



ICT *-contingency*

planning in abnormal conditions and exceptional situations



The functions vital to society are described in the Strategy for Securing the Functions Vital to Society (YETTS) and it also specifies which ministries are responsible for preparing for and dealing with exceptional situations related to threat scenarios. Preparedness consists of all measures to secure the smoothest possible operation of functions in all eventualities. ICT contingency planning means ensuring that ICT activities operate and information is secured by means of risk management both in normal and abnormal circumstances and in special and emergency situations as specified in the Strategy for Securing the Functions Vital to Society.

The operation of all organizations that are based on information technology services, basic registers and other corporate data are highly dependent on the smooth functioning of telecommunications and on the supply of electricity. This type of service network is operated and maintained by a network of in-house and external service providers.

Risks are high for a situation to arise where an environmental catastrophe, a major accident and a widespread information technology disruption, either wilful or accidental, may take place simultaneously. This is all the more challenging in times when companies and subcontractors providing and supplying services are required to minimize costs and optimize the use of resources, sometimes even to the point of risk levels.

Aspects related to ensuring the continuous management of operations and information security must be taken into account already at the outset, in the preliminary assessment stages of planning the operations, services and system development in organizations.

This makes it possible to cost-effectively plan for abnormalities in normal circumstances directly from the viewpoint of operational demands and to create a solid

foundation for preparedness in emergency conditions.

Organizations should specify the service level they require for each function and service, and determine a threshold level below which the functions and services are jeopardized after a given period of time has elapsed. The parties responsible for the functions determine and prioritize their continuity demands. These demands must be uniform throughout the service networks, otherwise the services cannot operate as required in different security conditions.

Continuity management and information security management measures allow organizations to improve their capacity to prevent disruptions in operations, reduce their effect on business operations and accelerate recovery from them.

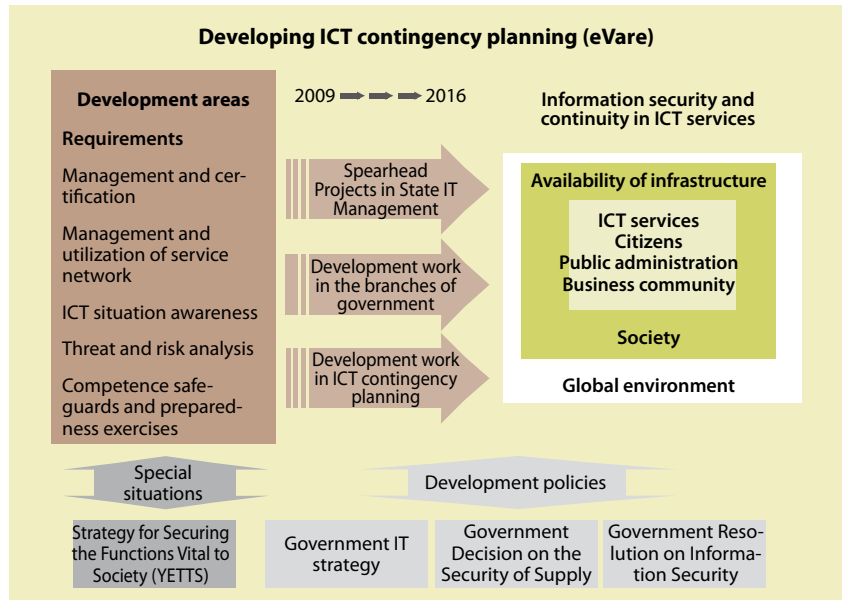


Development trends in the operating environment

- Services, processes, production chains and joint use of data and systems are all more automated and complex and become strongly integrated and networked.
- Services are acquired from a range of service network providers.
- Ownership relations and contract liabilities are constantly changing.
- International collaboration, steering and corporate governance is growing strongly.
- Threat scenarios become more sudden and grave .

The following principles apply when implementing ICT contingency planning

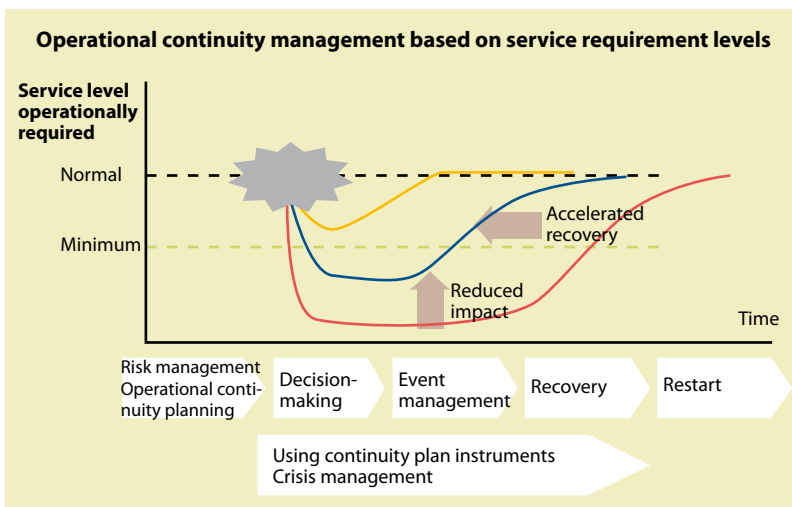
- ICT contingency planning based on risk management is implemented in the context of overall management, such as in connection with operating and financial plans and in performance management activities.
- Responsibilities, duties and seniority relations related to the operational continuity of core services, information security and emergency preparedness are specified in each organization's rules of procedure and in job descriptions.
- Each organization identifies the critical nature of its processes and operations and sets availability and service level requirements for them.
- The requirements are customized to cover the entire service network.

