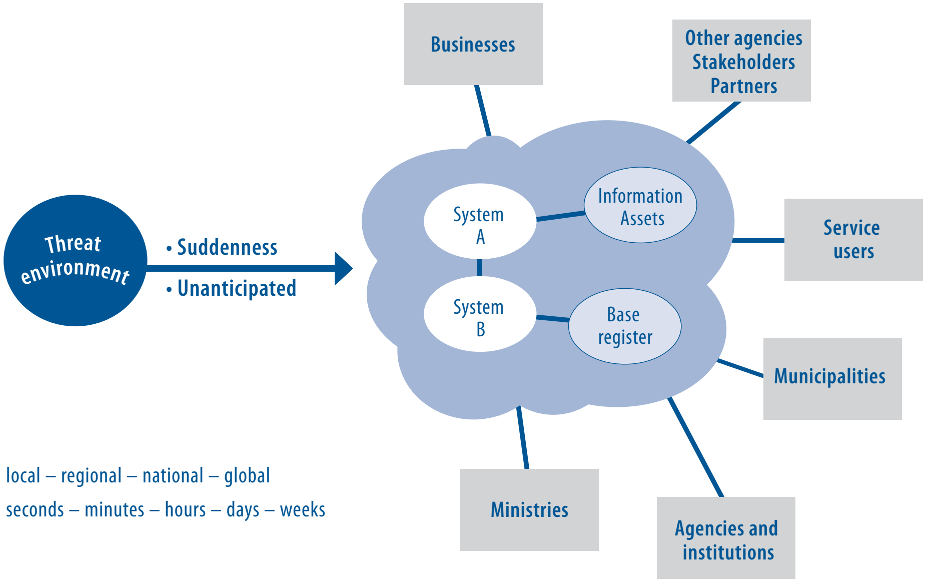
1.3 Security environment for ICT contingency planning

The functions vital to society are the indispensable intersectoral functional entities of society which have to be secured in all situations. Changes in the surrounding society, public administration and the threat environment influence opportunities to provide the services required by vital functions and they should also be taken into consideration in contingency planning needs for services.

From the perspective of ICT services, the most important trends in society are:

- Services, processes, production chains and systems are becoming highly automated, diversified, integrated and networked.
- Information sharing is expanding and becoming more automated.
- Services are being acquired from a service network consisting of many suppliers.
- ICT service chain ownership and contractual relationships are constantly evolving.
- The significance of international cooperation and control is growing strongly.
- The threat environment and threats are becoming more unexpected, professional and serious.

Figure 2: Interoperability of service network and systems is critical in managing abnormal situations



Disruptions may occur in both normal conditions and emergencies. Systems and contingency planning measures built in normal conditions provide the basis for measures in emergencies.

The threat scenarios of the Security Strategy for Society form a foundation for the planning of joint and integrated service network action in cooperation with public sector actors, businesses and organisations. Different actors can utilise the standardised material when preparing detailed threat assessments of their own fields and when evaluating the effects arising from threats on services.

Society today, with its IT-based services, is part of the cyber environment and also susceptible to the threats associated with it. The sudden realisation of threats is typical of the information technology operating environment, as is the rapid and unpredictable expansion of the effects of resulting disruptions. They may affect the information technology assets directly or have an indirect impact on support structures (for example staff). A disruption may arise from a natural phenomenon, an accident, a power outage, an information system error, a quality defect, a telecommunications failure, an equipment fault, an operational or access error, or a communications problem.

A disruption may also be caused intentionally, such as by malicious damage, vandalism or a cyber attack (targeted at equipment and systems).

Requirements for contingency planning are derived from an analysis of an organisation's tasks, activities and operating environment in relation to threat scenarios. Measures for the prevention and management of disruptions as well as the development of capabilities in relation to them are also formulated on the basis of the analysis. The strong development of the cyber environment, in particular, with its constantly evolving threats creates the need for the continuous assessment and development of contingency planning.

2 Structure of contingency planning requirements

2.1 Formation of requirements

The information management act (Laki julkisen hallinnon tietohallinnon ohjauksesta 634/2011) requires public sector authorities to plan and describe their enterprise architecture to facilitate and ensure the interoperability of public sector information systems. The Act also obliges public sector organisations to comply with interoperability descriptions and specifications, and imposes on the Ministry of Finance a steering and coordination requirement.

The Government Resolution on Enhancing Information Security in Central Government (26 November 2009) sets out guidelines for central government to enhance information security as a key aspect of leadership and management, competence, risk management, and administrative reforms and activities. In accordance with the resolution, the specification and implementation of the levels of information security, contingency planning, and protection is based on not only statutes and each organisation's individual objectives but also on the overall guidelines and recommendations on information security and contingency planning levels issued by the Ministry of Finance.

The purpose of uniform requirements is to harmonise key functions in the contingency planning of both the public and private sectors. This also promotes the continuity of services in various exceptional situations.

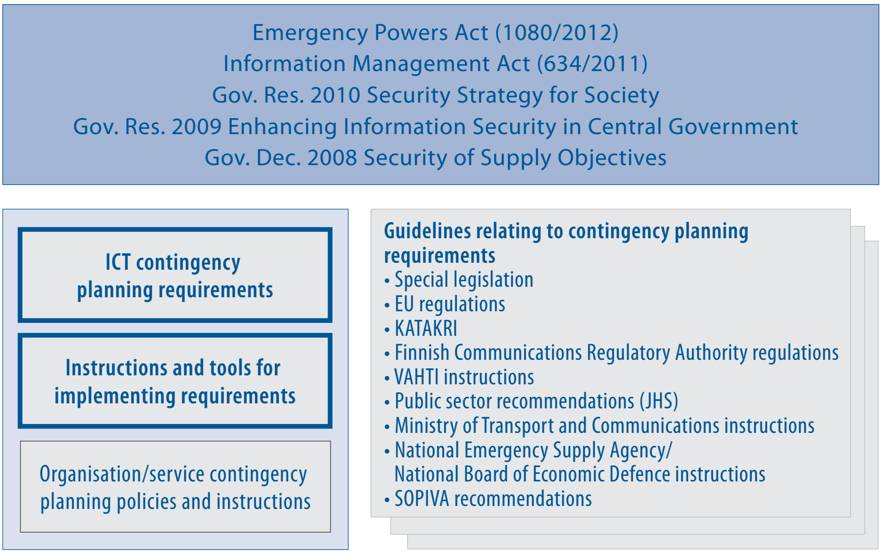
In the preparation of contingency planning requirements, EU and central government guidelines and regulations on continuity management and information security have been taken into account. These instructions also specify measures by which the ICT contingency planning requirements can be implemented. The key instructions concerning ICT contingency planning are listed in Appendix 2.

The contingency planning requirements (VARE) and the requirements of the Decree on Information Security in Central Government are primarily targeted at public sector organisations. The SOPIVA (contract-based contingency planning) recommendations and the HUOVI contingency planning self-assessment tool have been prepared for the use of companies critical for security of supply.

The main target group of the National Security Auditing Criteria (KATAKRI) is the public and private sector organisations or their information systems and telecommunications arrangements which have been the subject of a corporate security clearance and which handle international, security-classified information material.

The KATAKRI criteria may be used, where applicable, particularly in increased-, high- and special-level ICT contingency planning services to verify the fulfilment of requirements relating to the accessibility of information and services as well as premises security.

Figure 3: Legislation and guidance directing ICT contingency planning



Emergency Powers Act (1080/2012)
Information Management Act (634/2011)
Gov. Res. 2010 Security Strategy for Society
Gov. Res. 2009 Enhancing Information Security in Central Government
Gov. Dec. 2008 Security of Supply Objectives

ICT contingency planning requirements

Instructions and tools for implementing requirements

Organisation/service contingency planning policies and instructions

Guidelines relating to contingency planning requirements

- Special legislation
- EU regulations
- KATAKRI
- Finnish Communications Regulatory Authority regulations
- VAHTI instructions
- Public sector recommendations (JHS)
- Ministry of Transport and Communications instructions
- National Emergency Supply Agency/ National Board of Economic Defence instructions
- SOPIVA recommendations

2.2 ICT contingency planning requirement levels

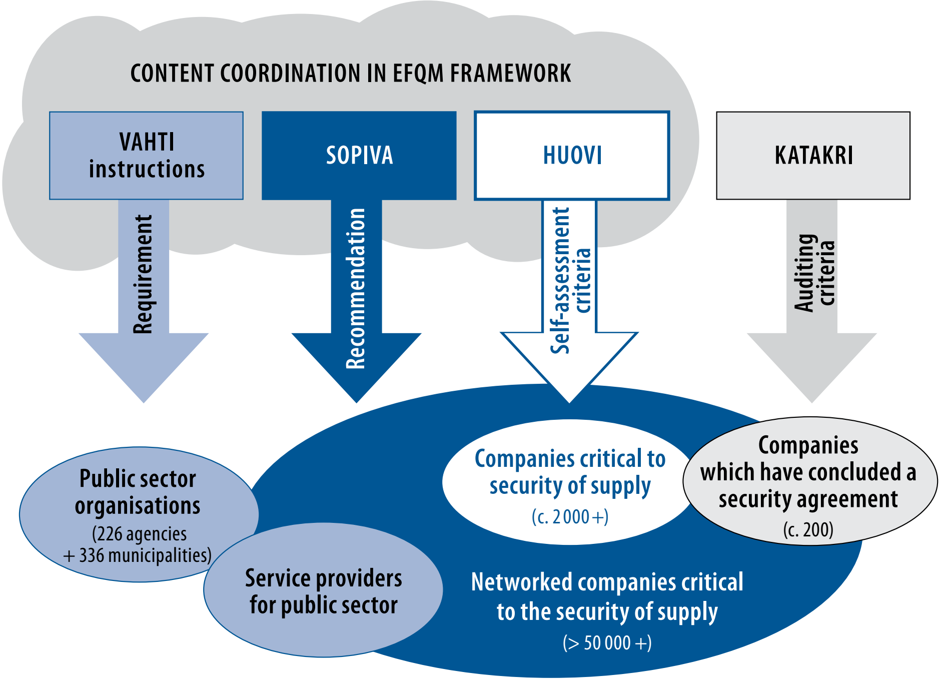
2.2.1 Formation of requirement levels

ICT contingency planning requirements are set for an organisation's activities and services, and for the implementation of ICT systems and services. The generally applied EFQM[1] and CAF[2] quality assessment models have been used as a reference framework, and the requirements are compatible with the ISO standards 27001 and 22301.

[1] The EFQM (European Foundation for Quality Management) forms a reference framework for enhancing competitiveness and quality while not aiming explicitly to direct what kind of practices organisations should apply. The model used is the assessment basis of the European Quality Award and the Finnish Quality Award.

[2] The CAF (Common Assessment Framework) is a quality assessment model for pubic sector organisations jointly developed by EU Member States.

Figure 4: Criteria directing ICT contingency planning and information security


CONTENT COORDINATION IN EFQM FRAMEWORK
VAHTI instructions
SOPIVA
HUOVI
KATAKRI
Requirement
Recommendation
Self-assessment criteria
Auditing criteria
Public sector organisations
(226 agencies + 336 municipalities)
Service providers for public sector
Companies critical to security of supply
(c. 2000+)
Companies which have concluded a security agreement
(c. 200)
Networked companies critical to the security of supply
(> 50 000 +)

The basic requirements that form the framework of the requirements are consistent with the SOPIVA recommendations and with the HUOVI maturity assessment model prepared under the guidance of the National Emergency Supply Organisation as well as with the Instructions on Implementing the Decree on Information Security in Central Government (VAHTI 2b/2010). The Decree on Information Security in Central Government specifies requirements relating to the processing of information by public authorities from the perspective of confidentiality. ICT contingency planning requirements focus on the availability of information and services.

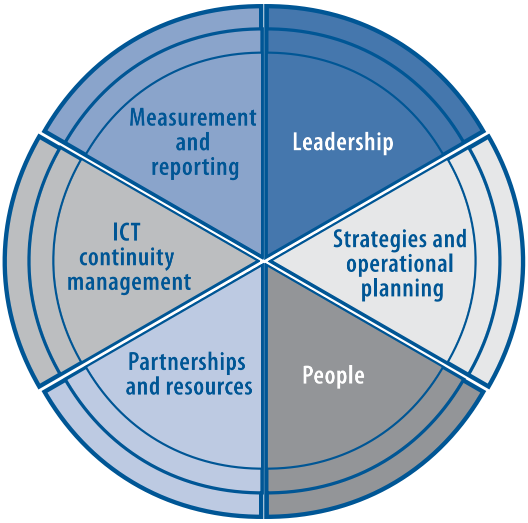
The ICT contingency planning requirements have been grouped into 6 sections. Sections 1–4 contain requirements relating to the maturity of an organisation or activity from the perspectives of strategic management, operational planning, human resources management and partnership network management. They are intended to integrate the management of ICT contingency planning into an organisation's normal activities. This contributes to safeguarding the continuity of operations and services and the availability of information as part of the service network, also in exceptional situations. Section 5 sets requirements for various technical systems, processes and solutions, and section 6 for the internal and external measurement of operations.

Contingency planning requirements are general requirements that describe the measures to be implemented in support of contingency planning. They are amplified by base-level, increased-level and high-level requirements, which provide instructions for implementation.

The purpose of the requirements is to provide guidance for organisations to develop their activities, the services they provide and the systems they own in an appropriate manner, to prepare contingency plans for various threats, and to prevent disruptions from arising.

When a system or service is procured, it is essential to verify that the asset to be procured fulfils the contingency planning requirements set for it.

Figure 5: ICT contingency planning requirements are grouped into six categories and three levels


Measurement and reporting
Leadership
ICT continuity management
Strategies and operational planning
Partnerships and resources
People

2.2.2 Requirement levels

The ICT contingency planning levels also aim to standardise contingency planning measures, so that in networked activities based on partnership and confidence it would be possible to recognise the ability of each party to withstand disruptions.

