Conclusions and recommendations of the National Audit Office

Risk management and continuity of operations in central government

The purpose of the audit was to assess the preparedness measures that ministries and central government agencies have taken to ensure the continuity of their operations during disruptions occurring in normal conditions.

The purpose of risk and continuity management is to safeguard the continuity of the organisation's core functions in normal conditions, during disruptions occurring in normal conditions and in emergencies. The management and supervision of the emergency preparedness referred to in the Emergency Powers Act (1552/2011) is the task of the Government and each ministry in its own area of responsibility. The Prime Minister's Office is responsible for preparing a situation picture for the Government, and the overall coordination of the management of disruptions.

No such division of responsibilities or centralised steering and management arrangements have been specified for disruptions occurring in normal conditions. However, a significant or serious disruption occurring in normal conditions and affecting services or other activities may interrupt or substantially reduce the level of the activities, or interrupt the process towards achieving a strategic objective important to the activities. Third parties or central government as a whole may also suffer extensive damage or incur substantial costs as a result of the disruption.

Moreover, operations in emergencies are partially based on a situation where organisations have systems ensuring the continuity of their operations, and procedures for normal conditions and disruptions occurring in normal conditions. The difference between normal conditions and emergencies is not always clear. For example, in power supply, there is often only a fine line between the security of supply in emergencies and the reliability of supply in normal conditions. Power generation and grid capacity, as well as the output must be ensured during normal conditions and in crises causing emergencies.

Disruptions occurring in normal conditions may also become prolonged and escalate into more serious situations. In such cases, we are dealing with situations resembling emergencies, making the security of supply a key issue.

Centralisation of central government functions, organisation of cross-administrative projects, and risk and continuity management in extensive operational chains were also examined in the audit. The aim was also to find out whether central government risk and continuity management provides a sufficiently accurate overview of the situation for Government-level decision-making.

The purpose was to ensure that central government authorities have taken adequate measures to safeguard their operational reliability and service capacity and to review the development needs and potential in central government risk and continuity management. The information produced in the audit can be used in the development of central government risk and continuity management.

Security of supply was left outside the scope of the audit because it is connected with emergencies and not with disruptions occurring in normal conditions. Cyber security and (partially) the measures taken to ensure the continuity of electronic services were also left outside the

document. These topics are discussed in the performance audit reports Steering of the operational reliability of electronic services (15/2017) and Cyber protection arrangements (16/2017).

For reasons of simplicity, all central government units (ministries and agencies) are referred to as *agencies* in this report. We also use the term *ministry* when referring to matters specifically concerning ministries.

Agencies should prepare plans to ensure the continuity of their operations

As a whole, continuity planning in central government agencies is not at adequate level.

There is considerable variation between agencies concerning the manner in which they have prepared risk and continuity management documents. Half of the agencies had a risk and a continuity management plan, or at least one of them, while one third of all agencies had not prepared any plans. Moreover, there were significant inadequacies in the contents of many of the plans. They had not been updated or tested, or no exercises had been held to practice the measures set out in the plans.

However, some of the agencies had already started drafting and developing risk and continuity management plans. Moreover, during the audit, many of the agencies started reviewing and developing their own risk and continuity management processes. By applying performance guidance, ministries can also draw the attention of the senior management of the agencies in their administrative branches to risk and continuity management. Risk and continuity management should be incorporated into agencies' everyday management and operations.

Good agency-level risk and continuity management is not always enough

The limited number of tools available to an agency and the narrow agency-based situation picture are not sufficient when increasingly complicated risks occurring in changing operating environments should be dealt with. Many of the operating practices currently applied in central government require a more comprehensive approach to risk and continuity management. In many of the functions important to continuity, agencies now purchase the services from nationwide service providers, while ICT, financial administration and premises services are operated on a centralised basis. Moreover, risk and continuity management problems increasingly concern long operational and interaction chains, the administrative branch as a whole, or cross-administrative issues. The risks are often of such nature that individual agencies are unable to successfully manage them (nor is economically practicable for them to do it).

The recent recommendation on the risk management policy model (2017) issued by the Government Financial Controller's Function[1] has generated positive impacts but only in the agencies for which the recommendation is intended.

Central government agencies should start managing a more complex and extensive system of risk and continuity management even though there is no legislation obliging them to do it

The organisation of central government risk and continuity management highlights the responsibility of individual agencies even though the oper-

ating practices and issues concerning society at large and central government have become more complex and now cover a broader range of sectors.

There is no risk and continuity management covering central government as a whole, and central government is not a system of which an overall picture of risks and the way in which they are managed would be produced in normal conditions. In most cases, systematic continuity management only covers specific information systems, processes or agencies.

The same risks often affect several different authorities irrespective of the administrative branch, and the impacts of cross-administrative risks are not limited to specific administrative branches. Managing them successfully requires solutions specific to administrative branches, as well as solutions across their boundaries. Uniform and systematic operating procedures for the management of such multi-sectoral risks are not yet an established part of central government. Risk and continuity management should also be transformed from agency-specific processes into a process covering administrative branches or the Government as a whole even though there are no legal obligations to do this.

Reliance on technology, concentration of central government-internal services and networked operating models require the examination and management of continuity risks across the boundaries of agencies and administrative branches.

Recommendations of the National Audit Office:

1. All agencies and ministries that have not yet prepared a risk management policy, as laid out in the 2017 recommendation of the Government Financial Controller's Function, should, without delay, prepare documents that are accordance with the model or meet the requirements set out in the recommendation.
2. The management of each agency should, as part of the management system, take measures to ensure the continuity of the agency's operations. The agencies should apply the following Vahti instructions in their risk and continuity management: Toiminnan jatkuvuuden hallinta (Operational continuity management; 2016) and Ohje riskienhallintaan (Risk management instructions; 2017) or corresponding recommendations and standards. Risk and continuity management is part of the overall management process and for this reason, it should also be part of performance guidance and be set out as concrete objectives and obligations in performance and management agreements.
3. A report assessing the need to expand risk and continuity management into a process covering administrative branches or the Government as a whole should be produced and the compilation of the report should be coordinated by the Government Financial Controller's Function. The appropriate ways of examining and steering risk and continuity management and determining the responsibilities in the process should also be examined. The work should involve the Ministry of Finance, the Prime Minister's Office and, in an appropriate manner, the senior management of the other ministries.
4. As part of its steering task, the Ministry of Finance should ensure the continuity of the centralised services provided by Valtori in an appropriate manner, both from the perspective of the customer and Valtori itself.

[1] Riskienhallintapolitiikkamalli: asiakirjapohja viraston riskienhallinta-politiikan valmisteluun sekä liitteet, 2017 (Risk management policy model: document template for agencies' risk management policies, and appendices, 2017).