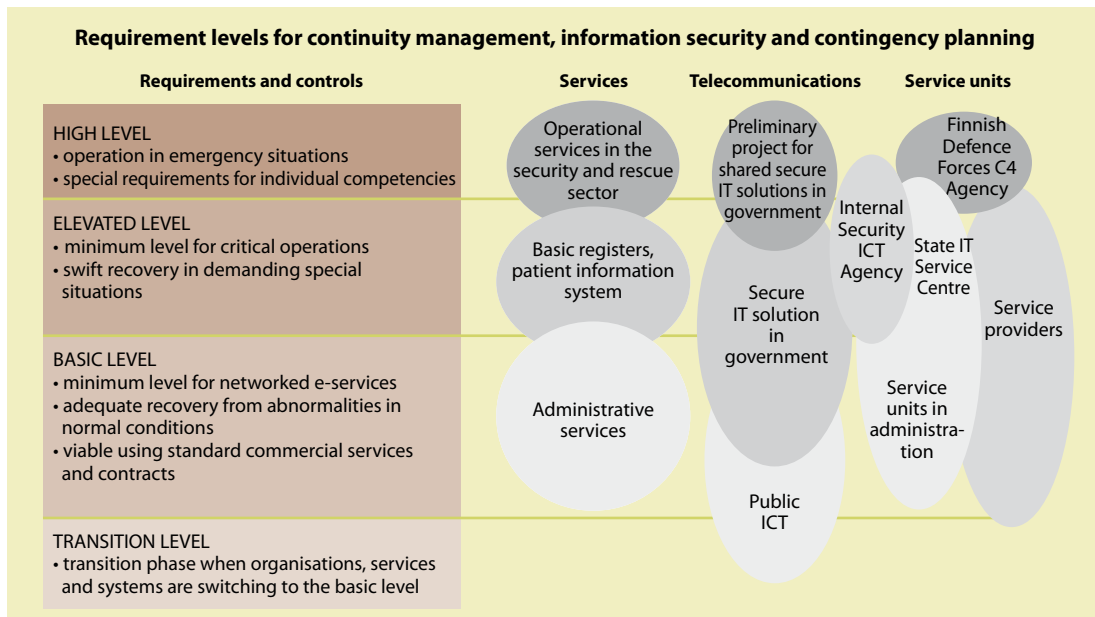


Reliability and security are the core requirements in ICT operations in public administration.

All actors operating in public administration are expected to meet uniform requirements and designated levels in information security and the ability to ensure continuity in operations and services in normal conditions, when disruptive incidents occur and in exceptional and emergency situations as specified in terms of the Strategy for Securing the Functions Vital to Society.

Requirements are set for the operations, services and ICT implementation in organizations from the viewpoint of operational continuity management and information security. These requirements include controls and gauges for basic levels, enhanced levels and high levels. Each organization determines at which level their own functions and the services it owns are placed.





General requirements in ICT contingency planning common to all actors

Strategic management and organization

- The organization has identified in its core functions the key operations, obligations and dependencies that steer operational continuity management, management in exceptional situations and information security safeguards.
- The requirements imposed by core functions for operational continuity management and for safeguarding information security have been specified.
- Operational continuity management and information security safeguards are organized and designated as a matter of course in ordinary management activities, organizational operations and partnership network management functions.
- Adequate resources have been allocated to operational continuity management and information security safeguards.

Collaboration, communication and reporting

- Plans on how manage continuity and safeguard information are implemented in collaboration between core and support functions.
- Cooperation with CERT-FI (Computer Emergency Response Team) functions smoothly and meets the organization's aims and obligations.
- Responsibilities and operating models between communications and reporting vis-à-vis the main stakeholders are specified and properly organized.
- Information on threat environments, the status of preparedness, the implementation and cost of development measures are all relegated to senior management.

Planning operations by means of risk management

- All operations take into account the interaction between the operating environment and the organization.
- A regular risk management procedure is in place.
- Risk management is used to control the execution of protective measures and the development of continuity management and information security.

Planning service continuity

- Measures to ensure service continuity management and information security are streamlined to the organization's core objectives.
- The execution of service continuity management and information security in the operating network is properly planned and settled.
- The management of service continuity in special situations has been properly planned and prepared.
- The execution of cooperation and communications in special situations has been properly planned and prepared.

Occupational skill needs and skills development

- Role- and job-specific requirements have been set for skill needs in continuity management and information security and these competencies are regularly enhanced.
- The organization encourages the staff to apply and develop good operating modes in continuity management and information security.
- The organization has in place a system for how to operate in situations of supervision and security breaches and where irregularities are detected.

Human resources management

- Key roles and key staff have been identified and back-up systems are in place.
- The use of human resources has been planned and calibrated to meet the requirements for securing continuity management and information security.
- Management instructions on how to operate in situations where disruptions occur in critical functions have been drawn up, and training and practice trials have been performed.

Contract management

- Key partners, subcontractors and resources for the organization's production have been identified.
- All contracts and agreements include requirements for operational continuity management and information security safeguards and how to impose them.

Safeguarding operations in special situations

- The management of special situations is properly organized and incorporated in the steering and operating models.
- The administrative obligation for securing the continuity of critical operations and information security is incorporated in the network of key suppliers.
- Collaboration with partners on how to manage disruptions and special situations is properly organized and designated.

Monitoring

- The execution and adequacy of continuity management and information security are monitored and evaluated.
- The activities are revised and developed on the basis of the evaluation results.