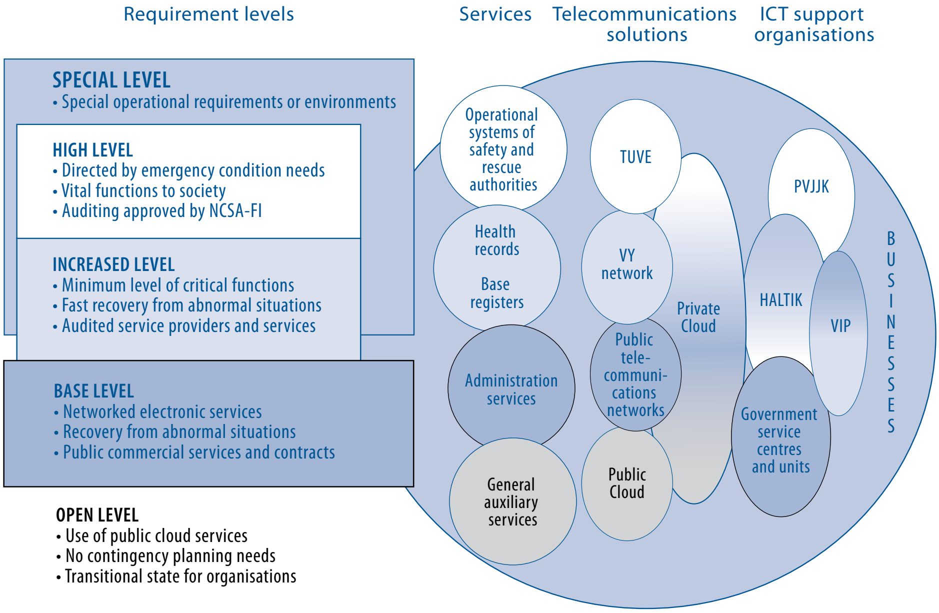
An organisation's functions and services are placed on information security and contingency planning levels in accordance with their needs. Each service may be on the base level for information security and on the high level for contingency planning or vice versa. Achieving an increased or high level of ICT contingency planning, however, also requires the fulfilment at least of the base level of information security.

A public authority may, on the basis of its risk analysis, also decide to fulfil certain requirements in a particular service. The selected level may also be implemented with individual additional requirements from the higher levels, for example, to improve the accessibility of a system in the event of evaluated threats. A system's availability requirement may also be raised temporarily to a higher service level for the duration of time-restricted events that are known in advance. This matter must be included in service agreements and processes.

On all ICT contingency planning levels, a public sector service may be implemented either by the organisation itself, public sector service providers or private sector service providers. On the high contingency planning level, specific assurances should be obtained that the service provider's fault correction expertise and availability are adequate for all disruptions possible in different threat scenarios.

Public sector services are placed on ICT contingency planning requirement levels mainly according to Figure 6 on the following page.

Figure 6: ICT contingency planning requirement levels


Requirement levels
Services
Telecommunications solutions
ICT support organisations
SPECIAL LEVEL
• Special operational requirements or environments
HIGH LEVEL
• Directed by emergency condition needs
• Vital functions to society
• Auditing approved by NCSA-FI
INCREASED LEVEL
• Minimum level of critical functions
• Fast recovery from abnormal situations
• Audited service providers and services
BASE LEVEL
• Networked electronic services
• Recovery from abnormal situations
• Public commercial services and contracts
OPEN LEVEL
• Use of public cloud services
• No contingency planning needs
• Transitional state for organisations
Operational systems of safety and rescue authorities
Health records
Base registers
Administration services
General auxiliary services
TUVE
VY network
Public tele-communi-cations networks
Public Cloud
Private Cloud
PVJJK
HALTIK
VIP
Government service centres and units
BUSINESSES

Open level

In the development of an organisation's contingency planning, the open level is the starting point. The identification of the organisation's contingency planning needs and classification of services onto the various levels of ICT contingency planning have not been completed.

The organisation may also, after careful consideration, implement some of its services and systems on an open level, in which case these will not fulfil the ICT contingency planning requirements. They may be, for example, provided from public cloud services. The service may be, for example, added value service to the public that can be out of operation for long periods without an organisation's basic tasks failing to be fulfilled, and people can also obtain a corresponding service from elsewhere. In such services, the customer may not set special requirements concerning ICT contingency planning.

Every public sector authority must, however, achieve the base level of ICT contingency planning, even though some services do not as planned fulfil the base level requirements and are implemented on the open level.

Base level

The base level securely enables an organisation's normal, highly networked operations. Typically, most of the systems supporting administration, such as travel management systems, are placed on the base level. Moreover, services and systems whose momentary failure in exceptional situations does not suspend an organisation's core functions are also placed on the base level. Disruptions are overcome through standardised, normal service agreements corresponding to the organisation's operational requirements. Typically, the base level systems' main operational focus is during office hours, fault correction can be initiated on the working day following detection and target recovery time from the disruption may be during the next working day.

Fulfilling the base-level requirements of ICT contingency planning does not give rise to significant additional costs if the requirements are taken into account from the beginning in the development of an organisation's activities, services and systems. Services and systems already in use are transferred to the base level again in connection with procurement, system modifications and updates.

Base-level verification may be done through self-assessment or using external services.

Increased level

The increased level is intended for an organisation's critical functions. It is appropriate to implement only part of an organisation's operations, services and systems on this level. Services and systems that support the vital functions of society or are important for the public in exceptional situations can also be placed on the increased level. Increased-level systems include patient data systems and base registers in so far as public authorities' increased- and high-level services are dependent on them. In organisations that are central for the vital functions of society, a communications system for the management of crisis situations should also be placed at least on the increased level.

Contingency planning measures that prevent disruptions and fault-tolerant solutions have been introduced on the increased level. Increased-level systems have round-the-clock monitoring and the capability to initiate fault correction without delay. On the increased level, standby procedures may also be required of a user organisation, ensuring that it can decide on measures in exceptional situations.

If telecommunications links from Finland to countries abroad have failed, it is essential to ensure the operation of services and systems important for functions vital to society and for operating in emergencies. In such cases, it is justified to set special requirements for increased-level service providers, for example in relation to services produced abroad and their external audits.

In verifying the increased level, it is also recommended that an external party be used.

High level

The high level fulfils the contingency planning needs for large-scale disturbances and emergencies in accordance with Security Strategy for Society threat scenarios in functions requiring special security. High-level systems include the government security network (TUVE) and the operational systems of the security authorities. Services and systems that must operate round the clock and whose short service breaks would result in serious operational disturbances or very significant economic effects are placed on the high level.

The high level sets significant additional requirements for an organisation's activities, expertise and systems implementation. High-level systems fall within the sphere of continuous round-the clock monitoring, management and fault correction. High-level systems also require that customer and user organisations have the ability to make quick decisions in exceptional situations. On the high level, it is particularly important to ensure the operation of telecommunications and the availability of information, services, maintenance and expertise, and that these functions are performed under Finnish legislation, taking emergencies into account. Services placed on the high level must operate, even if telecommunications links to countries outside Finland were down. In high-level services, it must be separately specified which information is to be stored and which management measures concerning the criticality of operations or contingency planning for emergencies are to be implemented in Finland.

High-level systems should be built so that the destruction of one data centre or telecommunications link does not result in the failure of the system.

The services of a party approved by the National Communications Security Authority (NCSA-FI) should be used to verify high-level ICT contingency planning.

Special level

Critical functions, services and systems are placed on special level when the nature and the availability of the service requires high contingency level as well as measures deviating from common methods and solutions.

The placing of a system in the special level is decided by the relevant ministry and approved by the Ministry of Finance. Service and system audits are performed by NCSA-FI or a party approved by it.

3 Using the contingency planning requirements

3.1 Using the requirements in the public sector

With respect to ICT contingency planning, the Ministry of Finance is responsible for determining and setting contingency planning requirements, issuing instructions and guidelines, and steering implementation. The contingency planning requirements used in the public sector should cover the entire process, also across administrative boundaries. In cross-administrative processes, each part of a process must fulfil the approved requirements. Possible deviations permitted for a particularly compelling reason must be approved separately and discussed with all organisations dependent on the process. The foundation of contingency planning is that every organisation included in a process has fulfilled the base level of information security in accordance with the Decree on Information Security.

Each public sector organisation must assess for which of its services and systems the base level of contingency planning is sufficient and which require increased- or high-level contingency planning. This assessment should highlight the needs of stakeholders that use the service. As a rule, systems and services are transferred to the chosen level in connection with a system update or a procurement process or when the system reaches the end of its lifecycle.

Public authorities should record for their own activities, services and systems the desired contingency planning levels. They should also include a timetable and the resources for achieving the levels in performance guidance, operational and financial planning, and reporting.

The placement of central government joint services and systems on the increased or high level and the coordination of flows of information and processes across administrative boundaries should be determined in cooperation between the ministries, coordinated by the Ministry of Finance.

The ministries have a significant role in steering the contingency planning of their own administrative branch through performance guidance. Based on the proposals of their agencies, the ministries confirm which systems of their administrative branch are to be placed on the high level in connection with operational and financial planning, performance guidance and monitoring.

Public sector organisations should assess the level of their services and systems and, if necessary, issue accreditations in accordance with Ministry of Finance instructions.

3.2 Applying the requirements in procurement and service agreements

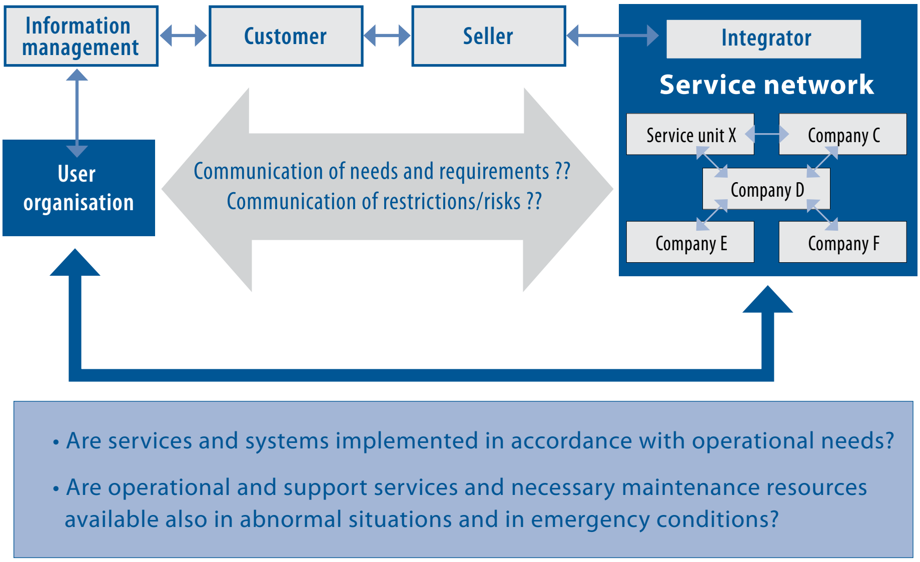
Every organisation is responsible for including the requirements in any invitations to tender and agreements. When preparing procurement and agreements, attention should be paid to which requirements are suitable as they are and which should be modified due to the nature of the procurement, so that they can be made binding on the service providers.

The Ministry of Finance specifies at an early stage the common binding requirements to be applied in procurement. These should also be included as far as possible in public sector joint framework agreements. Each organisation may in its own competitive tendering and framework agreements specify the binding requirements relating to the target of procurement if required by the service being purchased or its own operations.

Each organisation must ensure in its service agreements that the requirement level set for a service is conveyed in the procurement chain from the service provider to the network that participates in providing the service. Similarly, steps should be taken to ensure that any restrictions or residual risks inherent in the service are communicated to the service customer and user organisations.

The obligation to comply with the base level must also extend to subcontracting terms and to the partnership network. This procedure promotes the improvement of operational continuity in the key business network. Agencies should ensure that requirements are set for external and internal contractual partners and they in turn impose these requirements on their subcontractors.

Figure 7: Contingency planning requirements must be conveyed across the service procurement chain



- Are services and systems implemented in accordance with operational needs?
- Are operational and support services and necessary maintenance resources available also in abnormal situations and in emergency conditions?

Compliance with base-level and, if necessary, higher-level contingency planning requirements should be recorded in framework agreements and service agreements.

No requirements should be added to valid agreements during the agreement period otherwise than for particularly weighty reasons.

3.3 Applying the requirements for service providers

Contingency planning requirements should be extended to the public sector's internal and external service providers. The way the requirements are implemented may differ between the operators, as long as the desired objective is fulfilled in the said service or procurement and interoperability in networked operations is maintained.

Companies' contingency planning for disruptions in normal conditions and for emergencies is based as a rule on their business needs, statutory obligations and requirements specified in agreements. Companies may, on their own initiative, introduce the SOPIVA contingency planning management recommendations to support their business needs. Companies may also apply these contingency planning requirements in their own operations and in the contractual arrangements of their partnership networks. From the perspective of companies, the uniform setting of requirements for central government actors will simplify and standardise the fulfilment of customer requirements and provide a good tool for managing a company's own subcontractor and partnership network.

Companies providing a service to the public sector may be required to fulfil contingency planning requirements set in procurement and agreements for the service they sell and for related service provision. The implementation of increased- and high-level requirements may be restricted, if necessary, only to the unit that provides or maintains services of the level in question.

If a certain way of implementing requirements is for some special reason not prescribed in an invitation to tender, the company may if it so wishes also employ company-specific methods. In such cases, the company should state how the prescribed requirement will be fulfilled using the means employed by the company and propose a solution acceptable to the customer.

4 Contingency planning requirements

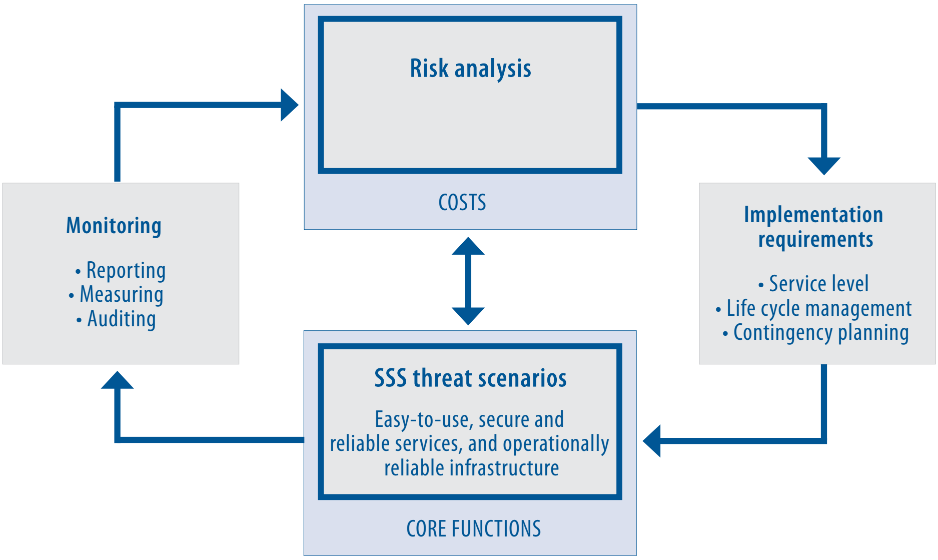
4.1 Leadership

Exceptional situations that threaten functions vital to society are generally managed according to the management code for normal conditions. In serious situations, crisis management models in accordance with the Security Strategy for Society are applied.

The support of the organisation's management is decisive when developing the operational reliability of the organisation and its services. Management's role is to create the appropriate conditions for the organisation's activities to continue in all exceptional situations.

Management decides on the objectives and policy outlines of contingency and continuity planning, and approves resources on the basis of a prepared development plan. The organisation's core operations must function in all exceptional situations outlined in the threat scenarios of the Security Strategy for Society.

Figure 8: ICT contingency planning and implementation process



Risk analysis

COSTS

Implementation requirements

- Service level
- Life cycle management
- Contingency planning

SSS threat scenarios

Easy-to-use, secure and reliable services, and operationally reliable infrastructure

CORE FUNCTIONS

Monitoring

- Reporting
- Measuring
- Auditing

To support this, the organisation needs easy-to-use, reliable and secure services, and an operationally reliable ICT infrastructure. Requirements for ICT services as well as an ICT contingency development plan are based on assessments of operational needs and risk and cost-benefit analyses. Feedback obtained through measurement and reporting is used to develop services and ICT contingency planning as part of normal operational and financial planning.

Internal communication is used to make staff better aware of the aims and significance of continuity management for the organisation's activities and for individual employees in all situations.

4.1.1 Strategic control

The key task of strategic control is to determine the contingency planning needs of the organisation and services and to integrate contingency planning into performance guidance as an essential part of each organisation's management as well as its operational and financial planning and implementation.

Requirement 1.1:

The organisation takes into account the legislation related to its activities and services and other standards steering ICT contingency planning, and these are implemented through contingency planning policies and actions.

- To fulfil its obligations, the organisation must be aware of their existence. Legislation and standards determine the minimum level for the implementation of ICT contingency planning. In addition, the organisation must take into account needs arising from the special characteristics of its activities. Understanding the internal and external interdependencies of functions is an absolute prerequisite for the cost-effective management of contingency planning. Management must ensure that subordinate organisations and units are clearly informed of their assignments and duties in emergencies.

Requirement 1.2:

ICT contingency planning policies have been specified based on the requirements set by the organisation's activities.

- Core functions and their support systems must operate as smoothly as possible in exceptional situations. Contingency planning measures must be scaled and targeted in accordance with operational needs. A useful working method is a Business Impact Analysis (BIA).

4.1.2 Organisation

Contingency planning should be organised as part of normal activity, based on the rules of procedure and task descriptions, so that responsibilities for steering and operating models remain as far as possible unchanged in exceptional situations and emergencies. The organisation's senior management prioritises the measures to be undertaken.

Requirement 1.3:
Incident management has been outlined, organised and taken into account in steering models.

- It is important to be able to make decisions and act quickly and effectively. This is possible when clear management responsibilities are known to all parties.

Requirement 1.4:
ICT contingency planning has been organised and responsibilities assigned as part of normal management, operations and partnership network management.

- Cost-effective action requires that all parties attend to the contingency planning of their own activities in accordance with common policies.

Requirement 1.5:
Sufficient resources for the objectives have been allocated to contingency planning and continuity management.

- The target level should be realistic, and sufficient resources should be allocated to achieving it. Only agreed and tested contingency planning measures help in preventing disruptions and in recovering from them. Specification of objectives and resources should be integrated into operational and financial planning.

Requirement 1.6:
Contingency planning and continuity management planning are implemented as a joint effort of core and support functions.

- Senior management appoints the staff members to implement cooperation. Cooperation is necessary so that the support functions essential for the core functions can also be taken into account in continuity planning, and so that the implemented measures are in line with each other.

4.1.3 Cooperation, communication and reporting

The organisation's management should make the reporting of ICT contingency planning an integral part of the donut dial for annual planning of management group and cooperation meetings. Management should also issue policy outlines and assign responsibilities for internal and external communications in exceptional situations as part of the implementation of operational continuity

Requirement 1.7:
The organisation's management monitors the development of contingency planning and cyber security as well as continuity planning, and the impacts and costs of these measures.

- The organisation's management is responsible for the functional capacity of services in exceptional situations. Management should steer contingency planning as part of management group working and demand adequate and explicit information about the state of ICT contingency planning to support decision-making. Continuity management cannot be successfully implemented without the commitment of management.

Requirement 1.8:
Communication and reporting responsibilities and processes have been specified and organised with key stakeholders.

- Due to outsourcing and the networked operating approach, organisations are dependent on their key stakeholders in safeguarding the continuity of their operations. Flow of information must work across organisation boundaries. It is essential to ensure the immediate communication of incidents and disruptions that affect services.

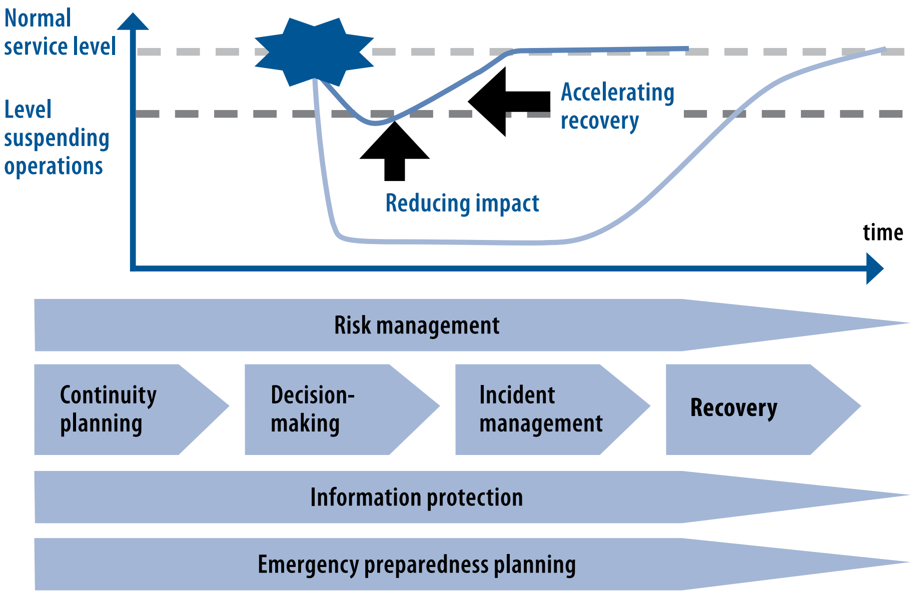
4.2 Strategies and operational planning

Statutory obligations must be taken into account when developing ICT contingency planning. Planning to safeguard the continuity of operations and services should be implemented as part of operational and financial planning. In operational planning, particular attention should be paid to the dependency of services on other services and other operators and on the created operational chain and network.

Risk management should be integrated into operational planning. When threat assessments are made as part of risk management, threat scenarios based on the Security Strategy for Society should be used. The organisation's risk analysis covers both the internal and external operating environment. The analysis of critical tasks comprises the operational risks of the organisation and its stakeholders. The development of contingency planning and continuity management is based on prioritisation of risks related to core and support functions.

It is important to specify the desired service level for each service. The level below which a service is no longer viable for the organisation using the service should also be identified. Acceptable measures by which the impact of disruptions can be minimised and the recovery of services can be accelerated to conform to service level requirements should be specified for each service.

Figure 9: ICT contingency planning is implemented through continuity management process



The organisation should have documented the contingency planning principles by which ICT contingency planning, continuity management and information security are implemented. Contingency planning can also be part of an organisation's emergency preparedness planning, implemented according to the Emergency Powers Act and the Rescue Act. Continuity planning includes contingency planning and recovery planning. It is essential to identify the correct order of measures from an effectiveness perspective. Public authorities, organisations that use and provide services, and the services themselves must fulfil at least the base level of information security according to the Decree on Information Security.

Continuity planning should be done in cooperation with service providers. Every service provider is bound by agreed measures. The special characteristics of activity in emergencies are taken into account in emergency preparedness planning, which can be implemented as part of normal continuity planning.

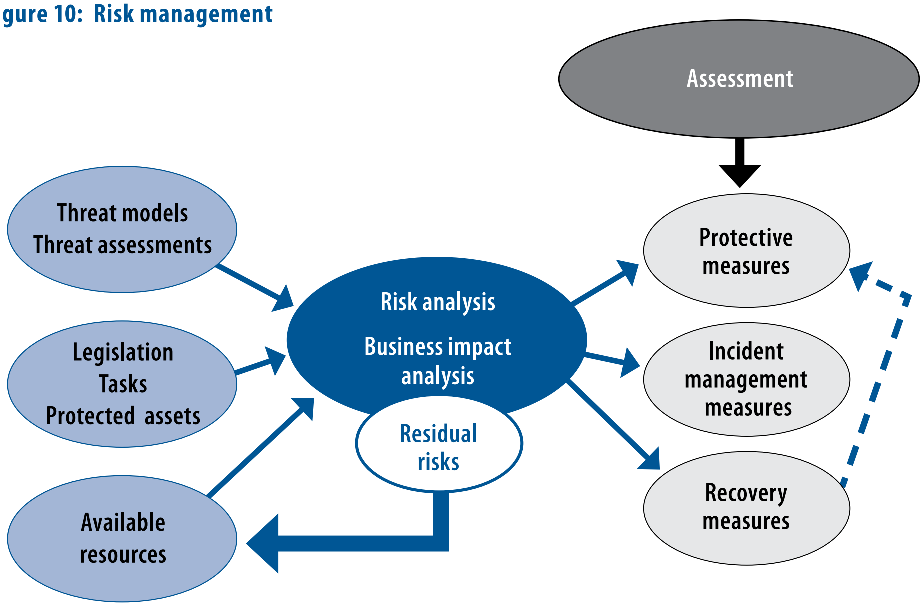
4.2.1 Operational planning through risk management

Risk management is used to scale and target contingency planning measures and resources appropriately to enhance the organisation's operations and its capacity to withstand disruptions.

In risk management, the significance of each service and system should be recognised for the organisation's own activities and for functions vital to society. In addition, an assessment should be made of the impact of threats – (including information and cyber security threats) outlined in threat scenarios – on the operation of services and systems. Services and systems should also be classified according to their criticality, so that corrective measures can be prioritised and targeted in exceptional situations.

The systematic assessment of threats is essential in risk management. It is also important to evaluate the tasks and requirements assigned to the organisation as well as the available resources. Based on them, it is possible to determine the most effective measures for ICT contingency planning (Figure 10).

Figure 10: Risk management



Requirement 2.1:
In operations, the interaction of the organisation and the operating environment should be taken into account.

- The operating environment and changes in it affect the organisation's operating capacity. Through interaction, the organisation can anticipate and influence matters affecting its activities.

Requirement 2.2:
The results of risk management direct the development of contingency planning.

- Through risk management, development measures can be targeted where the achieved benefit is greatest.

4.2.2 Service continuity planning

Organisations should identify the services and systems that need contingency planning measures, plan the necessary measures and arrange round-the-clock monitoring of important systems.

Requirement 2.3:
Contingency planning measures support the objectives of the organisation's core operations.

- Continuity management and information security are not ends in themselves; they must serve the organisation's activities.

Requirement 2.4:
Incident management and emergency procedures have been documented, training given and exercises held.

- Clear instructions and exercises create the preconditions for effective action in exceptional situations and facilitate, if necessary, the rapid application of documented processes in new types of situation. Contingency planning for disruptions in normal conditions also serves as a foundation for action in emergencies. If the organisation must make changes in emergencies to operating processes and services, these should be prepared during normal conditions.

Requirement 2.5:
Round-the-clock activity and CERT-FI cooperation should fulfil the organisation's objectives and obligations.

- Round-the-clock monitoring of important assets and CERT-FI cooperation are needed to ensure sufficiently fast reaction to threats. These are also important for the formation of the central government's situation picture.

4.3 People

The critical areas of special expertise required by the organisation’s core functions should be taken into account in the skills requirements of staff, training, service procurement and resourcing. Key staff members responsible for critical tasks are trained to be able to act in exceptional situations. The availability of human resources and expertise in exceptional situations and emergencies should be secured. An essential factor is ensuring the exemption of key staff from military service (VAP in Finland) in one’s own organisation and in the service provider network and subcontracting chains.

Strategic planning should also include anticipation of disruptions as well as contingency planning for special situations and emergencies. Risk analysis is directed at both the internal and external operating environment. The analysis of operational risks of the organisation and its stakeholders concerns their critical functions. Prioritisation of core and support functions’ risks directs the development of continuity management.

Statutory obligations must be taken into account in the development of continuity management and contingency planning for emergencies. The organisation’s management assesses the consequences of actual disruptions and decides on what measures should be taken to improve the operational processes.

4.3.1 Developing expertise and awareness

The organisation should specify the key requirements of contingency planning, continuity management and information security tasks and systematically enhance its expertise.

Requirement 3.1:
Role- and task-specific requirements have been set for ICT contingency planning expertise, its level is known, and it is developed.

- An essential prerequisite for continuity management and information security is that staff have sufficient expertise for their tasks and responsibilities. Skills shortages undermine productivity.

Requirement 3.2:
The organisation encourages staff to observe and develop good continuity management and information security procedures.

- Motivated staff produce good results effectively with less direction and monitoring.

Requirement 3.3:
The organisation has agreed a procedure for monitoring and handling security incidents and cases of misuse.

- Clear rules prevent misuse and ensure that the rights of staff and other parties are observed also if a staff member is suspected of misuse or has violated the rules.

4.3.2 Management of human resources and tasks

Risks arising from loss of key staff should be systematically reduced in the organisation and the availability of expertise ensured also in exceptional situations.

Requirement 3.4:
Key roles and people have been identified and back-up arrangements planned.

- Back-up arrangements are essential for ensuring that operations continue also when key staff are unavailable.

Requirement 3.5:
Staff have been hired and their roles have been planned and scaled in the manner required by the continuity management and information security of the organisation's core functions.

- If there are too few staff or their level of expertise does not fulfil requirements, some tasks will be performed poorly or not performed at all. Continuity of core functions must not be compromised under any circumstances.

4.4 Partnerships and resources

Central government internal and external service providers should fulfil the contingency planning requirements set for the service in question. The procuring organisation approves the procedures and technical solutions which satisfy the contingency planning requirements set for the service in the invitation to tender and specified in the contract negotiations. It also supervises their implementation and reporting. For each service, a coordinating person should be appointed to be responsible for ensuring that the partners and service provider networks are capable of recovering from incidents and disruptions. The coordinator may be from the organisation procuring the service or from a named partner.

The Ministry of Finance prepares, maintains and coordinates a list of shared public sector ICT contingency planning requirements to be included in procurement contracts. Those requirements from the list, which relate to the procured asset and are in accordance with legislation, are applied to each procurement contract.

When service suppliers and technologies are selected, the availability of maintenance services, resources and spare parts in exceptional situations and emergencies should be ascertained as required by the nature of the services.

4.4.1 Contract management

The contingency planning obligations in agreements cover the whole subcontracting chain and service provider network, taking into account the nature of each service provided and the role of the contracting parties in the provision of the service.

Requirement 4.1:

The partners, subcontractors and resources necessary for the organisation's activities have been identified.

- In networked activities, each party has obligations based on its significance in the cooperation. The key parties must be identified so that requirements incurring costs can be set only to those contractual partners on whom activities depend.

Requirement 4.2:

Agreements include requirements for contingency planning, continuity management and information security as well as their implementation.

- The requirements ensure that the contractual partner has understood the needs of the service and will provide the service as agreed. In critical services, the invitation to tender should specify the contingency planning requirements and possible special need for action in "force majeure" situations. At the contract stage, the partners must jointly agree which contingency planning measures are acceptable, fulfil the requirements and ensure that the service will be maintained in a manner possible also in "force majeure" situations.

4.4.2 Securing operations in special situations

Procedures and responsibilities in exceptional situations are agreed with the partner and service provider network.

Requirement 4.3:

The obligation to manage the continuity of critical operations and information security has been extended to the key supplier network.

- • It is not sufficient that an individual link of the service provider chain ensures continuity, because a chain is only as strong as its weakest link.

Requirement 4.4:

Cooperation with partners to manage disruptions has been organised and responsibilities assigned.

- Cooperation across organisation boundaries may be difficult, even in normal conditions – in a tight spot, the organisation must be able to act quickly and cannot afford problems with cooperation.

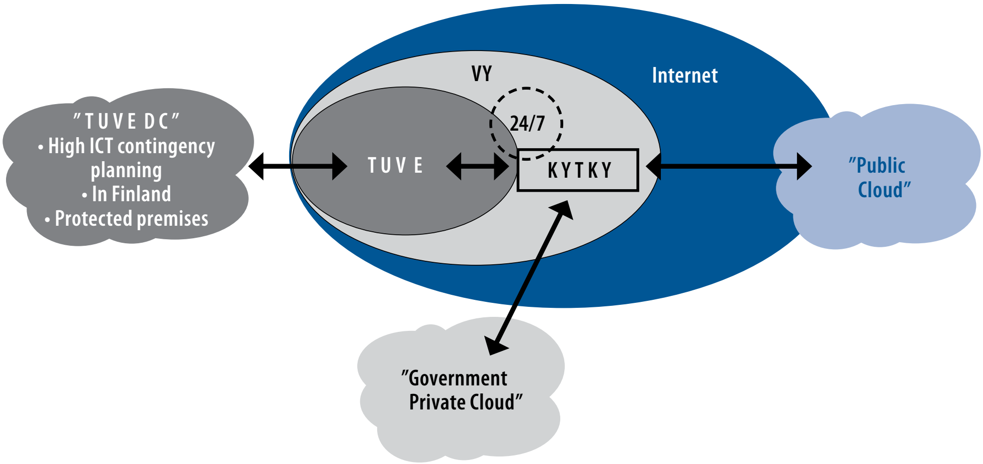
4.5 ICT continuity management

In public sector services, preparations should be made for events according to the threat scenarios of the Security Strategy for Society, and the continuity required by the nature of the organisation's activities must be secured in exceptional situations.

Information security (confidentiality – integrity – availability), contingency planning and cost-effectiveness should be given equal attention in society's information system solutions. For ICT contingency planning and interoperability, it is important to form service entities in which the maintainers and providers can be both public sector organisations and businesses, either together or separately. An example of the procurement of services on various levels is presented in Figure 11.

Service providers are responsible for the availability of the services and systems they maintain in accordance with the agreed service level. The operational requirements set by the owners are taken into account in the service levels. Taking threat factors into account, the implementation method and process for ICT contingency planning are described, implemented and tested, and training is organised.

Figure 11: Contingency planning and various network structures are taken into account when services are procured and implemented



4.5.1 Lifecycle management of ICT services and systems

The cost-effective implementation of fault-tolerant services requires that ICT contingency planning requirements are assessed and implemented at all stages of a system's lifecycle.

The threat scenarios and contingency planning of the Security Strategy for Society should be taken into account in the service architecture and lifecycle management. When developing their services, public sector authorities should take into consideration the service-level and recovery-time requirements set for the service as well as the need to control and prioritise the use and maintenance of their services in serious disruptions and emergencies affecting society. ICT contingency planning should be taken into account in the enterprise architectures of the public sector.

Requirement 5.1:
ICT contingency planning requirements are taken into account in ICT service lifecycle stages.

- Developing and acquiring secure and reliable systems is more cost-effective and productive than readjusting systems later. When ICT contingency planning requirements are taken into account at an early stage, the service will be more cost-effective.
- Disruptions and costs arising from the realisation of threat scenarios can be reduced, and continuity and fast restoration of services are ensured by means of architecture and technology solutions particularly in high-level systems.

4.5.2 Ensuring the continuity of ICT services

The information systems, databases and telecommunications of the most important services should be secured against incidents and network attacks.

Requirement 5.2:
The service provision of core functions has been secured and they have back-up procedures.

- Permitted downtime limits are specified for information systems enabling the organisation's core functions, and service provision should be based on these specifications. Operational continuity in exceptional situations is ensured by back-up procedures.

Requirement 5.3:
The information needed by critical functions has been secured in exceptional situations.

- Availability of information is an essential requirement for organisations. To ensure this, back-up solutions and time requirements, for example, are needed for operations in certain type of disruptions. In some services, this may restrict service provision from abroad only.

Requirement 5.4:
The realisation of threats is prevented by using physical security methods to protect the ICT environment.

- The risk and impact of external threats can be significantly reduced by locating offices and engine rooms appropriately and using structural solutions.

Requirement 5.5:
The operation of telecommunications is ensured as required by the criticality classification of services.

- The uninterrupted functioning of telecommunications is a critical element for the availability of information and services. This requires special measures, particularly in increased- and high-level systems.

Requirement 5.6:
Contingency plans have been prepared for information systems to ensure rapid recovery from disruptions.

- Unanticipated disruptions arising from the interaction of external factors and technical vulnerabilities are typical of today's operating environment. Reducing and recovering quickly from these disruptions is significantly promoted by planned and rehearsed procedures, technical back-up arrangements, and management and communication measures.

4.6 Measurement and reporting

> Measurement, reporting and auditing produce such information for management, strategies and operational planning that can be used to develop operations capable of withstanding disruptions in a cost-effective way.

The development, maintenance and operation of services is monitored based on the donut dial for annual planning and division of responsibilities approved by the organisation's senior management group.

The implementation and effectiveness of continuity management, information security and contingency planning should be monitored regularly using various assessments. Such assessments may be made by the organisation itself or by an external party.

Reporting consists of immediate notifications of disruptions and incidents as well as analysed summaries linked to the annual planning. Reporting is also part of normal operational and financial monitoring, such as the annual information report.

Requirement 6.1:
The implementation and appropriateness of ICT contingency planning is monitored and assessed.

- Indicators describe developments and create a foundation for decision-making. Monitoring and assessment are important, helping to detect and address possible shortcomings in good time.

Appendix 1 ICT contingency planning requirement cards

1 Leadership

1.1 The organisation takes into account the legislation related to its activities and services and other standards steering ICT contingency planning, and these are implemented through contingency planning policies and actions.

Base level

1.1-1: The organisation takes into account the legislation related to its activities and services and other standards steering ICT contingency planning, and these are implemented through contingency planning policies and actions.

Increased level

1.1-2: The organisation has a procedure for identifying ICT contingency planning requirements and introducing changes in these requirements into operational planning.

High level

1.1-3: The organisation's management has ensured that its powers in serious incidents and in emergencies are appropriate and that the organisation has the capability to apply them.

Examples to support the application of requirements:

1.1-1: On the base level, the public sector takes into account legislation, administrative branch regulations, government instructions, standards and agreements, and possible international obligations. Companies, on the other hand, take into consideration legislation, obligations specified in agreements, and possible sector-specific recommendations. It is particularly important that both the organisation acquiring the service and the organisation providing it know the regulations affecting the service and keep each other informed of these regulations.

Legislation steering an agency's activities and other related documents have been identified and recorded in the justifications of the information security and risk management policy. Agencies' strategies, principles and operational planning take note of the ICT contingency planning policy outlines prescribed in government-level steering documents.

1.1-2: It is essential that a party be assigned to be responsible for monitoring contingency planning requirements as a whole (including mandatory and recommended requirements) and for channelling changes in requirements into information security and continuity management. This party (individual or group) is to monitor changes and to ensure that information about changes is available to the organisation and they are taken into account and recorded in planning and development programmes. Management approves changes and monitors that they are put into effect. Similarly, the service managers of different parties assess requirements and submit proposals to the service's management group.

1.1-3: The agency has the capacity to make proposals to the ministry on the need to amend legal provisions that secure the organisation's core functions. Proposals prepared in advance provide the organisation additional powers via legislation to act in special situations and emergencies. Legal provisions bind the customer, and obligations are extended via agreements to service providers.

1.2 ICT contingency planning policies have been specified based on the requirements set by the organisation's activities

Base level

1.2-1: Management has determined the policies and objectives for operational continuity and ICT contingency planning.

1.2-2: ICT contingency planning responsibilities have been specified for process owners.

Increased level

1.2-3 Policies, objectives and resources for ICT contingency planning are reviewed in accordance with the donut dial for annual planning.

High level

1.2-4 The organisation's management has ensured that core functions in emergencies, and procedures managing their continuity, have been specified, documented and tested.

Examples to support the application of requirements:

1.2-1: Policies and objectives have been described, for example, in the organisation's information security and risk management policies and continuity plan. Models of plans and other documents are available in Appendix 1 of VAHTI 5/2009. Each ministry's management policies consist of decisions concerning, for example, operating principles and objectives. Based on these, a ministry gives to its administrative branch more detailed regulations and instructions through performance guidance. The agency's management decides its operational policies and issues related instructions and obligations for its field of operations in the form of performance targets. In companies, too, management decides the general operational principles and objectives in relation to business continuity and information security. Policy decisions may be, for example, an approved information security policy, risk management policy or business continuity strategy. Policies directed at services are recorded in service agreements or separate documents.

1.2-2: Different actors' roles and responsibilities are described, for example, in appendices to service descriptions and risk management and information security principles.

1.2-3: The agency's management determines continuity management policies on the basis of risk assessment, taking operational objectives into account. Measures carried out according to the development plan are discussed and assessed in connection with interim reporting. The annual report includes a summary assessing the effectiveness of measures. The development plan is included in the donut dial for annual planning of the agency's management group.

1.2-4: Core functions have been specified in the strategy, and continuity and contingency plans support them. Plans are tested regularly, for example in connection with the state leadership's preparedness exercise (VALHA) and other contingency planning exercises. Reporting and auditing procedures for exceptional situations and emergencies have been planned, instructions issued and exercises held. These procedures are incorporated into each acquired service.

1.3 Incident management has been outlined, organised and taken into account in steering models

Base level

1.3-1 Instructions have been issued and responsibilities assigned for decision-making concerning incidents and the handling of exceptional situations.

Increased level

1.3-2 The organisation's management ensures that operational and management models as well as recovery plans have been specified based on risk assessments for recovery from the most probable incidents.

1.3-3 Basic instructions for incidents have been given to staff and, through contractual obligations, to the service network.

High level

1.3-4: Organisational structures and operating models support the management and control of disruptions and emergencies and recovery from them.

1.3-5: The organisation has a procedure for learning from actual disruptions.

Examples to support the application of requirements:

1.3-1: Decision-making responsibilities and powers have been agreed. Deputies have been named and staff understand how incidents will be managed. This information can be given, for example, in the organisation's continuity management policy and management model document. A responsible party handles incidents. Reporting is done using a standardised form or electronically on the intranet, from where it is easy to link to the risk report, applying Chapter 2 of VAHTI 3/2005.

1.3-2: The continuity plan describes, for example via incident scenarios, the necessary recovery arrangements and their management. Recovery is planned for each service with the hosting service provider.

1.3-3: Continuity planning should also cover systems maintained by third parties. General instructions should relate, for example, to the use of premises (no access to building), introduction of back-up premises, telework opportunities, and prioritisation of tasks when several staff members are absent from work. Detailed system-specific instructions and plans have been distributed to key individuals electronically and on paper. Special instructions may be secret documents and intended for use only by named individuals, but secret material should be stored so that it can be accessed, if necessary, when the operating premises and normal information systems are not in use.

1.3-4: The threat scenarios of the Security Strategy for Society are taken into account in the organisational structures.

1.3-5: Experiences of disruptions are systematically collected and incorporated into operational, service and system development needs as part of operational and financial development according to the donut dial for annual planning.

1.4 ICT contingency planning has been organised and responsibilities assigned as part of normal management, operations and partnership network management.

Base level

1.4-1: ICT contingency planning management roles and responsibilities have been specified and they are included in job descriptions.

Increased level

1.4-2: The organisation's management has prioritised the tasks, services and resources in disruptions.

High level

1.4-3: For each service, availability of resources in disruptions and emergencies has been agreed with the service provider network.

Examples to support the application of requirements:

1.4-1: The organisation's tasks concerning contingency planning are specified on the basis of, for example, the Emergency Powers Act. The organisation uses personal job descriptions or role descriptions. The model for descriptions can be found in Appendix 2 of VAHTI 5/2009. The implementation procedure can be described in the governance model.

1.4-2: Tasks and prioritisation have been taken into account in the continuity plan. An annually updated list relating to this may be appended to the plan. Prioritisation of tasks, services and the use of resources should be based on realistic assumptions, for example using a thorough business impact analysis (BIA).

1.4-3: The continuity plan has specified the additional staff required to support core operations, both within the organisation and with service providers or partners. To support continuity planning, parties responsible for specific systems, services and/or customers have been designated to monitor the risks arising from incidents, their effects and costs.

1.5 Sufficient resources for the objectives have been allocated to contingency planning and continuity management

Base level

1.5-1: Objectives and resources for continuity management and information security have been specified in performance guidance.

Increased level

1.5-2: Resourcing of ICT contingency planning for incidents and emergencies has been taken into account in the agency's budget and in operational and financial planning.

High level

1.5-3: The availability and sufficiency of resources in emergencies has been secured.

Examples to support the application of requirements:

1.5-1: As part of performance guidance and operational and financial planning, the organisation's management has decided the level that the continuity management, information security and contingency planning must achieve or maintain in the different parts of the organisation. In connection with budgeting, human and other resources have been assigned to tasks relating to these areas.

1.5-2: The sufficiency of human resources should be assessed when continuity plans are prepared. Necessary supplies and other additional costs should be taken into account in the budget. As the party funding the administrative branch spending limits, the ministry decides the allocations for ICT contingency planning and continuity management. ICT contingency planning resources are allocated in the operational and financial planning process together with the approval of the continuity management development plan. The organisation's management monitors the actual investments made in continuity management via annual reporting and sets performance targets and provides resources according to the approved risk level.

1.5-3: The need for resources has been assessed against Security Strategy for Society threat scenarios. The sufficiency of resources is tested in contingency planning exercises, for example. In partnership agreements, the organisation should ensure that a sufficient number of staff are available for the maintenance of critical functions.

1.6 Contingency planning and continuity management planning are implemented as a joint effort of core and support functions

Base level

1.6-1: The organisation's security cooperation group also handles ICT contingency planning issues.

1.6-2: The organisation's management regularly discusses continuity and information security situation, policies and principles, as well as their implementation and coordination.

Increased level

1.6-3: The management of core function services in disruptions and special situations is planned in cooperation with support functions, key stakeholders and service providers.

High level

1.6-4: The effectiveness of plans in the service network has been verified.

Examples to support the application of requirements:

1.6-1: The agency/organisation has a cooperation group with representation from different sectors, including security, information security and emergency preparedness. The group discusses, for example, perceived risks, set information security objectives and their achievement, and changes arising from future needs. It is recommended that the cooperation group meet at least three times a year. Agreed measures are entered in the minutes and their implementation is monitored. Issues are discussed with service suppliers in regular meetings.

1.6-2: Continuity and contingency planning issues can be planned and discussed in units' management groups, in services steering groups and in the organisation's senior management group as a separate item, for example on the proposal of the cooperation group. An organisation following an information security management model in accordance with the ISO 27001 and ISO 27002 standards arranges management review sessions every six months.

1.6-3: Continuity management should be implemented so that all the necessary core and support functions are covered. Representatives of key support functions, such as information management, human resources management and estate management also participate in the organisation's continuity planning. Staff from certain sectors participate in the discussion of continuity management from their perspective. The organisation reviews annually how service providers implement continuity management in accordance with the security agreement.

1.6-4: Verification can be implemented in contingency planning exercises based on different scenarios.

1.7 The organisation's management monitors the development of contingency planning and cyber security as well as continuity planning, and the impacts and costs of these measures

Base level

1.7-1: The progress of decided development measures are reported to the organisation's management as part of normal reporting.

Increased level

1.7-2: The impact of changes in the operating environment as well as development needs and measures relating to contingency planning and incident management are reported to the organisation's management.

High level

1.7-3: Regular reporting to management is based on agreed continuity management indicators. The received data are used in operational development.

Examples to support the application of requirements:

1.7-1: The report on development measures given to the organisation's management includes an assessment of their effects on risks directed at the organisation. Reporting takes place according to the organisation's normal reporting schedule, for example once a month. An annual assessment of security issues and continuity management is made for each function and this is compared with the situation in previous years in order to detect possible changes.

1.7-2: The report includes information on the use of resources, the achievement of ICT contingency planning, continuity management and information security objectives, anomalies, measures taken as a result of anomalies, and other significant information security changes. Based on the reports, monitoring information is collected for use in training and instructions as well as for developing operational processes and improving their security.

1.7-3: The agreed continuity management indicators are used in operational and financial planning. In central government, it is recommended that indicators be used that can generate data for central government monitoring surveys.

1.8 Communication and reporting responsibilities and processes have been specified and organised with key stakeholders

Base level

1.8-1: Internal and external crisis communication principles, responsibilities and processes have been specified.

Increased level

1.8-2: Communication practices and responsibilities, and backup communication tools and processes in exceptional situations have been agreed.

1.8-3: Continuity management and information security issues are communicated to stakeholders annually or as agreed.

High level

1.8-4: Communication and reporting exercises concerning special situations and emergencies are held and developed based on stakeholder feedback.

Examples to support the application of requirements:

1.8-1: The organisation has a policy and instructions for internal and external communication. The practical implementation of crisis communication has also been described in the policy. Communication responsibilities have been described and communication roles have been specified. Stakeholders and contact points to which the organisation is responsible for service continuity and information security have been identified, for example in connection with the process descriptions. Communication is directed at these parties and it includes, for example, notification of long service interruptions, planned repair measures, service interruptions or inspections caused by malware, restoring back-ups of large amounts of data etc.

1.8-2: Verification methods have been prepared in advance and all parties are informed of them. Use of tools and equipment has been rehearsed. Telephone, telefax, couriers or face-to-face contacts should be available in addition to e-mail.

1.8-3: Reporting of service continuity management and information security affecting key stakeholders as well as communication of incidents have been organised and responsibilities assigned. There are templates for stakeholder reports and incident warnings in order to standardise the collection, analysis and transmission of information. Section 5.6 of VAHTI 6/2006 has an example of administrative branch internal reporting. Stakeholders include, for example, the ministry steering the organisation, the organisation's staff, administrative branch cooperation groups, different units under the organisation, CERT-FI, etc.

1.8-4: Communication back-up procedures are rehearsed as part of contingency planning exercises. The development of operational structures can be of assistance in accelerating communications. Feedback on the success of communications is collected as part of risk reporting.

2 Strategies and operational planning

2.1 In operations, the interaction of the organisation and the operating environment should be taken into account

Base level

2.1-1: The impact of disruptions based on the threat scenarios of the Security Strategy for Society on the most important services and the handling of information has been recognised and assessed.

Increased level

2.1-2: An up-dated documentation is provided on the key operating environments for the organisation's activities as well as on the services, systems and actors associated with them.

2.1-3: The organisation's management discusses and assesses the ICT dependencies of core functions at least once a year.

High level

2.1-4: Changes in the security and operational environment are recognised and the special requirements set by them are taken into account in the organisation's activities.

Examples to support the application of requirements:

2.1-1: In its continuity planning, the organisation has described how different events affect its activities and the handling of its tasks and how it has prepared for them. This requires sufficient documentation for the most important ICT services.

2.1-2: The organisation has a head office and regional units. Staff can also do telework. The regional units handle permit issues; other functions take place at the head office. Information systems relating to permit issues have also been located in the regional units' premises. The key information systems of the head office have been located in the service provider's premises. The identification of premises, functions and systems creates a foundation for more detailed security and continuity planning.

2.1-3: The agency's status and dependencies are assessed as part of the operational and financial planning process and necessary development measures are agreed based on the results of the assessment. The assessment of dependencies is part of the agency's risk management.

2.1-4: The senior management of the administrative branch (for example in a ministry) generally makes an assessment of a changed situation and issues instructions for measures to be initiated. These situations are rehearsed in contingency planning exercises, such as VALHA. As a security situation changes, it may be necessary, for example, that a proposal be prepared authorising the ministry to exercise certain powers under the Emergency Powers Act. Financial difficulties or ownership changes of a key service provider may require a quick reaction.

2.2 The results of risk management direct the development of contingency planning

Base level

2.2-1: Management approves the risk management policy and, on the basis of risk assessment, the measures to be undertaken. Management also accepts residual risks.

Increased level

2.2-2: ICT contingency planning, continuity management and information security procedures for incidents, cyber threats and emergencies are specified and documented based on risk management results and impact assessment.

High level

2.2-3: Risks are assessed in cooperation with stakeholders and service providers, using compatible risk management methods.

Examples to support the application of requirements:

2.2-1: The organisation has a policy, procedure and instructions for risk assessment and management. A record is kept of the biggest risks on an organisational and service network level, and the implementation of risk management measures is monitored. Residual risk acceptance criteria are documented and changes in the risks are monitored.

2.2-2: Risk management in central government is part of the operational and financial planning process. The State Budget Decree requires the implementation and assessment of risk management. Risk management covers recognition of threats, assessment of the magnitude of risks, prioritising risks, specifying the measures by which recognised risks are managed, and monitoring and assessing the adequacy of measures, for example in connection with performance reporting.

2.2-3: The administrative branch has standard risk management procedures and instructions, and risk management is developed on a collaborative basis. Service providers participate in the risk assessment of the services they provide, or communicate the results of their own risk analysis to the customer. Service providers do not, however, need to use the same risk management tools and instructions as the public sector; it is sufficient that the parties are able to use each others' results and understand them in the same way.

2.3 Contingency planning measures support the objectives of the organisation's core operations

Base level

2.3-1: Core function and process services and systems to be protected have been identified and placed on the base, increased or high level in accordance with the requirements of core functions and processes.

Increased level

2.3-2: The organisation is able to prioritise critical services over other services in disruptions.

High level

2.3-3: Core function process descriptions include essential measures relevant for ICT contingency planning.

2.3-4: Core function objectives include indicators measuring the implementation of ICT contingency planning.

Examples to support the application of requirements:

2.3-1: The organisation must identify its core functions. Functions that are central to the implementation of strategic tasks specified in the Security Strategy for Society should be identified in the first stage. Functions that are important for the management of disruptions according to the threat scenarios described in the Strategy should be recognised in the second stage. Contingency planning measures should be planned from the perspective of the objectives of core functions, processes, and services, not solely from the perspective of an individual support function or service.

2.3-2: The organisation's continuity plan includes principles on how operations are systematically organised in different situations and how changes are implemented. The time criticality of acquired services and priorities including their implementation should also be agreed with service suppliers. The organisation has reviewed in advance and described scenarios in which certain situations may arise. The organisation recognises the significance of each service for its activities.

2.3-3: One of an organisation's core functions is its customer service process. It describes how customer identities are checked, how transaction data are stored and how information is protected if it is transferred to another public authority.

2.3-4: Indicators should support operational and financial reporting, performance guidance agreed in central government, and information security surveys conducted by VAHTI on the development of central government information security.

2.4 Incident management and emergency procedures have been documented, training given and exercises held

Base level

2.4-1: The accessibility of ICT services in the event of a possible reduction of resources should be taken into account in incident management plans and procedures for core and support functions.

2.4-2: The updating of operational continuity, information security and contingency planning policies has been organised and responsibilities assigned.

Increased level

2.4-3: System-specific recovery plans have been prepared for the most critical services and key individuals have been trained in how to act in major incidents.

2.4-4: Operating instructions for incidents are developed on the basis of data collected and experiences obtained about disruptions and special situations.

High level

2.4-5: Capacity and resources for critical ICT services have been secured to the agreed minimum level.

2.4-6: Continuity and contingency plans and instructions are tested and rehearsed regularly on a practical level to manage special situations and emergencies.

Examples to support the application of requirements:

2.4-1: The organisation understands that in special situations the standard of ICT services in use may weaken and that activities will have to adjust to this, for example, by temporarily suspending less important functions. Adjustment measures have been planned in advance.

2.4-2: Responsibility has been assigned, for example to the information security manager, for the preparation of updates to the information security and risk management policy and the information security development plan, and to the emergency preparedness manager for updates to the continuity plan. An update schedule of once a year has been agreed, and the update work is incorporated in the donut dial for annual planning in connection with the testing of risk assessment and the continuity plan.

2.4-3: The organisation's system-specific instructions describe, for example: the system's dependencies on other systems, how the system is reinstalled, how data is restored, and how the system is tested to verify that it is again working normally.

2.4-4: The organisation has written instructions for the actions to be taken in the event of a power failure; telecommunications breakdown; system malfunction; strike involving key personnel or supplier; pandemic, fire, storm or flood. Management of Security Strategy for Society threat scenarios is based on good continuity planning. The continuity plan records the available staff, key individuals and their deputies, and an assessment of their availability.

During an incident, the person responsible keeps a log of the events. Every incident is reviewed afterwards with the aim of discovering how it occurred, what impact it had and whether the factor that gave rise to the situation could have caused some other event. In addition, it should be assessed how the staff managed the situation and whether it is necessary to make changes to instructions or arrange training for the future.

2.4-5: ICT services include, for example, telecommunications and hosting services, maintenance of information technology equipment, systems development, and change management. The minimum levels required by ICT services are specified in a service-level agreement (SLA) or in a continuity and recovery plan prepared for the service. Minimum levels may be set for time requirements, hardware platform or telecommunications capacity.

2.4-6: It is recommended that the continuity plan be desk-checked every couple of years. If the plan includes the use of back-up premises, exercises should be held to train and familiarise staff on how to act during incidents. A high-level organisation and its key suppliers participate in TIETO exercises or apply its scenarios in organisation-specific exercises. Operating instructions are developed on the basis of the lessons learned.

2.5 Round-the-clock activity and CERT-FI cooperation should fulfil the organisation's objectives and obligations

Base level

2.5-1: The organisation has a process for dealing with CERT-FI notifications.

2.5-2: The organisation notifies CERT-FI of serious and suspected information security breaches.

2.5-3: The need for round-the-clock monitoring of services, systems and networks has been specified.

Increased level

2.5-4: Key services and the necessary ICT are covered, as required, by 24/7 monitoring and the related reporting.

High level

2.5-5: The organisation's core activities have a 24/7 monitoring function, which cooperates closely with CERT-FI and the service network.

Examples to support the application of requirements:

2.5-1: The organisation has assigned individuals who receive warnings and notifications sent by CERT-FI.

2.5-2: The organisation has issued instructions and trained staff on the procedure for making notifications. Serious information security breaches include theft of personal data and extensive denial-of-service attacks.

2.5-3: Round-the-clock monitoring is arranged if necessary and should be specified separately for each unit. Base-level systems do not generally need round-the-clock monitoring, unless they are in use 24 hours a day. Cooperation models for the monitoring, management and maintenance of ICT systems have been organised and agreed in the key service provider network.

2.5-4: The organisation's Service Desk or Help Desk checks current warnings on the CERT-FI website and notifies the information security group of them. Other monitoring services for the information security situation can also be used. The service provider has a procedure for monitoring and reacting to notifications. The monitoring obligation is extended in agreements to service providers in accordance with the criticality classification of the service in question. In more complex environments, it is possible to use a solution that automatically scans the environment's equipment and software. The monitoring obligation and measures arising from notifications are agreed with the service provider.

2.5-5: Round-the-clock monitoring and reacting to threats may be implemented using the organisation's own resources, in cooperation with several government organisations or as a service purchased from a service provider. In critical and key environments, an intrusion detection system is in use. Reaction to problems detected by monitoring may have a longer response time outside normal working hours if the service itself is in use only during normal working hours. Some services may be time-critical at a certain time of the year, in which case monitoring, too, should be round-the-clock, while at other times 12/7 monitoring, for example, may be sufficient.

The service network consists, for example, of the hosting service supplier, the network operator and the subcontractors needed to provide the core functions.

3 People

3.1 Role- and task-specific requirements have been set for ICT contingency planning expertise, its level is known, and it is developed

Base level

3.1-1: Staff roles and responsibilities in the planning and implementation of continuity management and information security have been specified also taking incidents into account.

Increased level

3.1-2: The information security and ICT contingency planning training is followed in skills management.

High level

3.1-3: The requirements caused by disruptions and emergencies have been taken into account in human resources planning, job descriptions and training.

3.1-4: Measures to ensure and develop the competence of the service network have been organised, and key expertise essential for core functions has been identified.

Examples to support the application of requirements:

3.1-1: The organisation has specified roles in accordance with Appendix 2 of VAHTI 5/2009 and the expertise required by each task.

3.1-2: Induction includes a section on contingency planning, continuity management and information security. The induction covers, for example, the content of the most important instructions and continuity management plans from the point of view of information security policy and an individual's tasks. The inductor has written material on these issues. When instructions change, information briefings are arranged, and electronic channels are used to communicate this information. Changes in the organisation and operating environment as well as information security incidents are also taken into account in staff training.

3.1-3: When recruiting staff, the organisation's needs in continuity and contingency preparedness expertise are taken into account. The adequacy of staff expertise in relation to their job descriptions is examined in performance and development discussions and through skills surveys. Resources for the necessary training are systematically allocated and participation of staff in training courses is taken into account at the workplace.

3.1-4: In procurement, sufficient expertise and the maintenance of this expertise is required of key individuals involved in providing the service. Service network expertise is enhanced through joint exercises. The fulfilment of skills levels is monitored using skills surveys.

3.2 The organisation encourages staff to observe and develop good continuity management and information security procedures

Base level

3.2-1: The staff's awareness of and expertise in security matters is developed.

Increased level

3.2-2: Information security and contingency planning training has been integrated into the organisation's other training and activities.

3.2.3: Staff participate in assessing the effects of disruptions and special situations and in developing their management.

High level

3.2-4: Staff are encouraged to participate in cooperation that support contingency planning.

Examples to support the application of requirements:

3.2-1: The organisation regularly organises information briefings for staff in which the basic aspects of information security, continuity management and contingency planning as well as topical themes such as various scams and snooping (social engineering, phishing) are discussed.

3.2-2: It is recommended that in the organisation's and service's information security and contingency planning procedures most closely related to the topic of the session are integrated into all training.

3.2-3: Representatives from all levels of the organisation participate in continuity exercises and their analysis as well as in the planning of further measures. Key individuals from core functions participate in planning. To obtain a complete picture, it's important that participation is heterogeneous.

3.2-4: The organisation designates experts to cooperation groups.

3.3 The organisation has an agreed a procedure for monitoring and handling security incidents and cases of misuse

Base level

3.3-1: Staff know to whom cases of misuse and security incidents or the threat thereof must be reported.

3.3-2: The organisation has specified tasks or roles for which applicants must undergo background checks, and the background check procedure is documented.

Increased level

High level

3.3-3: The need and possibility in emergencies to restrict and monitor employees' actions (protection of privacy) in the workplace have been examined.

3.3-4: The organisation has, or is supported by, a group trained in investigating security incidents and this group holds regular exercises.

Examples to support the application of requirements:

3.3-1: Incidents are recorded in risk reports and supervisors must address negligence. The possible consequences of failure to comply with information security regulations and instructions have been described in the information security policy and they are communicated to all those working in the organisation. This corresponds to information security level requirement 1.3.3.2.

3.3-2: A security clearance can be made only if it is applied in the organisation. In addition to central government key staff, companies under a priority classification and their staff may be subject to security, should the organisation decide to conduct such checks. This depends on the classification of information to which staff have access in their work. Separate secrecy or confidentiality agreements are made, if necessary. This corresponds to information security level requirement 1.3.2.5.

3.3-3: The organisation has prepared procedures to restrict telecommunications, for example.

3.3-4: The information security group may consist of the organisation's own staff or representatives of the administrative branch or a service provider. Investigation of incidents requires sufficient technical and legal competence. When crimes are suspected, the police is the investigating authority. Further training for the information security group includes training in the investigation of various incidents and cooperation with the police. This corresponds to information security level requirement 1.3.3.4.

3.4 Key roles and people have been identified and back-up arrangements planned

Base level

3.4-1: Key roles have been identified and a deputy or deputies have been named for them.

3.4-2: Key staff responsible for critical tasks have been trained in how to act in incidents.

Increased level

3.4-3: Alternative procedures and deputy arrangements in special situations have been planned and prepared to ensure the performance of critical tasks.

3.4-4: Key staff are regularly trained in maintaining critical functions in special situations.

High level

3.4-5: Back-up arrangements required by critical tasks in emergencies have been tested and rehearsed.

Examples to support the application of requirements:

3.4-1: A deputy may also be an individual outside the organisation, in which case special attention must be paid to the training of the deputy and to ensuring that the deputy will be available when necessary.

3.4-2: System experts have sufficient knowledge of incident management instructions and the instructions are easily available. Staff who investigate information security incidents have been designated and trained.

3.4-3: An alternative procedure has been documented in the continuity plan.

3.4-4: The organisation arranges annually at least the desk-checking of a scenario related to some special situation. If possible, key staff also participate in central government joint exercises (e.g. VALHA, TIETO).

3.4-5: Testing and training is agreed in the organisation's operational and financial planning process. Key staff and their deputies participate regularly in exercises relating to special situations and their capacity to act in emergencies is assessed. Based on the exercises, additional training or exercises to improve the capacity to act correctly in such situations should be arranged, if necessary.

3.5 Staff have been hired and their roles have been planned and scaled in the manner required by the continuity management and information security of organisation's core functions

Base level

3.5-1: Exemptions of key staff from military service in emergencies are made and maintained.

Increased level

3.5-2: The service network's critical areas of special expertise have been identified and have been taken into account in the procurement of services, in the use of staff and in other resourcing.

High level

3.5-3: Exemptions of key staff from military service and the validity of related instructions are updated annually. This applies also to service chains.

3.5-4: For critical services, the right to strike has been suspended and the use of emergency work prepared.

Examples to support the application of requirements:

3.5-1: Exemptions of key personnel from military service are checked at least every two years and when there are changes in staff. The agency proposes exemptions to the general staff of the military province in which it is located. For further information, see section 89 of the Conscription Act.

3.5-2: Core functions and their processes have been described and related security controls specified and implemented. Staff and their deputies have been designated and they know their tasks. The competence and capacity of service network staff to deliver the service in various disruptions is known, and critical services are not acquired from suppliers whose capacity is not adequate.

3.5-3: For a high-level service, the list of exemptions of key staff from military service is always updated when there are changes in the staff providing the service, irrespective of whether the agency's own or a service provider's staff are involved. All staff on the list of exemptions from military service participate in an annual continuity exercise. If exemptions include staff who normally do some other work, then annual induction training, a temporary placement or other revision of the material included in handling the task should be arranged for them, so that they are able to carry out the task, if necessary. Staff who normally handle the task are inducted in the task on a regular basis, and they do not need separate annual induction.

4 Partnerships and resources

4.1 The partners, subcontractors and resources necessary for the organisation's activities have been identified

Base level

4.1-1: The significance of different service providers in the network for ICT services has been recognised.

Increased level

4.1-2: The most important aspects of the service network have been described. Continuity management procedures have been adopted and training provided.

4.1-3: In disruptions and emergencies, the availability of network services and other resources required by core functions and their continuity has been resolved.

High level

4.1-4: In disruptions and emergencies, the availability of network services and other resources required by core functions and their continuity is verified annually and in connection with major changes.

Examples to support the application of requirements:

4.1-1: The organisation's continuity planning identifies services vital for its core functions, assesses the effects that ICT service interruptions of different lengths have on the organisation's core functions. It also determines who provides these services to the organisation, who are the most important subcontractors and what their roles are in service provision. Dependency on external actors in particular should be ascertained for each core service and necessary measures determined.

4.1-2: Service network descriptions take into account the subcontractors of subcontractors that are significant for service continuity and security.

4.1-3: The structure of the ICT service chain, namely the service provider's most important subcontractors and their significance for service continuity (spare parts, maintenance staff, support measures, IT equipment premises etc.), has been specified in cooperation with the service provider using an appropriate method. Service network descriptions are reviewed and, if necessary, updated at least annually. Requirements and objectives for service network continuity management and information security have been agreed with service providers and training is provided to key staff.

4.1-4: The operational capacity of the service network may be assessed using surveys directed at service providers, experiences obtained from actual incidents, as well as joint exercises and audits. The service network is managed, and any ownership changes that take place in the network are monitored and assessed for their impact on the organisation's own activities. The objective is that the organisation will have a sufficiently good picture of the network that provides the service, so that it can assess what risks there might be to the network and take steps to manage them. In connection with operational changes, and as part of the change management process, the impact of changes on maintaining the continuity of ICT activity is assessed, for example, using desk-checking or risk management tools. The agreed level is verified annually in audits and service monitoring meetings.

4.2 Agreements include requirements for operational contingency planning, continuity management and information security as well as their implementation

Base level

4.2-1: The service agreement specifies the ICT contingency planning level that the service, the service provider and any subcontracting network should meet.

Increased level

4.2-2: The contracting parties review the implementation of the agreement as well as continuity management needs on an annual basis.

High level

4.2-3: The network's service and security agreements are maintained and compliance with them is audited regularly.

Examples to support the application of requirements:

4.2-1: The agreement and its annexes contain a list of the continuity management and information security requirements to be applied to the procurement, taking into account the responsibilities of the contracting parties. For example, requirements relating to the protection of premises do not apply to the service provider, if the delivery of the service takes place in the purchasing organisation's own premises.

In addition, the agreement should specify the right of the purchasing organisation or its representative to audit the implementation of requirements, the service provider's obligation to report observed incidents, and the sanctions if the service provider does not fulfil requirements as agreed and, despite a complaint, is not able to rectify the situation within a reasonable time.

4.2-2: Valid agreements should be reviewed and necessary additions or changes made to them. Continuity management should be reviewed by the contract group at least once a year. Updating a service level agreement may be necessary if the significance of a service for the organisation's activities changes substantially. A security agreement should be updated, for example, when a service provider moves to new premises or updates its security practices. An update may also be necessary if shortcomings in agreed practices are detected during exercises.

4.2-3: Auditing is based on annual planning and on an assessment of the selected subareas. Auditing plans are prepared in cooperation with the service provider, ensuring that overlapping audits are avoided. The effectiveness of a service provider's security management system can be trusted without separate auditing if it has been certified, for example, in accordance with ISO/IEC 27001 and ISO 27002 or other corresponding standard. In such cases, auditing can focus on the fulfilment of ICT contingency planning requirements.

4.3 The obligation to manage the continuity of critical operations and information security has been extended to the key supplier network

Base level

4.3-1: The contracting parties have agreed their responsibilities for the management and availability of resources.

4.3-2: The organisation is aware of the main supplier network's capacity to provide key services for the customer's activities in disruptions.

Increased level

4.3-3: The provision and maintenance of the most important services can be prioritised in the service network.

4.3-4: Cooperation processes for the monitoring, management and maintenance of ICT systems have been organised and agreed in the main supplier network.

High level

4.3-5: Continuity management procedures have been implemented in the whole service network, their effectiveness is tested and exercises are held regularly.

Examples to support the application of requirements:

4.3-1: In agreements, the service provider is obliged to require adequate continuity management and information security also from key subcontractors. Both the customer's and the service provider's responsibilities should be specified.

4.3-2: In invitations to tender and when the suitability of a provider is assessed, the provider's ability to fulfil the continuity of its services should be taken into account. The customer should verify how the provider is able to operate in disruptions and agree on that as part of a security agreement.

4.3-3: Service providers are aware of which of the services they provide are on base, increased and high level. If it is necessary to lower the level of a central government service because of a special situation or emergency, it should be done taking the contingency planning level of the services into account.

4.3-4: Procedures have been agreed in a security agreement. With respect to outsourced services, prioritisation might require changes to it. The cooperating parties have designated individuals responsible for coordinating cooperation. Cooperation is discussed between customer and service provider in service monitoring groups.

The organisation has service reporting and auditing procedures. Audits are agreed as part of a security agreement and there is a plan specifying the items to be audited annually. Auditing can be implemented, for example, using the auditing service of the Government IT Shared Service Centre.

4.3-5: The effectiveness of continuity plans is regularly assessed through desk-checking, joint service network exercises and audits.

4.4 Cooperation with partners to manage exceptional situations has been organised and responsibilities assigned

Base level

4.4-1: Incident cooperation principles with public authorities and other stakeholders have been planned and key staff have been trained in the main aspects.

Increased level

4.4-2: Service continuity and related threats are regularly assessed with stakeholders and service providers on the basis of Security Strategy for Society threat scenarios.

4.4-3: Incident cooperation and crisis communications between public authorities and key stakeholders have been planned and implemented, and their main content rehearsed.

High level

4.4-4: Emergency cooperation with public authorities and other stakeholders has been verified and rehearsed.

4.4-5: Emergency cooperation in the supplier network is tested and rehearsed regularly.

Examples to support the application of requirements:

4.4-1: Agreements specify the procedures and the parties' obligation to immediately communicate information security incidents and disruptions. Communication supports successful cooperation and may provide assistance in resolving an incident. The service-level agreement specifies how quickly corrective measures should be initiated.

4.4-2: Cooperation practices have been described in the continuity plan and they are discussed in training and exercises for key staff.

4.4-3: Crisis communications is part of the organisation's communication principles and have been described in the continuity plan. The organisation may participate, for example, in VALHA or TIETO exercises, which include communication in different situations.

4.4-4: The organisation holds exercises with public authorities and other stakeholders.

4.4-5: Cooperation is rehearsed, for example, in central government TIETO and VALHA exercises as well as in organisations' own contingency planning exercises.

5 ICT continuity management

5.1 ICT contingency planning requirements are taken into account in ICT service lifecycle stages

Base level

5.1-1: The process/function owner determines the information security and contingency planning level on which the system is to be placed.

5.1-2: ICT system owners know their ICT contingency planning responsibilities, and activities have been organised and responsibilities assigned accordingly.

5.1-3: The interoperability of information systems has been ascertained and described in public authorities' enterprise architectures.

Increased level

5.1-4: ICT contingency planning is included in the documentation of all lifecycle stages of ICT projects.

5.1-5: Threat assessments (Security Strategy for Society) and ICT contingency planning requirements are taken into account in architecture decisions.

5.1-6: Information security tests are performed before a system is approved into production.

High level

5.1-7: During development or customisation work, contingency planning reviews of critical elements are arranged and minutes kept of these reviews.

5.1-8: A system is audited before it is taken into production.

Examples to support the application of requirements:

5.1-1: Before each agreement, budget and development measure, the organisation must ensure that the system has been given an appropriate information and contingency planning level.

5.1-2: The key system maintenance tasks should include responsibilities for contingency planning and its implementation.

5.1-3: The interoperability of information systems is a basic prerequisite of contingency planning for disruptions. The information management act (Laki julkisen hallinnon tietohallinnon ohjauksesta 634/2011) obliges public authorities to describe how they implement and ascertain the interoperability in their enterprise architecture and to comply with these specifications in their system development.

5.1-4: In accordance with the phasing of information system development, an ICT project has been described as a process that includes review points for security issues. At each point, results are evaluated and a decision made on moving to the next development stage. Continuity management, information security and ICT contingency planning requirements are taken into account in architecture decisions, and project management and system development methods and instructions. The project management group decides whether measures are adequate based on a risk assessment. At the different stages of ICT projects, the implementation of continuity management, information security and contingency planning requirements is tested as well as assessed and audited. Tests are based on requirement specifications; deployment test results are compared with the requirement specifications. VAHTI checklists and such standards as NFPA 1600, ISO 27005 can be used in system development.

5.1-5: Continuity management, information security and ICT contingency planning requirements are emphasised in architecture decisions, project management and system development methods and instructions. Project management is audited by an external party. VAHTI checklists can be used in instructions.

5.1-6: Examples of different testing and auditing methods are the testing of undesirable characteristics and use cases as well as penetration testing without advance information (black-box testing) or with advance information (white-box testing).

5.1-7: Reviews are arranged, for example, as peer reviews, in project group or programming team meetings, or using an external auditor.

5.1-8: Audits are performed by an external auditor, for example the National Information Security Authority, or based on its instructions, e.g. the National Security Auditing Criteria (KATAKRI).

5.2 The service provision of core functions has been secured and they have back-up procedures

Base level

5.2-1: Core function back-up procedures and recovery from disruptions have been planned and documented.

Increased level

5.2-2: Incident management and back-up procedures have been agreed in, and instructions and training provided for core function service provision and management processes.

5.2-3: Back-up power supply for key services in disruptions has been ascertained on the basis of a risk analysis.

High level

5.2-4: The implementation of core function hosting services and operation in emergencies has been recorded in agreements, and emergency exercises have been held.

5.2-5: Supervised remote maintenance in disruptions must be possible for time-critical services, whose permitted down-time is separately specified.

5.2-6: Access rights to critical services and applications are managed and controlled in Finland.

Examples to support the application of requirements:

5.2-1: The organisation must identify its most important functions and the associated services.

5.2-2: The service supplier must describe and test its actions to be prepared for possible incidents. Back-up systems for service provision must be agreed in agreements.

5.2-3: If the organisation's premises have functions that cannot stop in the event of a power cut, a back-up power supply must be provided for the premises. Use of an uninterruptible power supply (UPS) is realistic against power cuts of less than an hour. If there is a risk of a longer power cut, a back-up power supply solution must be considered to secure supply of electricity. It should be possible to shut down systems in a controlled manner while UPS is active .The recommendations of the Finnish Communications Regulatory Authority and the KATAKRI criteria on this subject should be applied.

5.2-4: Testing in an early stage of the lifecycle reduces costs, and deployment testing in particular reduces changes after a system is taken into production. Cooperation models in the service provider network for the monitoring, management and maintenance of ICT systems have been regularly tested and rehearsed at intervals recorded in cooperation and service agreements. Production changes, the necessary expertise and resources, and transfer to back-up systems and recovery in emergencies have been planned, verified, documented and regularly rehearsed.

5.2-5: In serious disruptions, the organisation must initiate recovery measures immediately. It may be necessary to open a remote connection to enable maintenance. Where an external operator is involved, processes, premises and connections must be prepared and accredited in advance.

5.2-6: Large-scale, serious incidents might require rapid changes in access rights to services. For contingency planning, time criticality requires that these measures are performed in Finland and under Finnish legislation (e.g. telecommunications cuts, emergency powers etc.).

5.3 The information needed by critical functions has been secured in exceptional situations

Base level

5.3-1: Confidentiality, integrity and availability requirements have been set for the security of information resources.

Increased level

5.3-2: Use of information resources in disruptions has been planned, documented, implemented and tested.

5.3-3: In addition to back-ups of critical systems, the organisation should make safe copies to be stored in another building or in a different fire compartment from the original information.

High level

5.3-4: Use of information resources in emergencies has been planned, documented, implemented and tested.

5.3-5: Information resources of critical functions have been distributed geographically to at least two different locations in Finland.

5.3-6: The service provision of critical functions is located in Finland.

Examples to support the application of requirements:

5.3-1: The information management instructions and tools used by the organisation support the classification and archiving of information. Instructions include the management of information at different protection and security levels in the different stages of its lifecycle. Back-ups of information have been taken considering their importance for the organisation's activities.

5.3-2: The continuity management plan includes a section describing the handling of information. Plans are tested and their effectiveness is assessed regularly.

5.3-4: Decentralisation of operations is based on the central government organisation priority classification and on the significance of its core functions (services it provides) for the central government.

5.3-5: The service agreement includes contingency planning requirements for the service provider. The emergency preparedness plan describes the protection of information resources. The plan is tested and its effectiveness is assessed regularly.

5.3-6: The requirement applies to information systems important for national security. Examples are electricity distribution control systems and the connection points of telecommunications network nodes. Critical function systems and their information have been located geographically to at least two different high-level protection sites and the information is kept real-time.

5.4 The realisation of threats is prevented by using physical security methods to protect the ICT environment

Base level

5.4-1: The organisation has recognised the required protection class of the premises.

5.4-2: Important computer rooms and equipment should be protected against environmental hazards (burglary, fire, heat, humidity, gases, water and dust).

Increased level

5.4-3: The organisation has a plan for transferring ICT services to other premises if the current premises cannot be used.

High level

5.4-4: Key computer rooms have been protected against external attacks.

5.4-5: For high-level services, arrangements are made to provide a far-away back-up location, in which operations can be continued if the actual operating location can no longer be used.

Examples to support the application of requirements:

5.4-1: The organisation's priority classification is the foundation for continuity and emergency preparedness planning and the necessary protection solutions. Premises are separated into access areas, so that external parties cannot access working premises, and access from working premises to ICT premises is possible only by staff who have to enter them to perform their duties

5.4-2: General instructions complying with the purpose of the premises, such as instructions for telecommunications premises issued by the Finnish Communications Regulatory Authority, should be applied in protection,

5.4-3: The premises may be, for example, another office of the organisation in another locality. This has been taken into account in the continuity plan applying for example the KATAKRI criteria.

5.4-4: Important equipment is located in a computer room, which is protected in the manner described in Appendix 4 of VAHTI 2/2013. Premises are planned and built so that vandalism and terrorism, for example, are taken into account in their structural durability, applying for example the KATAKRI criteria.

5.4-5: The company Suomen Huoltovarmuusdata Oy, for example, offers high-security computer rooms and information storage, saving and back-up copying services for central government and private sector organisations that are critical for security of supply. The maintenance of high-level critical services is possible without external services and resources. The requirement is taken into account in the planning of premises, and a sufficient distance is decided on the basis of a risk analysis. Detailed strengths and material thicknesses in protective construction have been listed in a decree issued by the Ministry of the Interior.

5.5 The operation of telecommunications is ensured as required by the criticality classification of services

Base level

5.5-1: The organisation has recognised the degree to which telecommunications is critical in its own activities and services.

Increased level

5.5-2: The locations of telecommunications equipment, connections and connection points have been taken into account in protection classification.

5.5-3: The central government's key services are based on government shared secure communication solutions (VY network).

5.5-4: Together with the service provider, the organisation has analysed, planned and agreed the prioritisation of and changes in telecommunications services in disruptions.

High level

5.5-5: The public sector's most critical services and their data transmission are implemented as far as possible in accordance with government security network requirements.

5.5-6: Network environments and telecommunications services are secured in such a way that a deterioration of the service level on one operator does not interrupt the service required by the organisation's activities.

5.5-7: The organisation has planned, agreed and tested the prioritisation of and changes in the service network's telecommunications in emergencies.

Examples to support the application of requirements:

5.5-4: Together with the service provider, the organisation has agreed the use of telecommunications as well as telecommunications equipment and staff in disruptions. The organisation's ICT architecture requires that the service provider offers duplicated environments and that the time criticality of the service is specified in service agreements. The information technology environments of critical services are secured with an uninterruptible power supply for power cuts of at least four hours.

5-5-5: To ensure the sufficiently high-level implementation of services, the Ministry of Finance confirms the applicable requirements.

5.5-6: Telecommunications is duplicated physically along two different routes by two different operators. This requirement is stated in competitive tenders. The information technology environments of critical services are secured with a back-up power supply or back-up power connections so that the power supply can be initiated within one hour and maintained for one week. The technical and operational requirements of systems have been specified and their solutions have been determined and risks assessed. A separate telecommunications link through which it is possible to access a public information network (back-up link) may be installed for separately selected workstations.

5.6 Contingency plans have been prepared for information systems to ensure rapid recovery from disruptions

Base level

5.6-1: The organisation has a recovery process to secure core functions.

5.6-2: The capacity to initiate measures has been specified for each service.

Increased level

5.6-3: The organisation has written recovery plans for its most important systems.

5.6-4: Critical services' network, server and equipment environments are secured by duplication.

High level

5.6-5: Fault tolerance of server environments fulfils the requirements of disruptions and emergencies.

5.6-6: The organisation conducts exercises for disruptions in each service chain.

Examples to support the application of requirements:

5.6-1: The systems required by the organisation's core functions have been identified.

5.6-2: The operations manager has appointed for each ICT service a technical officer to initiate measures in accordance with the recovery plan. The ICT infrastructure, equipment, resources and expertise under the organisation's own control have been resourced for normal conditions and special situations. Outsourced services must have adequate service-level agreements.

5.6-3: The customer is always responsible for the existence of recovery plans. In an outsourced service, the provider is responsible for the preparation of system-specific recovery plans. The customer assesses recovery plans by testing them.

5.6-4: Together with the service provider, the organisation has agreed about the use of telecommunications and telecommunications equipment as well as about the responsibilities of staff in disruptions. The organisation's ICT architecture requires that the service provider offers duplicated environments and that time critical services are specified in service agreements. The information technology environments of critical services are secured with an uninterruptible power supply for power cuts of at least four hours.

5.6-5: Disruptions and emergencies described in the threat scenarios of the Security Strategy for Society (2010) are the guiding factors in the scaling and technical structures of server environments.

5.6-6: The organisation should know the level of effectiveness of the entire service chain and, as part of continuity and contingency planning, assess its effectiveness in different situations.

6 Measurement and reporting

6.1 The implementation and appropriateness of ICT contingency planning is monitored and assessed

Base level

6.1-1: The achievement of the target level of continuity, information security and contingency planning is monitored in the operational and financial planning process.

6.1-2: The state and development measures of information processing services supplied by service providers are monitored regularly.

6.1-3: Audits or self-assessments are carried out systematically and they are approved by management.

Increased level

6.1-4: Internal auditing as a function (audit plan) and supervisors regularly control that risk assessments of products, services, operations, processes and systems have been performed and that continuity management is taking place.

6.1-5: Reviews and audits of service network contingency planning and information security measures are performed.

6.1-6: Based on encountered incidents, the owner of the function or asset specifies and assigns responsibility for the measures by which perceived risks are reduced to an acceptable level.

High level

6.1-7: Contingency planning and information security audits are performed in accordance with instructions issued by the National Communications Security Authority.

Examples to support the application of requirements:

6.1-1: The organisation has an annual audit plan, based on which audits are performed, for example, concerning the organisation's management processes, the information security and continuity requirements of all outsourcing and service-level agreements, and critical information systems. The organisation may perform audits according to its own donut dial for annual planning.

6.1-2: A review by the customer is performed at an agreed time in order to discuss the state of agreed measures and decide about new continuity management measures that the service provider should carry out..

6.1-3: The management of an organisation has approved principles according to which units assess the information security of their own activities every other year and report on the results.

6.1-4: The results should be analysed; it is not sufficient to just follow the numbers. The number and severity of detected negative findings may be used as indicators of audits. The measurement process is important in order to discover further development measures. Indicator 1: How many development proposals are carried out? Indicator 2: How large a proportion of application development work is used to correct errors? It would be useful to have a common framework for measurement. Indicator 3: How many times the delivered system must be repaired after the first delivery?

6.1-5: To avoid overlap it is important to cooperate with internal auditing. Resourcing of information security for special situations and emergencies is monitored in the organisation's operational and financial planning. Auditing is scheduled with the service provider and this is documented to ensure the coordination of operational and financial planning. The organisation's security management coordinates audits and inspections.

6.1-6: Measures and their expected impacts are documented in the risk management monitoring report. New security controls are documented and their effectiveness in the process is monitored. High-level systems are audited by the National Communications Security Authority.

6.1-7: External resources are needed for the auditing of technical solutions, because the public sector does not have enough auditing expertise in various technical fields.

Appendix 2 Key statutes and instructions directing ICT contingency planning (in August 2012)

1 Acts and decrees

Acts and decrees		
Document	**Contingency planning content**	**Came into force**
Emergency powers act 1552/2011	Central government coordination, administrative branch obligations	2012
Act on information security assessment bodies (1405/2011)	The Finnish Communications Regulatory Authority's role as the approver of assessment bodies. The requirements for an information security assessment body.	2011
Act on the assessment of public authorities' information systems and telecommunications (1406/2011)	Information security assessment of public authorities' information systems or telecommunications. Finnish Communications Regulatory Authority's tasks in promoting and ensuring the information security of public authorities' information systems and telecommunications.	2011
Information management act (634/2011)	Steering and coordination obligation for the Ministry of Finance with respect to interoperability. To facilitate and ensure the interoperability of public sector information systems, a public sector authority must plan and describe its enterprise architecture. In addition it must adhere to the enterprise architecture and the interoperability descriptions and specifications required by it as well as sector-specific interoperability descriptions and specifications.	2011
Government Decree on Information Security in Central Government (Information Security Decree, 681/2010)	Obligations concerning the protection of information	2010
Conscription Act (1438/2007, section 91, military service register)	Information on conscripts and those who have performed civilian service, e.g. for contingency planning.	2007
Act on Voluntary National Defence (556/2007, section 7)	National Defence Association may organise e.g. contingency training. A public authority may invite its members to contingency planning work.	2007
Decree on the Prime Minister's Office (393/2007, section 1)	Prime Minister's Office's task 24: the Government's security services, forming a general picture of the state of security, and the Government's joint contingency planning for emergencies.	2007
Act on the Emergency Services College (607/2006, section 1)	The task of the college is, among other things, to provide training related to contingency planning.	2006
Rescue Act (379/2011)	Civil defence contingency planning obligation.	2003
Communications Market Act (393/2003)	Telecom operators' contingency planning obligation.	2003
Government Rules of Procedure (262/2003)	Permanent Secretaries are to attend to the general security and contingency of the ministry and its administrative branch.	2003
Act on Background Checks (177/2002)	Criteria for making background checks.	2002
Act on Radio Frequencies and Telecommunications Equipment (1015/2001)	ICT contingency planning obligation.	2001
Environmental Protection Act (86/2000)	Contingency planning obligation.	2000

Acts and decrees		
Document	**Contingency planning content**	**Came into force**
Act on the Openness of Government Activities (Openness Act 621/1999)	Document secrecy criteria, documents relating to contingency planning for emergencies, see section 24(1)(8).	1999
Act on Television and Radio Operations (744/1998)	Contingency planning obligation to broadcast official bulletins.	1998
Act of safeguarding security of supply (1390/1992)	National Emergency Supply Agency's task; management relations (Ministry of Employment and the Economy) Obligation for administrative branches (emergency powers act)	1992
Criminal Code (39/1889, Chapter 12, section 3)	Contingency planning information; spying.	1989

2 Government decisions and resolutions

Government decisions and resolutions		
Document	**Contingency planning content**	**Came into force**
Government decision on security of supply objectives (539/2008)	Regulations/restrictions on the provision of services from abroad	2008
Government Resolution on the Strategy for Security in Society 2010		2010
Government Resolution on Enhancing Information Security in Central Government	Priorities: Preventive measures and contingency planning; Safeguarding information and its value.	2009

3 Official regulations

3.1 VAHTI Instructions

The Ministry of Finance VAHTI Instructions		
Document	**Contingency planning content**	**Validity**
3/2010 Information Security Instructions on Internal Networks	Internal network threats and continuity planning checklists, list of requirements	3.12.2010
2/2010 Instructions on Implementing the Decree on Information Security in Central Government	Information availability requirements Information security levels	28.10.2010
6/2009 Targeted Cyber Attacks	Instructions on contingency planning for targeted information network attacks	17.11.2009
5/2009 Effective Information Security	General instructions on information security management	29.6.2009
3/2009 Logging Instructions	Reacting to information security anomalies	11.5.2009
2/2009 General Instructions on ICT Contingency Planning	General ICT contingency planning principles	14.4.2009
3/2005 Management of Information Security Incidents	Management of information security anomalies	1.1.2005
5/2004 Securing the State Administration's Key Information Systems	General instructions for ensuring the operation of systems	1.12.2004

3.2 Ministry of Transport and Communication Instructions

Ministry of Transport and Communication Instructions		
Document	**Contingency planning content**	**Validity**
Preparedness instruction 1/2003, securing communications networks and services	Gives operators and user organisations criteria for contingency planning in emergencies as well as in disruptions in normal conditions.	2003
EMP protection instruction (MTC 7/ETS/89, 21.6.1989).	Instructions on protection against electromagnetic radiation.	21.6.1989

3.3 Finnish Communications Regulatory Authority Regulations and Instructions

Finnish Communications Regulatory Authority (FICORA) Regulations and Instructions		
Document	**Contingency planning content**	**Validity**
FICORA 54 A/2012 M	Regulation ON COMMUNICATIONS NETWORKS AND SERVICES	3.5.2012
FICORA 57 A/2012 M	Regulation ON MAINTENANCE OF COMMUNICATIONS NETWORKS AND SERVICES, AS WELL AS PROCEDURES AND COMMUNICATIONS IN THE EVENT OF FAILURES AND INCIDENTS	23.1.2012
FICORA 53 A/2011	Regulation ON THE OBLIGATION TO RETAIN IDENTIFICATION DATA	24.5.2011
FICORA 43 D/2010 M	Regulation ON ELECTRICAL PROTECTION OF COMMUNICATIONS NETWORK	16.12.2010
FICORA 309/2011	Recommendations 309/2011 S ROUTING OF EMERGENCY TRAFFIC FROM CORPORATE NETWORKS	1.9.2011
FICORA 33 C/2006 M	Regulation ON CONTROLLING AND SECURING EMERGENCY TRAFFIC	16.10.2006
FICORA 47 C/2009 M	Regulation ON INFORMATION SECURITY MANAGEMENT OF TELECOMMUNICATIONS OPERATORS	27.8.2009
FICORA 54/2008 M	Regulation ON SECURING COMMUNICATIONS NETWORKS AND SERVICES	14.2.2008
FICORA 306/2006 S	Regulation ON LOCKING OF PROPERTIES' TELECOMMUNICATIONS ROOMS	15.11.2006
FICORA 57/2009 M	Regulation ON MAINTENANCE OF COMMUNICATIONS NETWORKS AND SERVICES AND PROCEDURE IN THE EVENT OF FAULTS AND INCIDENTS	20.10.2009
FICORA 58/2009 M	Regulation ON THE QUALITY AND UNIVERSAL SERVICE OF COMMUNICATIONS NETWORKS AND SERVICES	20.10.2009

3.4 Defence Administration Regulations and Instructions

Defence Administration Regulations and Instructions		
Document	**Contingency planning content**	**Validity**
Defence Command's documents 06:01-08	Electrical work instructions to be used in installation work and regulations on EMP, HPM, EMC and lightning protection.	
NATO recommendations MIL-STD-461, MIL-STD-188-125 measurement recommendation MIL-STD-462	EMP, HPM, EMC	

3.5 National Emergency Supply Organisation Instructions

National Emergency Supply Organisation Instructions		
Document	**Contingency planning content**	**Validity**
Operational Continuity Management (SOPIVA recommendations)	Recommendations for companies on operational continuity management	15.5.2009

Valid VAHTI publications

VAHTI 1/2012	VAHTI Annual Report 2011 (VAHTIn toimintakertomus vuodelta)
VAHTI 3/2011	Instructions on Government ICT procurement (Valtion ICT-hankintojen tietoturvaohje) *
VAHTI 2/2011	Information security instructions for management (Johdon tietoturvaopas) *
VAHTI 1/2011	VAHTI Annual Report 2011 (VAHTIn toimintakertomus vuodelta 2010)
VAHTI 4/2010	Information Security Instructions for Social Media *
VAHTI 3/2010	Information Security Instructions on Internal Networks (Sisäverkko-ohje) *
VAHTI 2/2010	Instructions on Implementing the Decree on Information Security in Central Government
VAHTI 7/2009	Government Resolution on Enhancing Information Security
VAHTI 6/2009	Targeted Cyber Attacks (Kohdistetut hyökkäykset) *
VAHTI 5/2009	Effective Information Security
VAHTI 4/2009	Information Security Instructions for Personnel
VAHTI 3/2009	Logging instructions (Lokiohje) *
VAHTI 2/2009	General Instructions on ICT Contingency Planning (ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin) *
VAHTI 9/2008	General Instructions for Project Information Security (Hankkeen tietoturvaohje) *
VAHTI 8/2008	Central Government Information Security Glossary
VAHTI 7/2008	Informationssäkerhetsanvisningar för personalen
VAHTI 6/2008	Information security is an attitude. – A report of public administration information security training needs (Tietoturvallisuus on asenne - Selvitys julkishallinnon tietoturvakoulutustarpeista) *
VAHTI 5/2008	Preliminary Study on Government 24/7 Information Security Monitoring (Valtion ympärivuorokautisen tietoturvavalvonnan hanke-esitys) *
VAHTI 4/2008	Activity Report of Central Government Information Security Assessment Pool (Valtionhallinnon tietoturva-arviointipoolin toimintaraportti) *
VAHTI 3/2008	Information Security Instructions on Central Government Encryption (Valtionhallinnon salauskäytäntöjen tietoturvaohje) *
VAHTI 2/2008	Personnel Security as Part of Information Security (Tärkein tekijä on ihminen - Henkilöstöturvallisuus osana tietoturvallisuutta) *

VAHTI 3/2007	Results through Information Security – General Instructions for Information Security Management (Tietoturvallisuudella tuloksia - Yleisohje tietoturvallisuuden johtamiseen ja hallintaan) (VAHTI 5/2009 in english)
VAHTI 2/2007	Smartphone Information Security – Good Practices (Älypuhelimien tietoturvallisuus – hyvät käytännöt) *
VAHTI 1/2007	From Participation to Influence – Central Government Challenges in International Information Security Work (Osallistumisesta vaikuttamiseen – valtionhallinnon haasteet kansainvälisessä tietoturvatyössä) *
VAHTI 12/2006	Identification in Public Sector Network Services (Tunnistaminen julkishallinnon verkkopalveluissa) *
VAHTI 11/2006	Guide for Information Security Trainers (Tietoturvakouluttajan opas) *
VAHTI 10/2006	Information Security Instructions for Personnel (Henkilöstön tietoturvaohje) (VAHTI 4/2009 in english)
VAHTI 9/2006	Principles and Good Practices of Identity and Access Management (Käyttövaltuushallinnon periaatteet ja hyvät käytännöt) *
VAHTI 8/2006	Information Security Assessment in Central Government (Tietoturvallisuuden arviointi valtionhallinnossa) *
VAHTI 7/2006	Change and Information security, from Regionalisation to Outsourcing – a Controlled Process (Muutos ja tietoturvallisuus, alueellistamisesta ulkoistamiseen– hallittu prosessi) *
VAHTI 6/2006	Setting and Measuring Information Security Objectives (Tietoturvatavoitteiden asettaminen ja mittaaminen)
VAHTI 5/2006	Instructions for Information Security in Case Management (Asianhallinnan tietoturvallisuutta koskeva ohje) *
VAHTI 4/2006	A Survey of the Central Government's Arrangement of 24/7 Information Security Activity (Selvitys valtionhallinnon ympärivuorokautisen tietoturvatoiminnan järjestämisestä) *
VAHTI 3/2006	A Survey of Information Security Resources in Central Government (Selvitys valtionhallinnon tietoturvaresurssien jakamisesta) *
VAHTI 2/2006	Electronic Mail-Handling Instruction for State Government
VAHTI 3/2005	Management of Information Security Incidents (Tietoturvapoikkeamatilanteiden hallinta) *
VAHTI 1/2005	Information Security and Management by Results
VAHTI 5/2004	Securing the Central Government's Key Information Systems (Valtionhallinnon keskeisten tietojärjestelmien turvaaminen) *
VAHTI 4/2004	Datasäkerhet och resultatstyrning
VAHTI 3/2004	General Instructions on Protection Against Malware (Haittaohjelmilta suojautumisen yleisohje) *

VAHTI 7/2003	Instructions on Risk Assessment to Promote Information Security in Central Government (Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa) *
VAHTI 3/2003	Recommendation on the Assessment of the Information Security Management System (Tietoturvallisuuden hallintajärjestelmän arviointisuositus) *
VAHTI 2/2003	Secure Remote Access from Insecure Networks (Turvallinen etäkäyttö turvattomista verkoista) *
VAHTI 1/2003	Central Government Internet Information Security Instructions Valtion tietohallinnon Internet-tietoturvallisuusohje
VAHTI 3/2002	Central Government Remote Working Information Security Instructions (Valtionhallinnon etätyön tietoturvaohje) *
VAHTI 4/2001	General Instructions of the Information Security of e-Services (Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje) *

* Only available in Finnish

MINISTRY OF FINANCE
Snellmaninkatu 1 A
P.O. BOX 28, 00023 GOVERNMENT
Tel. +358 295 16001
Fax (09) 160 33123
www.vm.fi

2b/2012
VAHTI
December 2013

ISSN 1455-2566 (print)
ISBN 978- 952-251-521-6 (print)
ISSN 1798-0860 (PDF)
ISBN 978-952-251-522-3 (PDF)